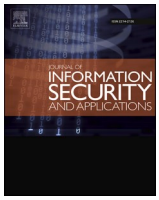
Journal of Information Security and Applications 88 (2025) 103927

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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



Towards an intelligent and automatic irrigation system based on internet of things with authentication feature in VANET

Huijing Zhang, Minbo Li *

School of Computer Science, Fudan University, Shanghai, China

ARTICLE INFO

Keywords:
Internet of Things
Vehicular ad-hoc network
Key agreement
User authentication
Intelligent irrigation
Fuzzy system
Security

ABSTRACT

Agriculture is essential for global livelihoods and economic stability, making efficient water management crucial. The Internet of Things (IoT) has revolutionized smart farming, offering advanced solutions such as precision irrigation systems. This paper presents an intelligent and automatic irrigation system that integrates IoT with vehicular ad-hoc networks (VANETs), with a particular focus on authentication and key agreement features. The system employs an energy-aware fuzzy routing algorithm and a neural network to optimize irrigation strategies based on real-time sensor data, including temperature and soil moisture. Key agreement mechanisms within the VANET framework ensure secure and authenticated communication between devices, safeguarding the integrity and confidentiality of irrigation data and control commands. This integration allows users to manage and monitor the irrigation system through mobile devices such as smartphones and computers, providing real-time insights and control. The proposed system is designed to be cost-effective, portable, and adaptable to various agricultural environments, including farms and greenhouses. Simulation results demonstrate that our system not only enhances network lifetime and power efficiency but also offers superior security and key management compared to existing protocols like WSN-IoT and LEACH. This approach addresses critical challenges in both secure communication and efficient water management, presenting a significant advancement in smart irrigation technologies.

1. Introduction

The agricultural sector is becoming an increasingly important industry in many countries, and it needs to become intelligent. Water is a valuable resource that needs to be kept using the most recent technology as the agricultural industry is currently utilizing intelligent modern technologies to develop solutions for resource efficiency [1,2]. In addition to industry, the Internet of Things (IoT) has expanded its possibilities in smart agriculture. Today, IoT is recognized as a new form of Internet use among users. Everything that may connect to the Internet in the IoT has a unique Internet address. The smart agriculture industry is just one of the numerous fields in which this new generation of the Internet finds applications [3]. The agricultural sector is a vital industry in many countries, and it needs to become an intelligent industry. The agriculture industry is currently utilizing cutting-edge intelligent technology to develop ways to use resources more efficiently, making water a valuable resource that needs to be managed with the help of these technologies. In addition to industry, IoT has advanced its potential in smart agriculture [4,5]. IoT is now acknowledged by users as a new way to access the Internet. Everything that may connect to the Internet in IoT has a unique Internet address. Water and agriculture intelligence is just one of the numerous domains in which this new generation of the Internet finds applications [2,6].

Using emerging technologies like IoT and networked communication equipment, modern and intelligent agriculture will be possible. There are several benefits to smart farming, including enhanced efficiency, maximized arable area, precise planning, and more. Farmers are now more profitable, the agricultural sector is more appealing, and they have access to tools that will help them deal with issues and problems in the future thanks to the application of current technology in intelligent agriculture [1,7]. An intelligent irrigation device is capable of communicating with several sensors and adjusting irrigation according to the data it obtains from them. These sensors can provide the central device with data about the quantity of moisture in the soil, the strength of the wind, and other factors like whether it is raining or not. Because irrigation is only carried out when your trees and plants require it, this method has an advantage over timer irrigation controls in terms of water use [8]. Smart irrigation, soil moisture, crop growth monitoring, and

* Corresponding author.
E-mail addresses: bxke05@163.com (H. Zhang), xptxp5@163.com (M. Li).

https://doi.org/10.1016/j.jisa.2024.103927

Available online 26 November 2024

remote damage detection are all achievable with the introduction of the IoT and digital transformation in rural regions. Smart agriculture is made possible by the employment of this technology. A new area of study is the remote management of agricultural operations using new technologies.

In general, the emerging technologies such as the IoT and Wireless Sensor Networks (WSNs) are playing a transformative role in reshaping rural and agricultural landscapes [9,10]. These technologies enable remote monitoring of agricultural activities, allowing farmers to stay informed about their crops without needing to physically inspect each field. For instance, soil moisture sensors help farmers identify when specific areas of the field require irrigation, ensuring water is used efficiently. Similarly, crop growth tracking allows the identification of potential issues like pest infestations or nutrient deficiencies before they become significant problems. Furthermore, damage detection systems powered by IoT sensors can alert farmers to issues such as broken irrigation lines, disease outbreaks, or adverse weather conditions, enabling timely interventions to minimize losses [2,11]. A neural network can significantly enhance these systems by analyzing the vast amounts of sensor data to derive actionable insights. For example, it can process data from multiple sensors to determine the optimal irrigation schedule, taking into account variables like current soil moisture, weather forecasts, and crop types. This level of automation not only reduces the burden on farmers but also ensures precision in water usage, leading to better crop yields and reduced wastage [2,3,12]. Moreover, the integration of these technologies with mobile devices such as smartphones and tablets provide farmers with real-time access to data and control over farming operations. This connectivity empowers them to make informed decisions on the go, enabling smarter, data-driven farming practices that improve productivity, conserve resources, and promote sustainable agriculture.

Vehicular ad-hoc networks (VANETs) have emerged as a critical component of intelligent transportation systems, enabling vehicles to communicate with one another and with roadside infrastructure dynamically [13,14]. VANETs are characterized by their high mobility, dynamic topology, and decentralized nature, making them suitable for applications like traffic management, road safety, and now, agricultural systems. Authentication is a vital aspect of VANETs to ensure that communication between nodes is secure and trustworthy. In VANET-based systems, authentication mechanisms verify the identities of communicating nodes, preventing malicious entities from interfering with the network [1,15]. Efficient and lightweight authentication schemes are particularly important due to the resource-constrained nature of many VANET devices, especially in environments like smart agriculture where the integration of IoT introduces additional complexities.

The advent of fifth-generation (5G) technology has significantly enhanced the capabilities of VANETs, offering ultra-low latency, high-speed communication, and robust connectivity. The 5G-enabled VANET architecture is shown in Fig. 1 [16]. A 5G-enabled VANET architecture integrates high-bandwidth communication with the mobility of vehicles, allowing real-time data exchange across vast geographical areas. In agriculture, this architecture facilitates seamless communication between IoT devices, mobile vehicles, and cloud-based systems, ensuring efficient resource management and control. The use of 5G networks also supports advanced applications like predictive analytics, remote monitoring, and real-time decision-making [3,16]. This architecture is particularly beneficial for deploying large-scale smart irrigation systems where reliable and fast communication is essential to handle dynamic and time-sensitive tasks.

Despite their potential, VANETs face significant security challenges due to their open and distributed nature. Key concerns include unauthorized access, data tampering, denial-of-service attacks, and eavesdropping, all of which can compromise the integrity and reliability of the network. For example, an attacker might spoof a legitimate device to disrupt irrigation schedules or manipulate sensor readings in a smart

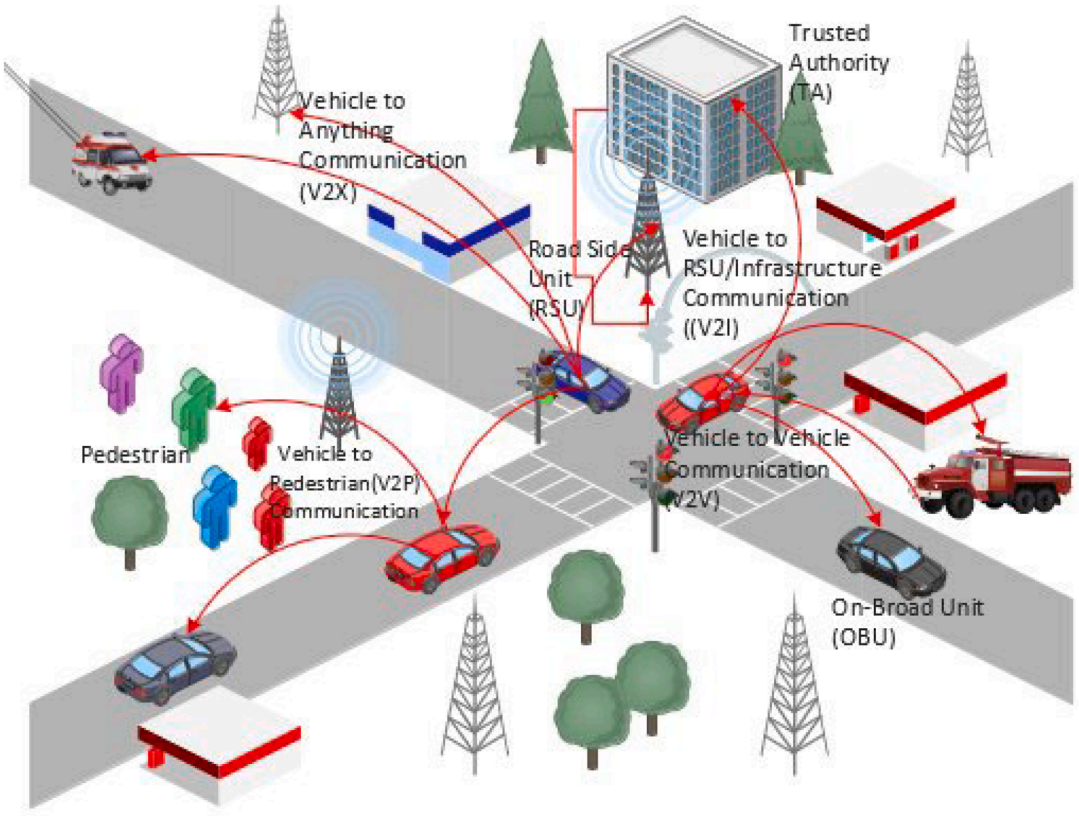


Fig. 1. 5G-enabled VANET architecture

agriculture system. Addressing these concerns requires robust security mechanisms, such as encryption, intrusion detection systems, and secure key management protocols [3,7]. Authentication plays a pivotal role in mitigating these risks by ensuring that only verified devices can participate in the network. The inclusion of such mechanisms in VANETs not only secures communication but also builds user trust in the technology, making it a viable solution for sensitive applications like smart irrigation.

Smart irrigation, soil moisture, crop growth monitoring, and remote damage detection are all achievable with the introduction of the IoT and digital transformation in rural regions. Smart agriculture is made possible by the employment of this technology. A new area of study is the remote management of agricultural operations using new technologies. This article uses wireless sensors and the IoT to construct an intelligent irrigation management system quickly and cheaply. A set of wireless sensors is part of the data extraction unit, which measures agricultural operations and gathers data on irrigation parameters. A neural network is trained to identify the optimal irrigation type based on data from sensors (temperature, soil moisture, etc.). The system's user can monitor agricultural products and oversee the process of gathering data via the IoT by connecting mobile devices—such as smartphones and laptops—to an Internet network. Furthermore, a rapid routing algorithm with a fuzzy foundation is intended to convey data that facilitates the distribution of energy usage throughout the network. In order to convey data from the hardware system to the interface software, such as a mobile application, the proposed technique focuses on the analysis of routing protocol in the WSN node. Meanwhile, the proposed work introduces an intelligent and automatic irrigation system that incorporates IoT and VANETs to ensure efficient and secure communication. One of the key features of this system is the integration of authentication and key agreement mechanisms within the VANET framework. These mechanisms safeguard the integrity and confidentiality of irrigation data, preventing unauthorized access and ensuring reliable operation. Additionally, the system employs an energy-aware fuzzy routing algorithm to balance energy consumption across the network, further enhancing its efficiency. This paper outlines the development and evaluation of the proposed system, which combines cost-effectiveness, portability, and adaptability to diverse agricultural environments. By addressing critical challenges in secure communication and resource management, the system represents a significant advancement in smart irrigation technologies, ultimately contributing to the broader vision of intelligent agriculture.

The main contribution of this paper is as follows:

- Setting up a neural network to identify the optimal irrigation type
- Developing an automated, low-cost intelligent irrigation system based on a fuzzy-based energy-aware routing approach
- Examining and contrasting the proposed approach to demonstrate the effectiveness of irrigation on greenhouses

The rest of the paper is organized as follows: Section 2 presents the background of the key concepts related to the research. Section 3 summarizes the related work in the field. Section 4 explains the system model in detail. Section 5 describes the proposed methodology. Section 6 provides a simulation analysis of the proposed approach. Finally, Section 7 concludes the paper.

2. Background

This section includes some basic concepts related to the motivation of presenting the proposed method and describing the problem.

