Traffic-Aware Secured Cooperative Framework for IoT-Based Smart Monitoring in Precision Agriculture

Ibrahim Abunadi [1,2], Amjad Rehman [1,2], Khalid Haseeb [2,3], Lorena Parra [4,*] and Jaime Lloret [4]

1   College of Computer & Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia
2   Artificial Intelligence and Data Analytics (AIDA) Lab, CCIS Prince Sultan University, Riyadh 11586, Saudi Arabia
3   Department of Computer Science, Islamia College Peshawar, Peshawar 25000, Pakistan
4   Instituto de Investigación para la Gestión Integrada de Zonas Costeras, Universitat Politenica de Valencia, 46022 Valencia, Spain
*   Correspondence: loparbo@doctor.upv.es

Abstract: In recent decades, networked smart devices and cutting-edge technology have been exploited in many applications for the improvement of agriculture. The deployment of smart sensors and intelligent farming techniques supports real-time information gathering for the agriculture sector and decreases the burden on farmers. Many solutions have been presented to automate the agriculture system using IoT networks; however, the identification of redundant data traffic is one of the most significant research problems. Additionally, farmers do not obtain the information they need in time, such as data on water pressure and soil conditions. Thus, these solutions consequently reduce the production rates and increase costs for farmers. Moreover, controlling all agricultural operations in a controlled manner should also be considered in developing intelligent solutions. Therefore, this study proposes a framework for a system that combines fog computing with smart farming and effectively controls network traffic. Firstly, the proposed framework efficiently monitors redundant information and avoids the inefficient use of communication bandwidth. It also controls the number of re-transmissions in the case of malicious actions and efficiently utilizes the network's resources. Second, a trustworthy chain is built between agricultural sensors by utilizing the fog nodes to address security issues and increase reliability by preventing malicious communication. Through extensive simulation-based experiments, the proposed framework revealed an improved performance for energy efficiency, security, and network connectivity in comparison to other related works.

Keywords: agriculture system; Internet of Things; fog system; soil monitoring; green energy

1. Introduction

Today, the Internet and the Internet of Things (IoT) dominate nearly everyone's life. IoT is a paradigm that connects things, people, or networks and allows them to process and react precisely to any kind of physical or virtual communication [1–3]. IoT has applications in every industry, including healthcare, agriculture, and home controllers. It efficiently provides user-required services by utilizing Internet connectivity, sensors, and a variety of other technologies and protocols for collecting and analyzing data [4–6]. The Internet of Things helps companies to automate operations and improve service delivery using Internet technologies and cloud-based data transmission. For the various industries it is utilized in, IoT does not permit the adoption of universal software architecture; instead, it must be modified to meet user requirements [7–9]. Nowadays, smart agriculture is more important than ever because of the expanding global population and rising food demand. In this context, smart technologies have become a crucial route to cutting-edge agricultural practices [10–12]. There are many different applications, protocols, and prototypes in the field of agricultural land.

Furthermore, several IoT policies and standards have been developed in the agriculture sector in numerous nations and organizations worldwide. Due to the limited boundaries of IoT devices, sensors, and actuators, a detailed study of IoT in the context of agriculture is required to understand the present state of research [13–15]. Throughout history, the agricultural industry has played a significant role in human cultures worldwide. Machine learning is a subset of artificial intelligence widely explored for identifying malicious attacks. Such a technique also focuses on making the system smart so that additional overhead can be reduced on the IoT devices [16,17]. The organization and practices of modern agriculture are significantly impacted by the development of information and communication technologies (ICTs). Despite the benefits of this evolution, several security concerns have the potential to negatively affect the agriculture sector [18–20]. Since farmers could sustain a significant financial and personal loss in the event of a data breach, data integrity and confidentiality are critical security concerns within the agricultural sector [21–23]. In this work, the main contributions are as follows:

i. It provides a strategy to effectively manage IoT resources, identify the redundant nodes that are collecting the same data and forbid using them. Such a scheme is efficient in utilizing the resources of the network and prolonging the system life cycle.

ii. It develops intelligent methods using distributed machine learning to predict routing decisions for the selection of optimal forwarders with increasing data delivery and load balancing.

iii. Another aspect of the proposed framework is the usage of a fog system to establish a secure chain in the presence of unidentified and faulty nodes by establishing a reliable group of nodes.

iv. We verified the proposed framework with other work and the results demonstrate enhanced performance for various network parameters.

This paper is further organized as follows: the discussion for related studies is presented in Section 2. Section 3 presents the detail of the proposed framework. In Section 4, the simulation environment is briefly explained. Section 5 presents the results and discussion of the experiments. Lastly, the conclusion is in Section 6.

2. Related Work

The smart city emerged as a concept with the fast growth of dependable information and communication models and the combination of sensor technologies [24–26]. Modern fog computing technology develops intelligent networks combining IoT networks and cloud platforms. Fog computing is applied at the network edge, and they perform a significant number of tasks in terms of processing, storage, and communication. Networking devices such as routers, gateways, etc., make up fog computing. Compared to sensor nodes, these devices have more processing, transmission, and storage capabilities [27,28]. In an IoT system, fog nodes received data from sensors and are further forwarded for high-cost processing with the support of data centers. A smart city promotes sustainability by utilizing various sensors to collect information from the environment while providing improved social facilities, transportation, and accessibility. The gathered information can then be utilized to manage urban infrastructure, including water supply, food services, environmental monitoring, and traffic congestion [29–31]. Smart agriculture is based on the IoT with future generation networks and is expected to benefit from the intelligently developed methodologies. The objectives of this strategy are to preserve water resources, lessen soil erosion, and improve soil quality [32,33]. An effective and scalable protocol for the remote monitoring and decision making of farms in rural areas is named the CL-IoT protocol, and it was proposed to focus on the requirements for smart farming applications [34]. To decrease network communication delay, latency, and energy consumption, cross-layer-based clustering, and routing algorithms were developed. The cluster head (CH) selection method based on cross-layers has been proposed as a means of solving the energy efficiency issue for resource constraint networks. Each sensor's physical, medium

access control (MAC), and network layer parameters were analyzed and chosen as the optimal CH for effective data transfer. The algorithm with a novel probabilistic decision rule that was inspired by nature is proposed and serves as a fitness function to choose the best path for data transfer. To choose the cluster head, a hybrid artificial neural network and decision tree method were built with the cognitive radio [35]. The base station receives