2.1. Motivation

Information for computers, and consequently the Internet, comes virtually exclusively from people. This idea, which forms the basis of intelligent technology, can be applied to farms, greenhouses, gardens, and fields to effectively control irrigation. The field of smart farming is well-established, and there are many advantages to integrating technology and farmers' knowledge, such as better crop health, increased hygiene, quicker tracking, better water management, and more. According to Rajkumar et al. [1], one of the most crucial resources in agriculture is water. Humans are the largest user of water resources because they use a lot of it—nearly 100 times more than they need for personal consumption—in agriculture and because they utilize 70% of rivers and groundwater for irrigation [7]. Furthermore, evaporation losses in traditional agriculture account for nearly half of the water used. This has prompted a great deal of research into the effective use of this finite resource. In the topic of smart agriculture, many research groups have done a great deal of effort and continue to do so. The majority of IoT technologies recommends using WSNs to control water usage.

Both IoT and big data are concerned with the platforms that enable us to gather information from a wide range of sensors and utilize it to create models. One of the driving factors behind the big data explosion has been IoT. This has led to a change in data architecture from the 2Vs (Veracity and Validation) model to the 3Vs model (Volume, Velocity, and Variety). The term "veracity," which was first used by International Business Machines (IBM) [17], describes the extent to which a dataset contains noise, missing data, or unknown data. Validation, as it relates to big data, is the process of determining whether the data is reliable enough for additional usage. Big data and IoT advancements have made data analysis techniques a very popular topic for study and conversation. The growing importance of this issue is also reflected in the IoT and big data companies' expanding revenue [17].

IoT systems are typically made up of a heterogeneous collection of networked devices that produce vast amounts of various types of data at various rates. Upon perusing the publications pertaining to IoT-big data, it becomes evident that the primary focus of these conversations is on the various stages of data collection, processing, analysis, and storage. As a result, four subfields can be distinguished within this field: analysis, processing, transmission, and storage [3,18]. In order to create databases that are suitable for the volume and diversity of the data, the storage sector concentrates on the IoT's data storage procedures and applications. The transfer of data to storage databases is the main topic of the transmission subfield. The processing subfield deals with data analysis, either in batch or in real time. The volume of data produced by IoT systems could previously be easily handled by conventional data analysis techniques. These techniques, however, are ineffective for turning the data produced by modern IoT systems into big data. Thus, the analysis area deals with the development of a set of reliable data analysis techniques that are necessary to extract useful knowledge from the large data generated by the IoT. An overview of the connection between big data and IoT is shown in Fig. 2 [19,20].

Even though the number of IoT devices has increased over the past ten years, producing vast volumes of data has not stopped, these data will be meaningless if not properly analyzed. The amount of data we produce rises when we use IoT devices, which presents excellent prospects for value extraction through data analysis. But these massive volumes of data are only within the control of big data technologies and frameworks. In addition to allowing for the extraction of useful information from IoT data, big data analysis solutions can also lower the amount of data that IoT systems need to store. Data mining techniques are typically employed by the technologies that are frequently utilized for large data research. The data mining techniques offer effective ways to describe or forecast large amounts of data as well as spot patterns in historical data that may be applied to fresh data. To evaluate the gathered data and raise the IoT systems' level of intelligence, numerous data mining techniques have been employed. According to Mohindru et al. [21], there are three types of data mining techniques employed in the IoT: descriptive, predictive, and categorical.

Our requirement for more advanced data processing techniques grows along with the number of IoT devices. Real-time sensor data

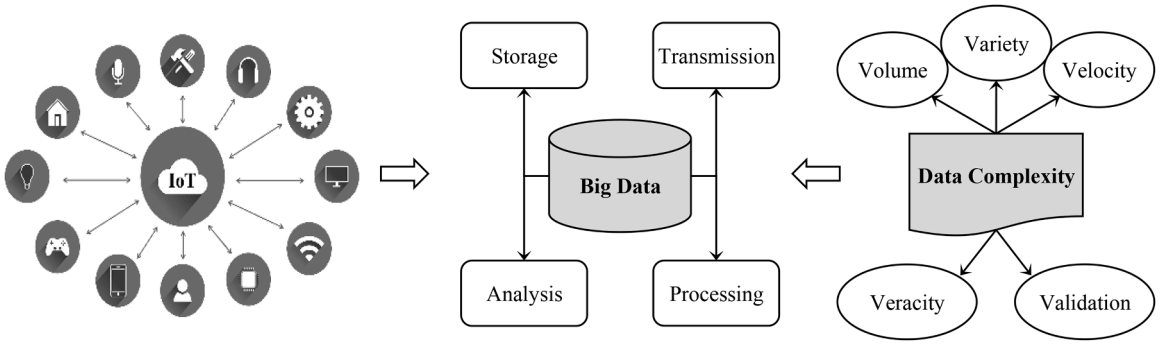


Fig. 2. IoT and big data relationships

processing in the IoT is essential for business purposes in order to identify patterns. With the use of data mining and artificial intelligence techniques, sensor data may be efficiently gathered and stored by the big data technologies currently in use. Data integration, data filtering, data cleansing, and other procedures, each with a distinct function, are frequently included in data mining operations. Classification, analysis, prediction, clustering, and pattern recognition techniques are among the data mining techniques frequently used for knowledge extraction from data. Fig. 3 depicts the fundamental architecture of data mining for IoT applications [19,20].

2.2. Neural networks

Advancements in sensor technology and the widespread adoption of smart solutions across various domains, including environmental, industrial, and medical sectors, have created numerous opportunities for innovative applications [22,23]. Applications simultaneously are becoming more complex; thus, the end-user needs a platform that carries these applications to support mobility and flexibility to act more adaptively to new requirements. Also, when designing the system, it must be taken wider than what was before. Typically, applications based on WSNs, broadcast, monitoring systems, IoT, and peer-to-peer relay we can rely on including cloud services. Time and location are the most stringent restrictions for these systems and services. Thus, the situation is more stringent in terms of multimedia data transmission, and to overcome network problems special processing and protocols are used for multimedia applications (broadcast, telephone, etc.) [24,25]. Because of the flow of data packets in the network, the Quality of Services (QoS) must be considered, such as delay, data loss rate, and costs, to maintain the quality of data transmission. Therefore, routing is a crucial factor that has a significant impact on packet switching in network performance.

Since of the constraints governing the process of exchanging packets on the network, routing algorithms should provide the most appropriate path (optimum) for the network according to the traffic volume and QoS conditions. Therefore, arithmetic operations must be performed when the transmission command is received between the network's routers. Neural networks are at the forefront of these operations because they perform enormous operations to manage the situation in conjunction with the rest of the transmission process procedures. This study investigates using the neural network, which is fully compatible with the multi-routing of Internet networks.

2.3. Authentication in VANET

Authentication in VANETs is a critical security mechanism that ensures the integrity, reliability, and trustworthiness of communication between vehicles and other network entities [3]. In VANETs, vehicles continuously exchange a significant amount of data, including location, speed, traffic conditions, and emergency alerts. Since this information can directly impact the safety and efficiency of transportation systems, robust authentication mechanisms are necessary to verify the identity of each communicating entity and prevent malicious activities [1,26]. The primary goal of authentication in VANETs is to confirm that the data received by a vehicle or infrastructure component originates from a legitimate source. This is typically achieved through cryptographic techniques, such as digital signatures, certificates, or key agreement protocols. For instance, each vehicle may possess a unique digital

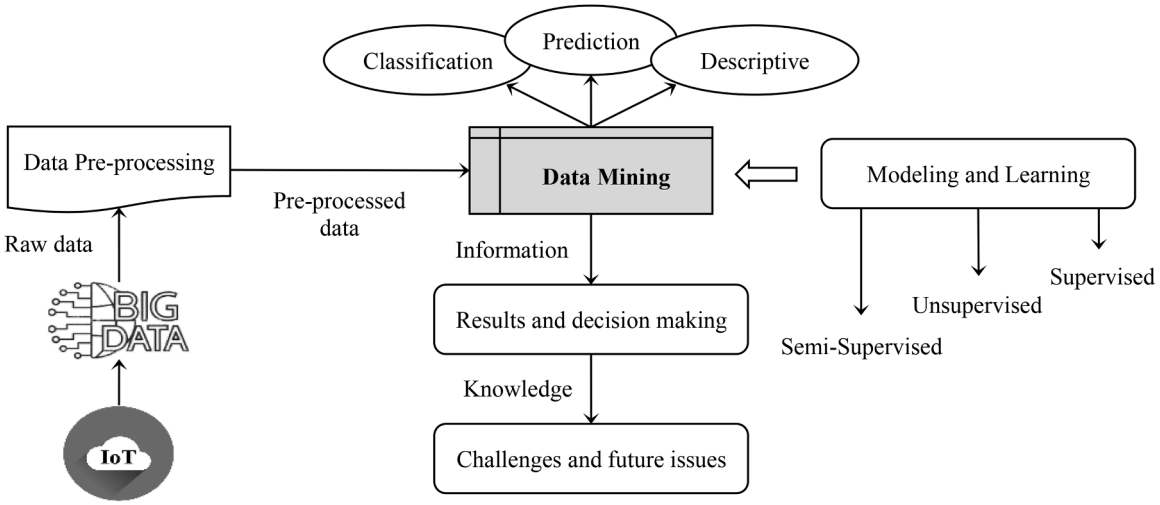


Fig. 3. IoT applications' data mining architecture

certificate issued by a trusted Certificate Authority (CA). Before accepting data from another vehicle, the recipient verifies the sender's certificate and digital signature, ensuring that the message is authentic and unaltered. Fig. 4 shows the taxonomy of authentication schemes [27].

Authentication in VANETs also faces unique challenges due to the highly dynamic and distributed nature of these networks. Vehicles are constantly entering and leaving communication zones, which makes maintaining real-time authentication a complex task. Additionally, authentication mechanisms must be efficient to handle the high mobility of vehicles without introducing significant delays [3,28]. Lightweight cryptographic algorithms and group-based authentication techniques are often employed to achieve this balance between security and performance. Another key aspect of VANET authentication is privacy preservation. While it is essential to verify the identity of vehicles, exposing their exact identity or location to unauthorized entities could lead to privacy violations. To address this, pseudonym-based authentication schemes are widely used [29]. Vehicles use temporary pseudonyms instead of permanent identifiers, which are periodically changed to prevent tracking while maintaining secure communication. Overall, authentication in VANETs plays a foundational role in building trust and enabling secure communication in intelligent transportation systems. By preventing unauthorized access, detecting fake messages, and ensuring data integrity, authentication mechanisms contribute significantly to the safety, reliability, and efficiency of VANET applications.

3. Literature reviews

The field of smart irrigation has witnessed significant advancements in recent years, with various studies leveraging technologies such as the IoT, VANETs, and machine learning to optimize water management in agriculture. This section reviews the most relevant works in this domain, highlighting their contributions, limitations, and how the proposed system advances the state of the art [1]. The application of VANETs in agriculture is an emerging trend that seeks to enhance real-time communication and data exchange in large and distributed farming areas. Unlike traditional WSNs, VANETs offer higher mobility and flexibility, making them suitable for dynamic agricultural environments [2,3]. Previous works in this area have primarily focused on improving routing protocols to ensure reliable data transmission. However, limited attention has been given to integrating VANETs with IoT for smart irrigation and addressing the associated security concerns. Security and authentication are critical aspects of any system involving IoT and VANETs. Numerous studies have proposed mechanisms for secure communication in these networks [3,7]. For example, lightweight cryptographic algorithms and blockchain-based solutions have been explored to protect data integrity and prevent unauthorized access. While these approaches enhance security, they often impose computational overhead, making them unsuitable for resource-constrained environments like agricultural IoT systems.

The IoT and irrigation intelligence have been extensively studied in agriculture in an effort to reduce water use and improve the quality of agricultural output. Krishnan et al. [30] proposed fuzzy logic based on IoT-based intelligent irrigation systems. This study computes the input parameters and generates the engine condition output using a fuzzy logic controller. A neural network- and IoT-based water pumping control system for intelligent irrigation was proposed by Karar et al. [31]. This research uses a Multi-Layer Perceptron (MLP) and a combination of sensors to reduce water waste in IoT irrigation processes. A machine learning method, like the MLP neural network, is a useful tool for supporting the automatic control of irrigation systems based on the IoT and for controlling water consumption.

Agrinex, a low-cost wireless network-based intelligent irrigation system, was proposed by Tiglao et al. [32]. Using a wireless sensor and excitation network, this offers an alternative to current monitoring techniques in agricultural land and an irrigation mechanism to support resource saving measures. The Agrinex system consists of a network-like arrangement of in-field nodes that function as an actuator on a drip irrigation valve in addition to being sensors for temperature, humidity, and soil moisture. An improvement in IoT security through the use of encryption methods for intelligent irrigation systems was proposed by Mousavi et al. [33]. In order to safeguard sensitive data in IoT-based intelligent irrigation systems, this study proposes a novel hybrid encryption technique that combines the safe Hash algorithm, elliptic-curve encryption, and hedge encryption. The outcomes validate this model's efficacy and provide evidence for secrecy based on confidentiality analysis.

Nawandar and Satpute [34] proposed the WSN-IoT algorithm, an intelligent IoT-based module that is inexpensive and can be used to create an intelligent irrigation system. This software's features include a manager mode for user interaction, the ability to estimate the type of irrigation by making settings only once, remote data monitoring, and neural network-based decision making for intelligent support. Furthermore, even from a distance, the system notifies the user via MQTT (Message Queuing Telemetry Transport) and HTTP (Hypertext Transfer Protocol) of the current crop and irrigation conditions. Alomar and Alazzam [35] proposed utilizing fuzzy logic and an IoT controller to create an intelligent watering system. This study aims to develop an IoT

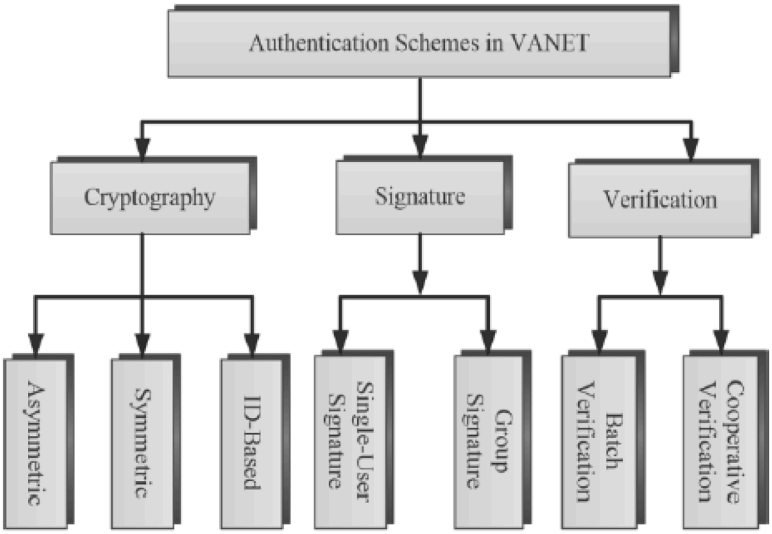


Fig. 4. Taxonomy of authentication schemes

based irrigation system that uses fuzzy logic to increase production while reducing irrigation frequency. The system comprises of a Mamdani fuzzy controller that measures the soil moisture content and outdoor temperature using specific sensors. It then applies a set of fuzzy rules to regulate the water pump's flow as well as the ideal frequency and timing of irrigation.

Ni et al. [36] proposed an ant gene colony routing optimization algorithm in an IPv6 environment to optimize four QoS constraints: cost, delay, data loss rate, and bandwidth. Since there was no pheromone at the beginning, it took a long time to create one and determine which course of action was best. Early on, the ant colony algorithm was kept running at a comparatively slow search pace. Mofaddel et al. [37] introduced an improvement of the multi-routing based on the ant colony algorithm, compared with the MAODV (Multicast operation of the Ad hoc On-Demand Distance Vector (AODV)) proactive routing protocol to ensure the reliability of networks while providing QoS constraints (cost, delay, and hop count). Hamed et al. [38] presented an improvement for multi-routing using the ant colony algorithm. Compared with the Atzori and Raccis algorithms, theirs considers QoS constraints, delay, cost, and hop count, thereby producing results with a higher performance than the two previously mentioned algorithms.

Anibrika et al. [39] introduced an improvement in the Energy Efficient Optimum Multicast Routing Algorithm (EEOMRA) using the ant colony algorithm considering four parameters: residual energy, connections established, dead nodes, and network lifetime. Li and Peng [40] introduced an improvement in the traditional ant colony algorithm that runs slowly using the fortified ant protocol. In order to increase multicast routing speed, the protocol introduces the concept of elite ants and initially provides a sorting algorithm based on the ant colony algorithm. Thereby making their algorithm comparable to AODV, Dynamic Source Routing (DSR), and Area Operation Centers (AOC) routing algorithms. Zhang et al. [41] improved the ant colony algorithm using a cloud model. For a lower cost multicast routing tree that satisfies the bandwidth, latency, and delay jitter conditions, the innovative main point is to combine the solution generation process of the Ant Colony Optimization (ACO) compared to the traditional ant colony algorithm.

Pullagura and Rao [42] proposed an effective multiple routing protocol using an Ant algorithm with an Improved Pheromone Update Rule (AIPUR) for Mobile Ad-Hoc Networks (MANETs). During the enhanced pheromone update, the worst ants are identified and removed using the modified Technique for Order Preference by Similarity to Ideal Solution method (TOPSIS). Initially, grouping is performed for the authentication process and the group header is optimized by increasing its security level, energy availability, and bandwidth. Kavitha and Ganapathy [43] used an ant colony algorithm in multi-routing in wireless networks to compare the performance of the current Three Pheromones ACO (TPACO) system with the proposed an Efficient and Optimal Routing - ACO (EOR-ACO) system. Here, the considered factors were as follows: bandwidth integrity, delivery rate, delay, throughput, and remaining energy.

Batth and Singh [44] introduced a comparison between three routing protocols used in mobile ad hoc networks after using the ant colony algorithm in each of them. The comparisons considered three main factors, namely, Packet Delivery Break (PDB), throughput, and routing for a variable simulation time. Reshadi and Mirmahaleh [45] propose two algorithms to improve the performance of models that use deep neural networks for mapping in IoT networks. So that an algorithm was created to reduce the time and the other to reduce the energy on the network, which leads to an increase in data flow so that the two algorithms were included in a flexible structure to support the mapping of models for different reconfiguration so that the results of the analysis indicate a reduction in energy by a rate ranging from 21-92%, in addition to a reduction in time by a rate ranging from 14-21%.

Gopikrishnan et al. [46] proposed a multicast sensor hybrid model for IoT networks that saves energy and time. It is based on identifying and recording sensors for IoT applications Hybrid framework for Sensor Identification and Registration (HSIR) therefore, the results indicate that the model is efficient in terms of sensing points on the network that contributes in achieving a multicast path with a decrease in energy and time, compared to three protocols (SMART LINK and RIoT) and CASSARAM a context-aware sensor search, and ranking model. Chuang and Tsai [47] proposed a routing algorithm to reset transmission between nodes based on calculating the specific location of each metadata for mobile networks and the IoT to increase the efficiency of the network in terms of reliability to avoid the use of fake nodes, in addition to the nodes that refuse to forward so that the results of performance evaluation indicate a decrease in the cost of a path in large and mobile networks.

Sedaghat and Jahangir [48] proposed a routing algorithm for mobile networks and the IoT to improve network performance in terms of access time to destination nodes called R2T-DSDN reliable real-time distributed controller-based Software-defined network. Therefore, the algorithm is based on statistical and probability models to determine critical and non-critical cases of the network; the main controller of the network structure distributes network traffic dynamically. The results indicate that the algorithm achieves a success rate of 97.9% for packet arrival. Hashemi and Shams Aliee [49] proposed a model to increase the reliability of the Routing Protocol for Low-Power and Lossy Networks (RPL) in order to overcome the limitations of the RPL protocol led to loss of network performance in mobile networks. It is called DCTM-IoT dynamic and comprehensive trust model for IoT, where a dynamic trust model was integrated into the protocol to protect against routing attacks so that the results indicate the efficiency of the model over the standard protocol in terms of energy savings, packet loss rate and delay, in addition to reducing attacks on the network.

4. System model

In this approach, users can access the VANET service cloud through a user terminal equipped with a biometric smart card reader. This terminal can be integrated into vehicles, located in offices or homes, or included in other mobile devices based on the user's preference. Users can utilize any available terminal to retrieve information objects they are authorized to access, as specified by the credentials embedded in their smart card [50–52]. The design assumes that an Authentication Server (AS) possesses the necessary functionality to act as a Legal Executor (LE), responsible for ensuring the smooth operation of the system and performing any required legal procedures. This section provides a detailed explanation of how the proposed protocol facilitates the retrieval of information objects from the VANET cloud using the user's biometric smart card. The protocol is structured into three key phases: registration, login, and general authentication. Each phase plays a critical role in establishing secure and reliable access to the system.

During the registration phase, the *AS* generates a smart card for each authorized user P_id_i and subsequently distributes the card upon successful completion of the registration process. It is presumed that all transactions between P_id_i and *AS* are conveyed only over designated secure channels. The procedures listed below are executed by both P_id_i and *AS* parties to achieve successful registration with *AS*. The initial user P_i selects their identification id_i, password pw_i, personal biometric features B_i', and a 128-bit random integer r_i. In the subsequent stage, the proposed protocol employs a fuzzy extractor to compute the biometric key, utilizing a roughly uniformly distributed random probabilistic generation function $G(.)$. This fuzzy extractor tackles both error tolerance and non-uniformity [53]. This reliably creates R randomly by extracting from the provided biometrics B_i' and has a size of r bits. R is defined as the biometric key of P_id_i and is represented as $R \in \{0, 1\}^r$. A secure sketch function $G_s(.)$ and a fuzzy extractor are defined to regenerate biometric keys. The fuzzy extractor produces P as an output from the provided biometrics B_i' (which are close to the original biometrics). It should be observed that R is upheld as uniformly random for the

specified P. The proximity between B_i' and the original biometrics is determined by the Hamming distance $h_m^b(B_i', BioOri_i) \leq h_m$, where h_m is an acceptable error tolerance level. The $G_s(.)$ function generates the biometric key for $P_i d_i$ by utilizing two inputs, B_i' and P, so that $F_i = G_s(B_i', P)$, while according to the defined parameters, $F_i = R$.

During the authentication phase, the *AS* initiates the process by receiving $M_1 = \left(E_{P_{k_{i1}}}\{P_i d_i, f_{i1}, m_{i1}, m_{i2}, K_{i_L}, K_{i_A}, T_l\}, P_i d_i\right)$ and subsequently authenticates the user. A secret session key is established between them for subsequent secure communication through successful authentication. If the timestamp is determined to be within the valid limit, then *AS* generates a response. In the subsequent phase, r_i is obtained by the *AS* as $v = (P_{k_{i1}} \parallel T_{A_r}) \oplus K_{i_L}$. In the subsequent phase, it computes $(f_{i1}||T_{A_r}||T_l \parallel r_i)$ and assesses its equality with m_{i2}. Consequently, the equality confirms the veracity of user $P_i d_i$. Otherwise, the authentication procedure is canceled by the *AS*. In the subsequent stage, *AS* produces a 160-bit key P_{AS} and embeds it into m_{i6} to signify a successful GAP phase, hence reusing the shared-secret key for a specific session to circumvent the redundant general authentication phase and computes the following: $m_{i3} = v \oplus r_{LE}$, $m_{i5}' = (P_{k_{i1}}||T_{A_r}||r_i||r_{LE}||T_{LE}\| K_{i_A})$, $m_{i6} = m_{i5}'||(P_{AS} \oplus f_{i1})||T_{A_r}$.

5. Methodology

This research provides an intelligent neural network and fuzzy logic-based crop monitoring and irrigation system. By considering the requirements of both soil and plants, the proposed intelligent irrigation system effectively uses water. To do this, it is necessary to take into account the following parameters that are obtained from WSN: irrigation technique, rainfall, location, plant growth stage, ambient humidity, ambient temperature, evaporation rate, soil moisture, crop growth rate, crop planting time, crop water requirement, kind of mechanical stimulus, and maximum and minimum temperature. These factors often indicate how much water a product needs, which can be utilized to create an intelligent, self-contained irrigation system that doesn't require human input. The proposed intelligent irrigation system monitors the environment continuously, reads sensor data, connects to a broker to share information, selects an irrigation mode, determines the output amount of water, transfers the decision to the Irrigation Unit (IU) [20]. A conceptual architecture of the proposed technique, comprising four layers, is depicted in Fig. 5.

The first layer deals with gathering data via a WSN that has a set number of nodes. The irrigation parameters can be collected by the nodes utilized in this part using their sense of environment. These nodes may send data via radio frequency protocol and transform analog signals

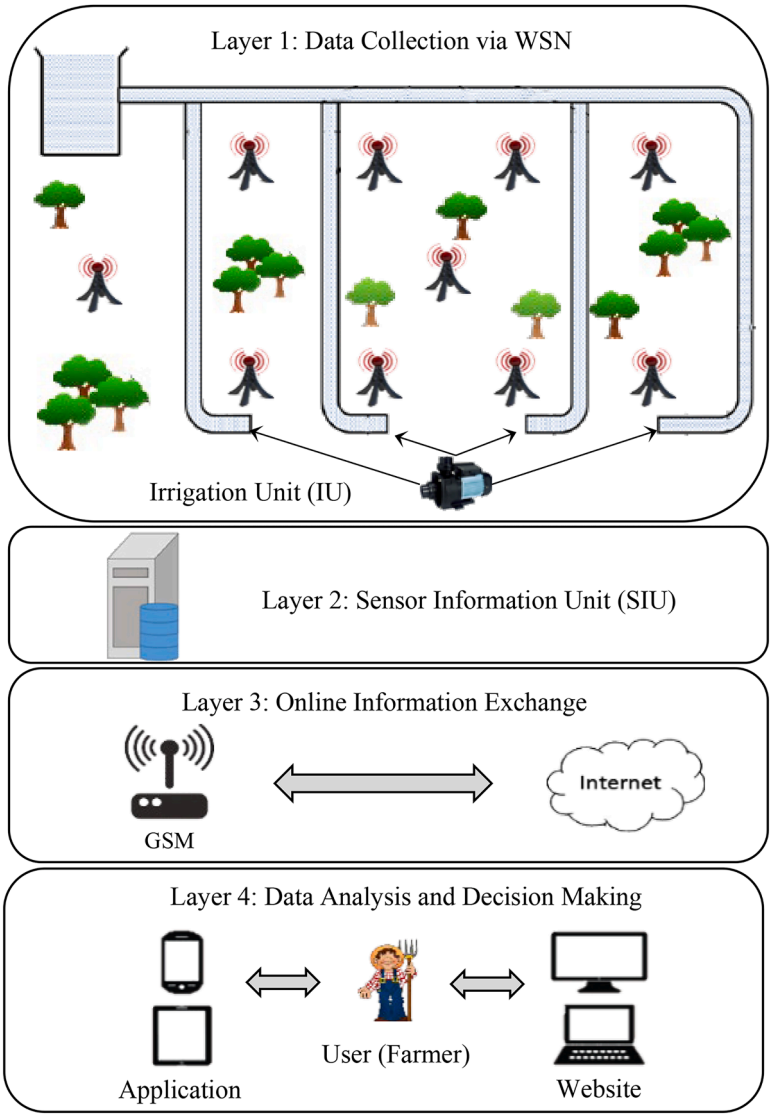


Fig. 5. Architecture of the proposed irrigation system

to digital ones. Apart from WSN-related apparatus, the IU provides a water supply that has the ability to uphold decisions that have been submitted. A Sensor Information Unit (SIU), which is in charge of processing data and corresponding with Internet-connected devices, makes up the second layer. SIU can converse and share information as well. The SIU can transmit data obtained from the WSN to the server (or application) via a GSM (Global System for Mobile) modem linked to the Internet, which makes up the third layer. As a result, the server handles data analysis, which makes the system design simpler. A server or application platform that allows the user (farmer) to access and control its data makes up the fourth tier. An application is any program or website that operates on a desktop computer or mobile device [20].

In this study, an efficient and inexpensive management system for IoT-based intelligent irrigation has been developed. To gather data, a variety of wireless sensors are employed. Information from these sensors includes temperature, moisture content of the soil, light intensity, frost monitoring, and more. Utilizing this data will enable improved irrigation system management and measurement of agricultural activities. A neural network is trained to identify the optimal irrigation type based on the data gathered. Here, an expert will supply a sequence of real inputs and outputs to train the neural network. The system's user can monitor agricultural products and oversee the process of gathering data via the IoT by connecting mobile devices—such as smartphones and laptops—to an Internet network. Furthermore, a fast-routing technique with a fuzzy foundation is intended to convey data [20]. At the start of the setup, the proposed routing algorithm generates a routing table for each sensor; the routing table is only updated in the event that one sensor—the neighborhood switch—is turned off. Fig. 6 displays the

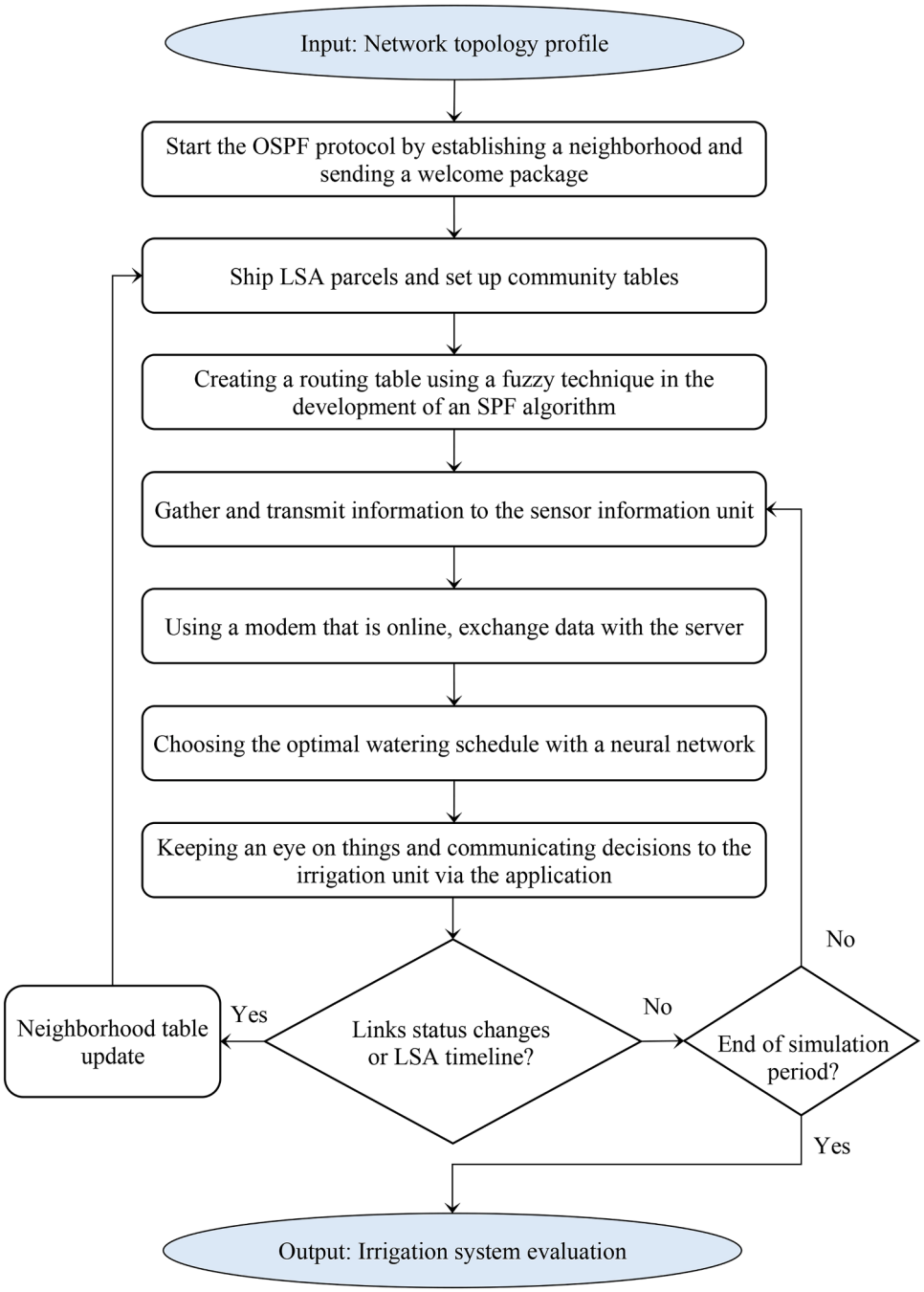


Fig. 6. Flowchart of the proposed method

proposed method's flowchart.

When implementing the proposed irrigation system, OSPF (Open Shortest Path First) is the fundamental routing protocol to use. According to Vetter et al. [54], this protocol uses the SPF algorithm, which is solely based on bandwidth, for routing. In this work, a fuzzy system is used to improve the OSPF protocol's routing process. Based on a set of standard parameters, the network topology specification is taken into consideration as input in this case.

The target network is a WSN network that has a number of data-sending sensor nodes. The OSPF protocol is initially based on the WSN. Sending a "hello" message and setting up a neighborhood table do this. Subsequently, a Link-State Advertisement (LSA) message is sent between the sensor nodes to ascertain their communication state, and the network neighborhood table is generated accordingly [20]. After receiving the LSA message, every node updates its neighborhood database and notifies the other nodes in its vicinity with another LSA message. This definition of neighborhood is based on a threshold distance. For every node, a routing table is made in the next stage. To do this, the SPF method is developed for each node using a fuzzy approach. Based on LSA messages, the OSPF protocol alternately updates the neighborhood table. But only two situations result in the LSA being sent: 1) Modifications to the link status (e.g., cutting off a node's energy); and 2) A time interval (e.g., every second). As a result, each node updates its neighborhood table whenever something changes and sends an LSA to all of its neighbors to let them know about it.

5.1. Developing a routing table using a fuzzy method

In the proposed routing scheme, the source node is first thought of as the node on the current path ($node_c$). After that, every possible node is considered to determine the next $node_c$. That's mean, $andid(node_c) = \{node_1, node_2, \ldots, node_{z1}\}$. It shows that there are $z1$ potential candidates for the current $node_c$. Here, nodes that are close by are thought of as potential candidates. Following this, we compute the effect of selecting each node from the list of potential nodes using a law-based fuzzy system. The following step is to choose one of the candidate nodes to serve as the path's next node. This choice is made using a combination of the influence coefficient and the roulette wheel technique. If $node_1$ is chosen, it will be treated as the current node, so $node_c$ will be the same as $node_1$. Each time a node is chosen as a destination, this procedure is carried out for that node. Fig. 7 shows the proposed structure of the fuzzy system [20].

The impact of each candidate node is determined by a fuzzy system that takes into account the following parameters: "bandwidth of the link between the current node and the candidate node," "distance of the candidate node from the SIU," "residual energy of the candidate node," and "distance of the candidate node from the current node." Here, energy (*ER*), distance (*DS*), and bandwidth (*BW*) are the input parameters. The average sound is defined as the product of the candidate node's distance from the SIU and the distance from the current node. After being normalized to the maximum value, these parameters are transformed into a fuzzy set using the trapezoidal algorithm, which has three modes: low, middle, and high. The examined trapezoidal fuzzy set is illustrated in Fig. 8 [20]. The influence coefficient, which is approximated by the trapezoidal fuzzy set, is also the output of the fuzzy system.

An expert-created database of fuzzy rules defines the outcome. The multiplier-field operator is used to determine the membership degree of each input pattern [20]. Table 1 displays the fuzzy rules under consideration.

5.2. Neural network-based irrigation type selection

Most research employs a threshold to determine the appropriate watering method. If the temperature falls below -5 degrees, there is a chance of freezing, prompting the need for irrigation. Yet, the variables being analyzed frequently encompass ambient temperature, humidity, and soil-water content, which do not offer a straightforward correlation for decision-making. This research aims to utilize a neural network model in place of a threshold to make optimal decisions in the present by considering prior circumstances. A neural network is being trained to select the optimal watering method using data collected by the IoT. The neural network is trained using a sequence of real input-output pairs provided by an expert. The system takes into account inputs such as rainfall, soil moisture, crop water requirement, ambient humidity,

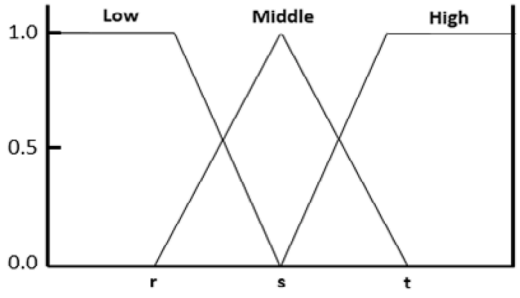


Fig. 8. Fuzzification to create fuzzy system input parameters

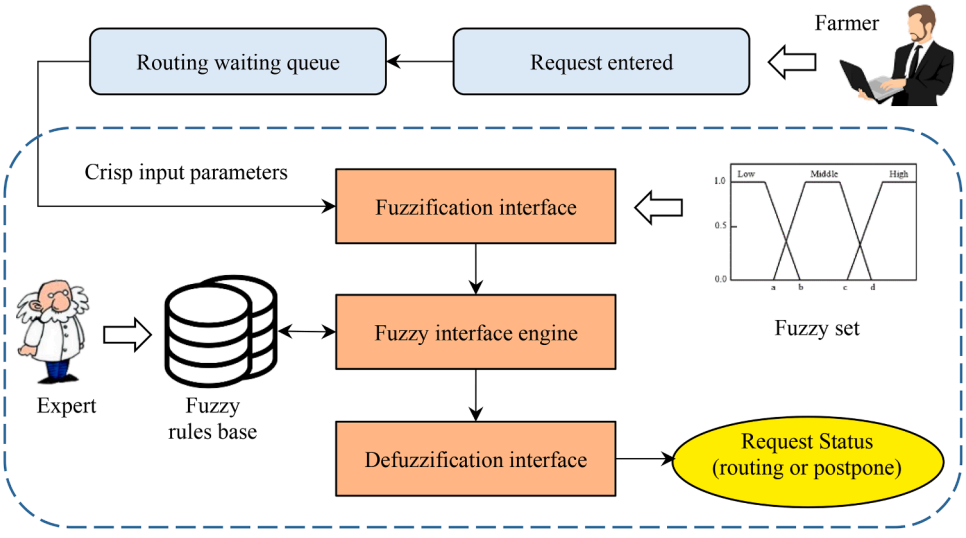


Fig. 7. The framework of the proposed fuzzy filtering method

Table 1
. Database containing fuzzy rules utilized in a routing algorithm

Law number	System input			System output
	Bandwidth	Distance	Energy	Impact coefficient
1	Low v Mid	Low	Low	Low
2	High	Low	Low	Mid
3	Low v Mid v High	High v Mid	Low	Low
4	Low	Low	Mid v High	Mid
5	Mid v High	Low	Mid	High
6	Low v Mid	Mid	Mid	Mid
7	Low v Mid	High	Mid v High	Low
8	High	High	Mid	Mid
9	Mid v High	Low	High	High
10	Low v Mid	Mid	High	Mid
11	High	Mid v High	High v Mid	High
12	Mid	High	High	Mid

ambient temperature, crop growth rate, evaporation rate, and crop planting time. The system's output consists of many types of irrigation, such as high-pressure drip irrigation, high-pressure sprinkler irrigation, low-pressure sprinkler irrigation, low-pressure drip irrigation, high-pressure surface irrigation, and low-pressure surface irrigation.

This research utilizes a MLP neural network with three layers: input, hidden, and output. The input features match the parameters obtained from the sensors, and the number of outputs corresponds to the specified forms of irrigation. The neural network has one hidden layer with four neurons. There are 1000 learning courses, and the learning process involves using the declining gradient method. Each node's output is determined by computing the weighted sum of its input values and applying the sigmoid function. The Mean Squared Error (MSE) is used to estimate and quantify the accuracy of the output by calculating the squared differences between the predicted values and the actual target values from the dataset. It serves as a key performance metric for assessing the deviation of the predicted outputs from the ground truth. An example of the MLP architecture employed in this study is illustrated in Fig. 9, which showcases a 3–4–1 configuration [20]. This configuration comprises three input nodes for receiving data, four nodes in a single hidden layer for intermediate processing, and one output node for generating the final prediction. This structure is designed to balance complexity and computational efficiency while effectively capturing the underlying patterns in the data.

5.3. Security analysis

The principal objective of the credential scheme is to consistently uphold user privacy by enabling individuals to obscure identifiable personal attributes in network interactions. The dissemination of information to unauthorized individuals to gain access to services is referred to as credential lending, sharing, or transfer [55,56]. This proposed protocol adheres to the non-transferability of credential attributes. The examined attributes (A) include A1 (Circumvention depends on), A2 (Circumvention by), A3 (Universality depends on), A4 (Credential cloning), A5 (Unintended sharing), and A6 (VANET system value). Table 2 illustrates the functional relationships among Attributes, Non-Transferability, and Transferability.

The formal security analysis of the proposed protocol indicates that V for VANET is conducted using the widely-accepted ROR (real-or-random) model. The ROR includes a mechanism to simulate a genuine attack by an adversary (A), so capturing the adversary's capabilities in an actual attack. Table 3 contains the descriptions of the various symbols for queries and notations utilized in the semantic security proof. The opponent A engages as an active player, either $P_i d_i$ or AS, at the t^{th} instance with V. We have evaluated all potential inquiries to substantiate formal security issues.

The advantage function of an adversary A in undermining the semantic security of the proposed method V by accurately predicting the

Table 2
. Comparative analysis of credential attributes regarding transferability and non-transferability.

A	Non-Transferability	Transferability
A1	Complete confidentiality	Open access control
A2	Independent	Exclusive partners
A3	Confidentiality across all scenarios	Environmental confidentiality
A4	More challenging	Less challenging
A5	Unattainable	Very likely
A6	Enhanced worth	Minimal improvement

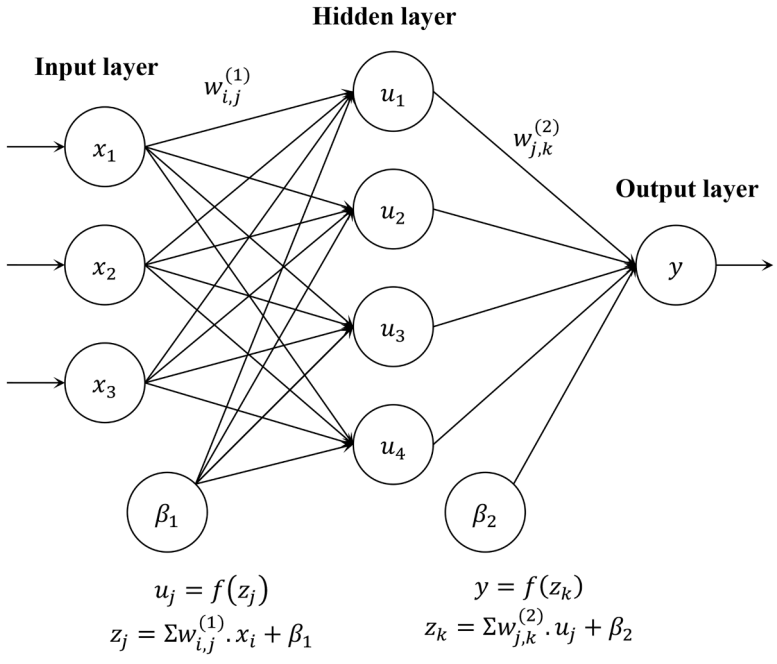


Fig. 9. An illustration of the architecture of a MLP neural network

Table 3
. Diverse ROR inquiries with corresponding descriptions.

Query	
Execute($P_i d_i$, *S*)	This enables $\mathscr{A}$ to receive messages passed among $P_i d_i$ and *AS* during the actual implementation of the procedure.
Send(*V*, *p*)	It enables $\mathscr{A}$ to transmit a plea message *p* to 1> to V^t. In accordance with protocol, $\mathscr{T}^t$ responds to *A*.
Reveal($\mathscr{T}^t$)	It facilitates the disclosure of the shared key K_{shd_i} produced between $P_i d_i$ and *AS*.
Corrupt($P_i d_i$, *a*)	The accuracy of '*a*' facilitates the retrieval of the user's credentials stored in *SC* to reference adversary $\mathscr{A}$.
Test($\mathscr{T}^t$)	Through this inquiry, $\mathscr{A}$ submits a proposal to $\mathscr{T}^t$ for the current shared session key K_{shd_i}, and $\mathscr{T}^t$ responds probabilistically as a consequence of an unbiased coin flip *b*.

bit b' is denoted as $Adv_V^{VANET} = |2\Pr[b = b'] - 1|$. A biometrics-based authentication mechanism combined with a password is considered semantically secure if the advantage function Adv_V^{VANET} is marginally higher than $\max\left\{q_s\left(\frac{1}{2^{|\mathscr{D}|}}, \frac{1}{2^{l_b}}, \varepsilon_{bm}\right)\right\}$, where q_s, $|\mathscr{D}|$, l_b and ε_{bm} retain their original definitions. Assuming the adversary *A* operates with the complexity of a polynomial algorithm $t_{\mathscr{A}}$. The adversary performs *H, S*, and *E* with maximal time complexities q_H, q_s and q_e, respectively, to compromise the established semantic security of the proposed protocol *V*. According to the definition, we have:

$$Adv_V^{VANET} = \frac{q_H^2}{2^{l_H}} + \frac{(q_s + q_e)^2}{2^{l_r}} + \max\left\{q_s\left(\frac{1}{2^{|\mathscr{D}|}}, \frac{1}{2^{l_b}}, \varepsilon_{bm}\right)\right\} \tag{1}$$

where q_s, q_H, l_H, l_r, $|\mathscr{D}|$, $l_b$and ε_{bm} carry the same meaning.

5.4. Objectives

The objectives encompass several critical factors, including latency cost, which refers to the delay experienced during data transmission and processing; service cost, which accounts for the expenses incurred in delivering the required services; throughput, representing the volume of data successfully processed within a given timeframe; fog utilization, which measures the efficiency of resource usage in fog computing environments; and response time, denoting the time taken to respond to a user's request or task. These factors collectively ensure the system's performance, cost-effectiveness, and responsiveness.

Latency Cost (LC): In the context of VANETs, latency cost encompasses various components, including queuing latency (the time spent waiting in a queue), communication link latency, and processing latency. The orchestrator node, tasked with managing IoT services within the fog domain, contributes to communication link latency through factors such as $L_O^{f^j}$, L_O^{IoT}, L_O^{MM} and L_O^{NN}. However, in many studies, these specific latencies are often overlooked due to their negligible impact on overall system performance. Consequently, the latency cost for each IoT service is primarily determined as the sum of queuing latency and processing latency. Let $L_{s^l}^Q$ represent the queuing latency for a task s^l. Additionally, $L_{s^l}^{f^j}$, $L_{s^l}^O$, $L_{s^l}^{MM}$, and $L_{s^l}^{NN}$ denote the processing latency for s^l on a fog node f^j, the orchestrator node, the cloud, and the fog domain, respectively. Here, $L_{s^l}^{MM}$, which corresponds to executing s^l in the cloud, is primarily influenced by the distance to the cloud due to its abundant computational resources. On the other hand, $L_{s^l}^{NN}$ incorporates communication link latency because s^l must be transferred across fog domains. In general, processing latency is determined by the specific entity tasked with providing resources for s^l. According to prior studies, the processing latency values for $L_{s^l}^{f^j}$ and $L_{s^l}^O$ are equivalent and are calculated using Eq. (2) [57,58]. This comprehensive calculation framework ensures an accurate assessment of latency cost in VANET-enabled fog computing systems.

$$L_{s^l}^{f^j} = L_{s^l}^O = \frac{Sz_{s^l}.\mathbb{S}_{s^l}}{\mathscr{F}} \tag{2}$$

where $\mathbb{S}_{s^l}$ denotes the number of cycles necessary to execute s^l, Sz_{s^l} represents the bit count of s^l, and $\mathscr{F}$ indicates the frequency of the node hosting s^l.

The overall latency cost for s^l is computed according to Eq. (3). The orchestrator node executes the placement, and L_τ^O, representing the placement delay during the time period τ, is incorporated into the total latency [57,58].

$$LC(s^l) = L_\tau^O + \left[x_{s^l}^{f^j}.L_{s^l}^{f^j} + x_{s^l}^O.L_{s^l}^O + x_{s^l}^{MM}.L_{s^l}^{MM} + x_{s^l}^{NN}.L_{s^l}^{NN}\right] \tag{3}$$

where $x_{s^l}^{f^j}$, $x_{s^l}^O$, $x_{s^l}^{MM}$, and $x_{s^l}^{NN}$ represents binary decision variables for f^j, the orchestrator node, cloud, and fog, respectively. The value of each decision variable for s_l is ascertained according to Eq. (4).

$$x_{s^l}^{dv} = \begin{cases} 1 & If\ s^l\ is\ placed\ on\ dv \\ 0 & Otherwise \end{cases} \tag{4}$$

where *dv* denotes a fog entity upon which s^l can be implemented.

Service Cost (SC): The expense associated with implementing an IoT service encompasses both communication and compute costs, which fluctuate depending on the service's deployment location [59]. The communication cost pertains to the execution time of the IoT service, as indicated in Eq. (5). The computational expense correlates with the financial cost of implementing the IoT service, as illustrated in Eq. (6).

$$cm_{dv} = C_{dv}.\frac{cv_{\alpha,\beta}}{B} \tag{5}$$

$$cp_{dv} = P_{dv}(t_\beta - t_\alpha) \tag{6}$$

where cm_{dv} and cp_{dv} denote the costs of communication and computation on device dv, respectively. C_{dv} and P_{dv} represent the costs associated with the communication and compute units on device *dv*, respectively. $[t_\alpha, t_\beta]$ denotes the temporal interval for the execution of IoT services. $cv_{\alpha,\beta}$ denotes the data size inside the interval $[t_\alpha, t_\beta]$. Ultimately, B represents the output bandwidth. As per references [57–59], *B* is established at 20 Mbps and C_{dv} is set at 0.1.

The overall cost for performing s^l can be determined by incorporating cm_{dv} and cp_{dv}, as outlined in Eq. (7). The binary decision variables are determined by the entity allocated to s^l.

$$SC(s^l) = x_{s^l}^{f^j}\left(cp_{f^j} + cm_{f^j}\right) + x_{s^l}^O(cp_O + cm_O) + x_{s^l}^{MM}(cp_{MM} + cm_{MM}) + x_{s^l}^{NN}(cp_{NN} + cm_{NN}) \tag{7}$$

Throughput (TP): Throughput is a metric used to assess the deployment quality of an IoT application or service. Inadequately defining the QoS requirements for an IoT service results in deployments characterized by elevated costs and diminished throughput. The throughput for the fog domain is computed using the service exit rate and time differential, measured in Bytes/s [58]. Eq. (8) computes the throughput rate subsequent to the implementation of s^l.

$$TP(s_l) = \frac{DR_{dv}^{s^l}}{\max(PT_{s^l}, 1)} \tag{8}$$

where PT_{s^l} denotes the temporal disparity for s^l and $DR_{dv}^{s^l}$ represents the service egress rate that applies selectivity to the influx rate.

Fog utilization (UF): Increased consumption of fog resources by nodes enhances ecosystem functioning. Consequently, it is imperative to optimize fog consumption using fog nodes [57]. Eq. (9) illustrates the fog use subsequent to the deployment of s^l.

$$UF(s_l) = \frac{\sum_{f^j \in D} Adap_{f_j}^{s^l}.uf_{f_j}}{P(s^l)} \tag{9}$$

where uf_{fj} denotes the quantity of fog employed by f_j. $P(s^l)$ denotes the priority assigned to the execution of s^l. Additionally, $Adap_{f_j}^{s^l}$ indicates the compatibility of s^l with f_j, as given by Equation (10).

$$Adap_{f_j}^{s^l} = Adap_{f_j}^{s^l}(M).Adap_{f_j}^{s^l}(P).Adap_{f_j}^{s^l}(S).Adap_{f_j}^{s^l}(L) \tag{10}$$

where the symbols *P, M, S,* and *L* denote processor, memory, storage, and latency, respectively. Ultimate compatibility is attained through the integration of processor, memory, storage, and service latency. These compatibilities, as delineated by Eqs. (11–14), are determined according to [57,58].

$$Adap_{f_j}^{s_l}(P) = \begin{cases} 1 & P_{fj}(\Delta t) \geq P_{s^l} \\ 0 & Otherwise \end{cases} \tag{11}$$

$$Adap_{f_j}^{s_l}(M) = \begin{cases} 1 & M_{fj}(\Delta t) \geq M_{s^l} \\ 0 & Otherwise \end{cases} \tag{12}$$

$$Adap_{f_j}^{s_l}(S) = \begin{cases} 1 & S_{fj}(\Delta t) \geq S_{s^l} \\ 0 & Otherwise \end{cases} \tag{13}$$

$$Adap_{f_j}^{s_l}(L) = \begin{cases} 1 & \widehat{LC}(s^l) \leq D_{s^l} \\ 0 & Otherwise \end{cases} \tag{14}$$

where Δt denotes a particular time interval within the fog domain, and $\widehat{LC}(s^l)$ represents the mean latency and deployment cost of s^l across all nodes in the existing fog domain.

Response Time (RT): Executing an IoT service necessitates four stages: transmitting the service, deploying the service, executing the service, and delivering the service outcome. Consequently, the response time for s^l can be determined using Eq. (15).

$$RT(s^l) = WT_{s^l} + MT_{s^l} + DT_{s^l} \tag{15}$$

where WT_{s^l} denotes the service deployment duration, predicted based on the resource allocation time necessary for s^l. MT_{s^l} denotes the runtime linked to s^l, quantified by the use duration of fog resources by s^l. Furthermore, DT_{s^l} denotes the communication duration, encompassing both the transmission time of DT_{s^l} and the response time for the result of DT_{s^l}.

6. Simulation

This section evaluates the performance of the proposed method in comparison with similar methods. We have performed extensive simulations that confirm the performance results of the proposed method.

6.1. Experimental setup

The simulation is conducted using MATLAB 2019a software on an Asus laptop equipped with an Intel Core i7 CPU running at a frequency of 3.0 GHz and 16GB of RAM. The IoT WSN topology is used for the simulation. The experiments set specific values for the parameters of the proposed approach. The simulation consists of 5000 cycles, with LSA sending occurring every 5 cycles. The agricultural land measures 100 × 100 meters and hosts 100 sensor nodes randomly distributed. Each node starts with an energy of 0.2 joules. Data packets are 4 KB in size, Hello packets are 25 bits, the SIU is located at 50 × 50 meters, and there are 12 fuzzy rules.

6.2. Result in irrigation system

The energy consumption model is utilized for transmitting and receiving data [60,61]. In this approach, nodes transmit packets at maximum power level if the distance between them exceeds the threshold distance; else, packets are sent at an average power level based on the distance. The energy consumption for transmission nodes (E_{tx}) and receiving nodes (E_{rx}) is quantified using Eqs. (16) and (17) in this model.

$$E_{tx}(d) = \begin{cases} E_{elec} \times l + \varepsilon_{fs} \times l \times d^2, & d < d_0 \\ E_{elec} \times l + \varepsilon_{mp} \times l \times d^4, & d \geq d_0 \end{cases} \tag{16}$$

$$E_{rx} = E_{elec} \times l \tag{17}$$

In these interactions, the energy needed to send or receive is one bit [62,63]. The package size and the distance between the sender and receiving nodes. Amplifier energy is used to increase the strength of the signal. Typically, the threshold is defined as Eq. (18).

$$d_0 = \sqrt{\varepsilon_{fs}/\varepsilon_{mp}} \tag{18}$$

A neural network has been trained using data collected by the IoT to identify the optimal irrigation method. The neural network configuration details are presented in Table 4.

In-depth tests have been conducted in this section to assess the proposed algorithm performance. First, the research on convergence of neural networks with 100 periods is introduced. Fig. 10 displays the neural network learning outcomes. The error is expressed as MSE. During the validation procedure, period 85 had the best performance, with an MSE of 0.0037699.

Fig. 11 reports the network's remaining energy from separate nodes after routing cycles are finished in another experiment. The results indicate that most nodes have zero or nearly zero energy at the end of the routing cycle, given their initial energy of 0.2 J. Additionally, only 6 of the 100 network nodes have energies higher than 0.1 J, and the nodes' residual energy variance is approximately 0.03. These findings show that the network's energy usage is distributed appropriately.

The network's residual energy in the proposed technique is then compared to the routing cycles against the WSN-IoT algorithm and the LEACH (Low Energy Adaptive Clustering Hierarchy) protocol. The network's residual energy is equal to the residual energy of all nodes at each routing cycle. The comparison's outcomes are shown in Fig. 12. The network energy in the first simulation round is 20 J. In this case, a declining trend in network energy is seen for all approaches during routing cycles. Compared to previous methods, the proposed method has a lower rate of acceleration in energy reduction. The proposed strategy is superior since it distributes energy use properly and uses energy-aware routing techniques.

In a different experiment, the number of active nodes and the network lifetime were compared using various routing cycle algorithms. Fig. 13 displays the comparison's findings. The first node to die in the routing round according to the proposed technique is 2109. For the LEACH protocol, this threshold is 1057, while for the WSN-IoT

Table 4
. Neural network design specifics for irrigation schedule determination.

Parameters	Values
Inputs	There are seven inputs: ambient temperature, soil moisture, crop growth rate, ambient humidity, crop water need, crop planting time, evaporation rate, and rainfall.
Hidden layer configuration	A hidden layer with 4 neurons
Number of learning epochs	1000 epoch
Learning algorithm	Gradient descent
Output	There are six categories of irrigation outputs: high-pressure surface irrigation, low-pressure sprinkler irrigation, high-pressure sprinkler irrigation, low-pressure drip irrigation, high-pressure drip irrigation, and low-pressure surface irrigation.
Number of training records	500 records
Record-making approach	For every feature, produce a uniform distribution of random values between 0 and 1.

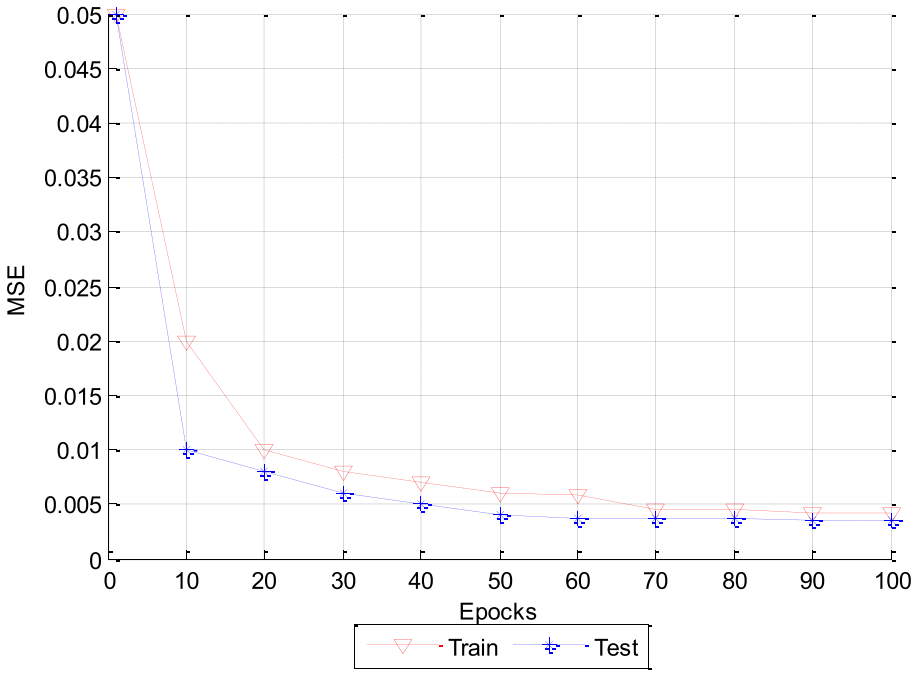


Fig. 10. Convergence outcomes for neural networks

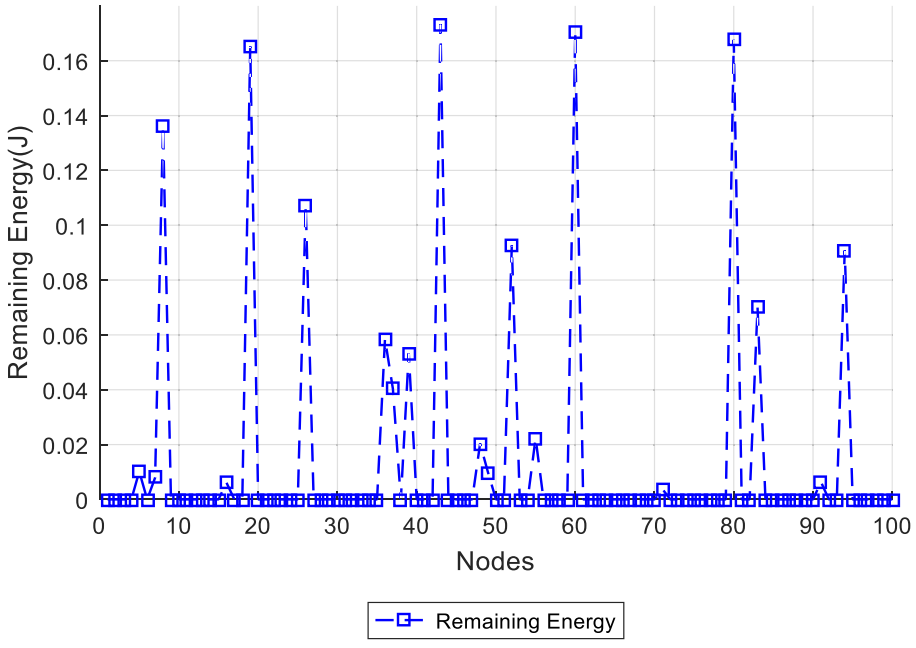


Fig. 11. Network energy residual depending on each node

algorithm, it is 1625. Better network life is thus provided by the proposed approach. Furthermore, the proposed approach with 22 active nodes outperforms the LEACH protocol with 2 and the WSN-IoT algorithm with 4 active nodes after 5000 routing cycles.

After 5000 routing rounds are completed, Table 5 presents a comparison of several approaches based on the numerical results of various criteria. Overall, compared to LEACH protocol and WSN-IoT algorithm, the proposed approach based on IoT architecture and fuzzy based energy-aware routing algorithm has shown better results.

6.3. *Results of authentication in VANET*

Table 6 illustrates the complexity of signature verification for both individual users and groups of users. Fig. 14 illustrates the functional availability index profile of LEACH, WSN-IoT, and the suggested technique. The Functional-Event-Availability (FEA) index rises proportionately with the total number of events. The FEA index measures a system's ability to reliably perform its intended functions during specific operational events. It evaluates key metrics such as response time, success rate, and resource utilization to ensure functionality under predefined conditions. In VANETs, for instance, the FEA index assesses the reliability of secure authentication during vehicle communication in

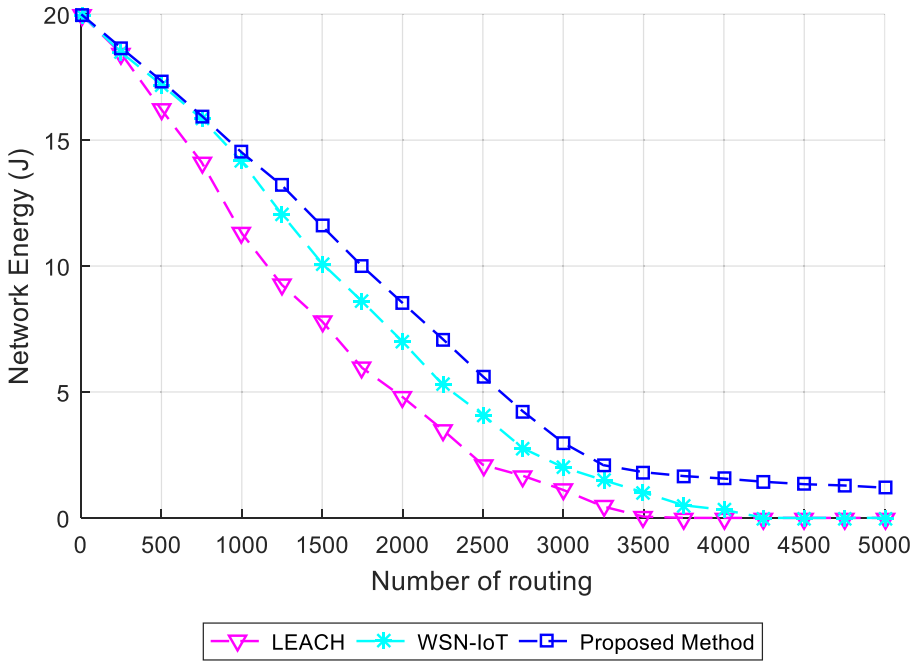


Fig. 12. Comparison of various approaches for network residual energy

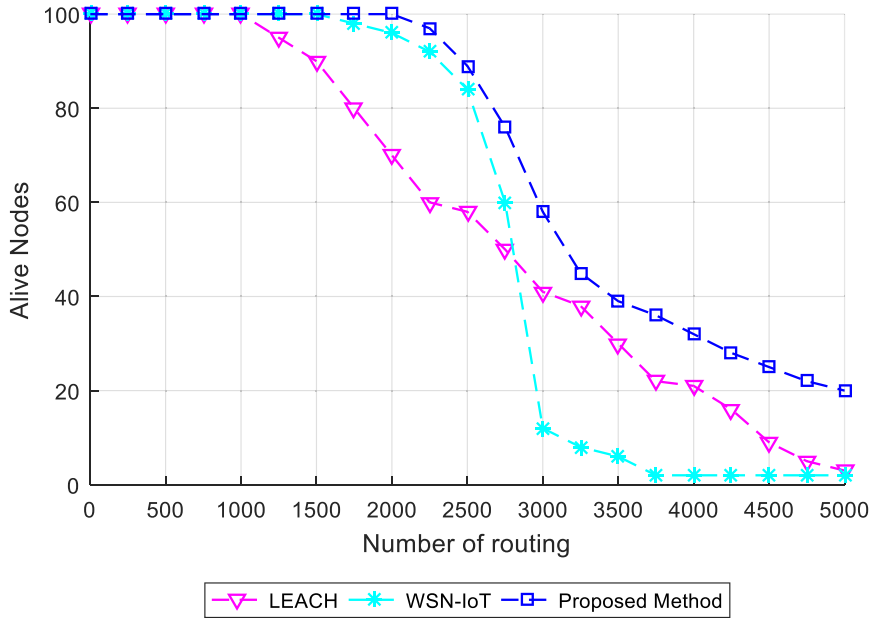


Fig. 13. Comparison of several approaches' live network node counts

Table 5
. Evaluation outcomes of comparable techniques using various criteria.

Methods	Network life	Number of packages sent	Residual energy variance	Average route length
LEACH	1057	2446	0.012	3.4
WSN-IoT	1625	2801	0.005	3.1
Proposed Method	2109	3207	0.003	2.9

Table 6
. Comparative analysis of time complexity for signature verification with respect to individual and group.

Methods	Single user verification	Group user verification
LEACHy	$O(N)$	$O(\log N)$
WSN-IoT	$O(N^2)$	$O(LogN^2)$
Proposed Method	$O(N\log N)$	$O(LogN)$

dynamic environments, considering factors like computational overhead and real-time performance. Similarly, in IoT-based applications, it ensures that devices can monitor and respond to triggers effectively, even in resource-constrained settings. The FEA index is vital for analyzing availability and reliability in critical systems such as smart irrigation, disaster management, and secure vehicular networks.

Figs. 15 and 16 illustrate the E2DS (End-to-Destination-Source delay)

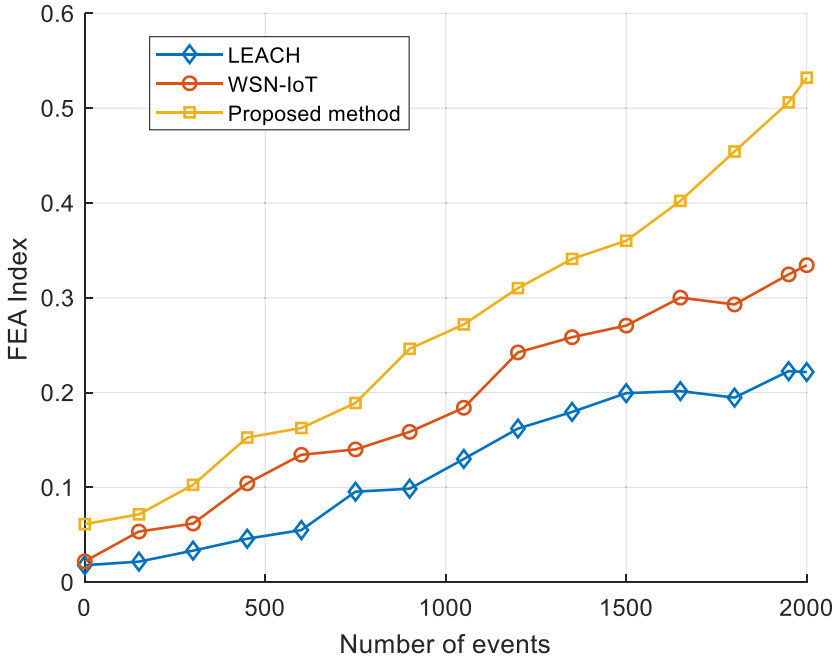


Fig. 14. FEA index of LEACH, WSN-IoT, and proposed method

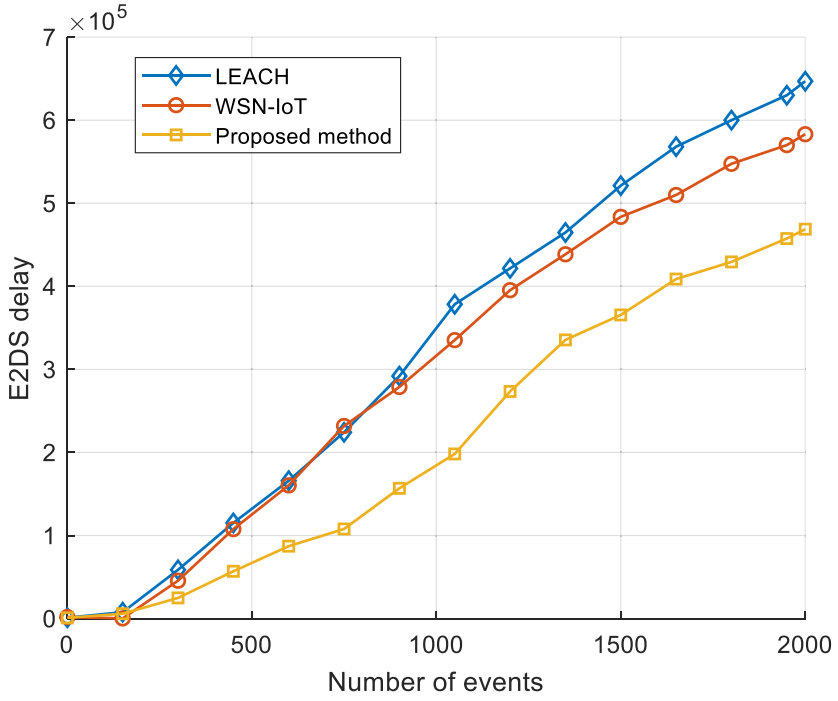


Fig. 15. E2DS delay of LEACH, WSN-IoT, and proposed method based on the individual verification

curve of individual signature verification and group verification, respectively. The suggested method demonstrates reduced time expenditure for signature verification in both individual and group contexts. The E2DS delay refers to the total time taken for a data packet to travel from the source to the destination and back to the source in a network. This delay consists of three main components: the forward delay, which is the time for the data to reach the destination; the processing delay at the destination, including time spent on verification or decision-making; and the return delay, which is the time taken for the acknowledgment or response to return to the source. The E2DS delay is an important metric for evaluating network performance, particularly in latency-sensitive applications like VANETs, where it helps measure the efficiency of communication protocols, including routing and security mechanisms.

7. Conclusions

There is not enough food in the world to feed everyone as the population grows. Despite the abundance of fertile land, conventional agriculture may be contributing to the current fall in food production. As a result, intelligent agriculture and the integration of emerging technology with agriculture are essential. Furthermore, the majority of people rely on agriculture for their livelihood, and it plays a significant

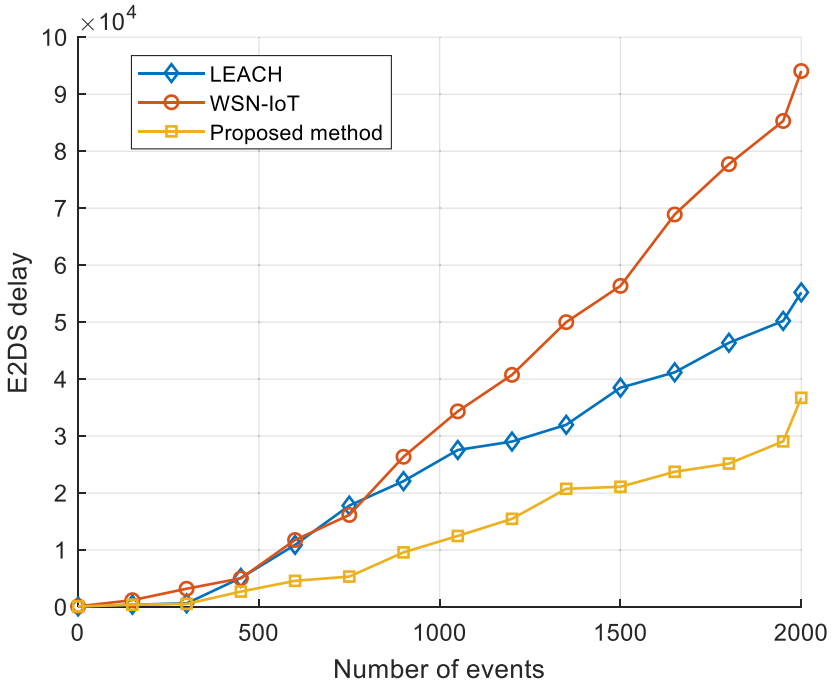


Fig. 16. E2DS delay of LEACH, WSN-IoT, and proposed method based on the group verification

part in the global economy. Because of this, water is a valuable resource that needs to be preserved by utilizing cutting-edge technologies. Smart farming is now possible thanks to the expansion of the IoT capabilities. This study presents the design of an automated intelligent irrigation system at a reasonable cost. In this case, the IoT is used to create devices with capabilities like remote data monitoring, neural network-based decision making for intelligent support, scheduling irrigation, and manager mode for user engagement. These devices also automatically connect with each other within the system. Input parameters are computed using a fuzzy logic controller, which also generates motor status outputs. The proposed system has shown to be capable, affordable, and movable, making it appropriate for usage in farms and greenhouses. This leads us to continue developing the algorithm by improving routing efficiency in terms of dependability to guarantee packet preservation and by continuously adding hops with varying network node strengths to guarantee access to the destination node, particularly in WSNs for the oil and gas industry. In order to facilitate and expedite data transfer between the sensor nodes and the node processing unit, it is also advised for future work to employ an IoT-enabled microcontroller. Another recommendation of this research is to use and compare the OSPF protocol's performance with other novel protocols, including the Enhanced Interior Gateway Routing Protocol (EIGRP).

CRediT authorship contribution statement

Huijing Zhang: Methodology, Resources, Validation, Writing – original draft, Writing – review & editing. **Minbo Li:** Writing – review & editing, Methodology, Data curation, Conceptualization.

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

Funding

No funding was received for this work.

Ethics approval

The paper reflects the authors' own research and analysis in a truthful and complete manner.

Consent to publish

Informed consent was obtained from all participants.

Data availability

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

References

[1] Rajkumar MN, Abinaya S, Kumar VV. Intelligent irrigation system—An IOT based approach. In: 2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT). IEEE; 2017. p. 1–5.
[2] Xiao Z, Fang H, Jiang H, Bai J, Havyarimana V, Chen H, Jiao L. Understanding private car aggregation effect via spatio-temporal analysis of trajectory data. IEEE Trans Cybern 2021;53(4):2346–57.
[3] Xiao Z, Shu J, Jiang H, Min G, Chen H, Han Z. Overcoming occlusions: Perception task-oriented information sharing in connected and autonomous vehicles. IEEE Netw. 2023;37(4):224–9.
[4] Ding C, Zhu L, Shen L, Li Z, Li Y, Liang Q. The Intelligent Traffic Flow Control System Based on 6G and Optimized Genetic Algorithm. IEEE trans Intell Transp Syst 2024. https://doi.org/10.1109/TITS.2024.3467269.
[5] Huang Y, Feng B, Cao Y, Guo Z, Zhang M, Zheng B. Collaborative on-demand dynamic deployment via deep reinforcement learning for IoV service in multi edge clouds. J Cloud Comput 2023;12(1):119.
[6] Yue W, Li J, Li C, Cheng N, Wu J. A Channel Knowledge Map-Aided Personalized Resource Allocation Strategy in Air-Ground Integrated Mobility. IEEE Trans Intell Transp Syst 2024;25(11):18734–47.
[7] Liu S, Niu B, Zong G, Zhao X, Xu N. Adaptive fixed-time hierarchical sliding mode control for switched under-actuated systems with dead-zone constraints via event-triggered strategy. Appl Math Comput 2022;435:127441.
[8] Liu Y, Fan Y, Zhao L, Mi B. A refinement and abstraction method of the SPZN formal model for intelligent networked vehicles systems. KSII Trans Internet Inf Syst 2024;18(1):64–88.

[9] Wei F, Niu B, Zong G, Zhao X. Adaptive neural self-triggered bipartite consensus control for nonlinear fractional-order multi-agent systems with actuator fault. Nonlinear Dyn 2024. https://doi.org/10.1007/s11071-024-10234-5.

[10] Zhu B, Liang H, Niu B, Wang H, Zhao N, Zhao X. Observer-based reinforcement learning for optimal fault-tolerant consensus control of nonlinear multi-agent systems via a dynamic event-triggered mechanism. Inf Sci 2025;689:121350.

[11] Yue S, Xu N, Zhang L, Zhao N. Observer-Based Event-Triggered Adaptive Fuzzy Hierarchical Sliding Mode Fault-Tolerant Control for Uncertain Under-Actuated Nonlinear Systems. Int. J. Fuzzy Syst. 2024. https://doi.org/10.1007/s40815-024-01834-9.

[12] Fu Y, Li C, Yu FR, Luan TH, Zhao P. An incentive mechanism of incorporating supervision game for federated learning in autonomous driving. IEEE Trans Intell Transp Syst 2023;24(12):14800–12.

[13] Sun G, Sheng L, Luo L, Yu H. Game theoretic approach for multipriority data transmission in 5G vehicular networks. IEEE Trans Intell Transp Syst 2022;23(12):24672–85.

[14] Wu X, Ding S, Wang H, Xu N, Zhao X, Wang W. Dual-channel event-triggered prescribed performance adaptive fuzzy time-varying formation tracking control for nonlinear multi-agent systems. Fuzzy Sets Syst 2025;498:109140.

[15] Li C, He A, Liu G, Wen Y, Chronopoulos AT, Giannakos A. RFL-APIA: a Comprehensive Framework for mitigating poisoning attacks and promoting model aggregation in IIoT Federated Learning. IEEE Trans Industr Inform 2024;20(11):12935–44.

[16] Hota L, Nayak BP, Kumar A, Ali GMN, Chong PHJ. An analysis on contemporary MAC layer protocols in vehicular networks: State-of-the-art and future directions. Future Internet 2021;13(11):287.

[17] Mohindru G, Mondal K, Banka H. Internet of Things and data analytics: A current review. Data Min Knowl Discov 2020;10(3):e1341.

[18] Ding Y, Zhang W, Zhou X, Liao Q, Luo Q, Ni LM. FraudTrip: Taxi fraudulent trip detection from corresponding trajectories. IEEE Internet Things J 2020;8(16):12505–17.

[19] Zhong Y, Chen L, Dan C, Rezaeipanah A. A systematic survey of data mining and big data analysis in internet of things. J Supercomput 2022;78(17):18405–53.

[20] Rezaeipanah, A. (2021). An IoT Fast and Low Cost Based Smart Irrigation Intelligent System Using a Fuzzy Energy-Aware Routing Approach. Preprint in Research Square. DOI: 10.21203/rs.3.rs-685815/v1.

[21] Mohindru G, Mondal K, Banka H. Internet of Things and data analytics: A current review. Data Min Knowl Discov 2020;10(3):e1341.

[22] Zhang H, Zou Q, Ju Y, Song C, Chen D. Distance-based support vector machine to predict DNA N6-methyladenine modification. Curr Bioinform 2022;17(5):473–82.

[23] Cai, J., Guo, D., & Wang, W. (2024). Adaptive fault-tolerant control of uncertain systems with unknown actuator failures and input delay. *Measurement and Control*, 00202940241289217. DOI: 10.1177/00202940241289217.

[24] Xue B, Li R, Cheng Z, Zhou X. High-Affinity Peptides for Target Protein Screened in Ultralarge Virtual Libraries. ACS Central Science; 2024. https://doi.org/10.1021/acscentsci.4c01385.

[25] Han A, Yang Q, Chen Y, Li J. Failure-distribution-dependent H∞ fuzzy fault-tolerant control for nonlinear multilateral teleoperation system with communication delays. Electronics (Basel) 2024;13(17):3454.

[26] Cao C, Wang J, Kwok D, Cui F, Zhang Z, Zhao D, Zou Q. webTWAS: a resource for disease candidate susceptibility genes identified by transcriptome-wide association study. Nucleic Acids Res 2022;50. D1D1123-D1130.

[27] Azam F, Yadav SK, Priyadarshi N, Padmanaban S, Bansal RC. A comprehensive review of authentication schemes in vehicular ad-hoc network, 9. IEEE access; 2021. p. 31309–21.

[28] Sun G, Zhang Y, Yu H, Du X, Guizani M. Intersection fog-based distributed routing for V2V communication in urban vehicular ad hoc networks. IEEE Trans Intell Transp Syst 2019;21(6):2409–26.

[29] Peng X, Song S, Zhang X, Dong M, Ota K. Task Offloading for IoAV under Extreme Weather Conditions Using Dynamic Price Driven Double Broad Reinforcement Learning. IEEE Internet Things J 2024;11(10):17021–33.

[30] Krishnan RS, Julie EG, Robinson YH, Raja S, Kumar R, Thong PH. Fuzzy logic based smart irrigation system using internet of things. J Clean Prod 2020;252:119902.

[31] Karar, M. E., Al-Rasheed, M. F., Al-Rasheed, A. F., & Reyad, O. (2020). IoT and neural network-based water pumping control system for smart irrigation. arXiv preprint ar*Xiv:2005.04158*.

[32] Tiglao NM, Alipio M, Balanay JV, Saldivar E, Tiston JL. Agrinex: A low-cost wireless mesh-based smart irrigation system. Measurement 2020;161:107874.

[33] Mousavi SK, Ghaffari A, Besharat S, Afshari H. Improving the security of internet of things using cryptographic algorithms: a case of smart irrigation systems. J Ambient Intell Humaniz Comput 2021;12(2):2033–51.

[34] Nawandar NK, Satpute VR. IoT based low cost and intelligent module for smart irrigation system. Comput Electron Agric 2019;162:979–90.

[35] Alomar B, Alazzam A. A smart irrigation system using IoT and fuzzy logic controller. 2018 Fifth HCT Information Technology Trends (ITT). IEEE; 2018. p. 175–9.

[36] Ni, W., Xu, Z., Zou, J., Wan, Z., & Zhao, X. (2021). [Retracted] Neural Network Optimal Routing Algorithm Based on Genetic Ant Colony in IPv6 Environment. *Comput Intell Neurosci*, 2021(1), 3115704.

[37] Mofaddel MA, Younes A, El-Sayed HH. Multi-objective multicast routing based on ant Colony optimization in mobile ad-hoc networks. J Statist Appl Prob Accept 2021;10(3):687–94.

[38] Hamed AY, Alkinani MH, Hassan MR. Ant colony optimization for multi-objective multicast routing. Comput Mater Contin 2020;63(3):1159–73.

[39] Anibrika BSK, Asante M, Hayfron-Acquah B, Gavua EK. An Energy-Efficient Routing Algorithm With Ant Colony Optimization Framework For Mobile Adhoc Networks: A Perormance Study. Int J Mod Trends Eng Res (IJMTER) 2020;7(5):64–83.

[40] Li QQ, Peng Y. A wireless mesh multipath routing protocol based on sorting ant colony algorithm. Procedia Comput Sci 2020;166:570–5.

[41] Zhang X, Shen X, Yu Z. A novel hybrid ant colony optimization for a multicast routing problem. Algorithms 2019;12(1):18.

[42] Pullagura JR, Rao DV. An Efficient Multicast Routing Protocol Based on Ant with Improved Pheromone Updating Rule in Manet. J: Int J Simul: Syst, Sci Technol IJSSST 2018;19(6):1–9.

[43] Kavitha V, Ganapathy K. Efficient and optimal routing using ant colony optimization mechanism for wireless sensor networks. Period Eng Nat Sci 2018;6(1):171–81.

[44] Batth KK, Singh R. Performance evaluation of ant colony optimization based routing algorithms for mobile ad hoc networks. Int J Adv Technol 2017;8(2):1–7.

[45] Reshadi M, Mirmahaleh SYH. Mapping and virtual neuron assignment algorithms for MAERI accelerator. J Supercomput 2022;78(1):238–57.

[46] Gopikrishnan S, Priakanth P, Awangga RM. HSIR: hybrid architecture for sensor identification and registration for IoT applications. J Supercomput 2019;75:5000–18.

[47] Chuang YT, Tsai JJ. cRedit-based and reputation retrieval system. J Supercomput 2021;77:10184–225.

[48] Sedaghat S, Jahangir AH. R2T-DSDN: reliable real-time distributed controller-based SDN. J Supercomput 2021;77:12420–57.

[49] Hashemi SY, Shams Aliee F. Dynamic and comprehensive trust model for IoT and its integration into RPL. J Supercomput 2019;75:3555–84.

[50] Sun G, Song L, Yu H, Chang V, Du X, Guizani M. V2V routing in a VANET based on the autoregressive integrated moving average model. IEEE Trans Veh Technol 2018;68(1):908–22.

[51] Wei F, Xu N, Huang S, Cao Y. Disturbance observer–based adaptive neural finite-time control for nonstrict-feedback nonlinear systems with input delay. Tran. Ins. Measu. Control 2024:01423312241261084. https://doi.org/10.1177/01423312241261084.

[52] Sun G, Zhang Y, Liao D, Yu H, Du X, Guizani M. Bus-trajectory-based street-centric routing for message delivery in urban vehicular ad hoc networks. IEEE Trans Veh Technol 2018;67(8):7550–63.

[53] Yao Y, Shu F, Cheng X, Liu H, Miao P, Wu L. Automotive radar optimization design in a spectrally crowded V2I communication environment. IEEE Trans Intell Transp Syst 2023;24(8):8253–63.

[54] Vetter B, Wang F, Wu SF. An experimental study of insider attacks for OSPF routing protocol. In: Proceedings 1997 International Conference on Network Protocols. IEEE; 1997. p. 293–300.

[55] Rong Y, Xu Z, Liu J, Liu H, Ding J, Liu X, Gao J. Du-bus: a realtime bus waiting time estimation system based on multi-source data. IEEE Trans Intell Transp Syst 2022;23(12):24524–39.

[56] Sun G, Wang Z, Su H, Yu H, Lei B, Guizani M. Profit maximization of independent task offloading in MEC-enabled 5G internet of vehicles. IEEE Trans Intell Transp Syst 2024;25(11):16449–61.

[57] Lin Y, Shi Y, Mohammadnezhad N. Optimized dynamic service placement for enhanced scheduling in fog-edge computing environments. Sustain Comput: Inf. Syst. 2024;44:101037.

[58] Guo C, Rezaeipanah A. Dynamic service function chains placement based on parallelized requests in edge computing environment. Trans Emerg Telecommun Technol 2024;35(1):e4905.

[59] Tang L, Zhang L, Xu N. Optimized backstepping-based finite-time containment control for nonlinear multi-agent systems with prescribed performance. Optim Control Appl Methods 2024;45(5):2364–82.

[60] Nawandar NK, Satpute VR. IoT based low cost and intelligent module for smart irrigation system. Comput Electron Agric 2019;162:979–90.

[61] Li T, Hui S, Zhang S, Wang H, Zhang Y, Hui P, Li Y. Mobile User Traffic Generation via Multi-Scale Hierarchical GAN. ACM Trans Knowl Discov Data 2024;18(8):1–19.

[62] Wang T, Zong G, Zhao X, Xu N. Data-driven-based sliding-mode dynamic event-triggered control of unknown nonlinear systems via reinforcement learning. Neurocomputing 2024;601:128176.

[63] Zhao H, Wang H, Chang X, Ahmad AM, Zhao X. Neural network-based adaptive critic control for saturated nonlinear systems with full state constraints via a novel event-triggered mechanism. Inf Sci 2024;675:120756.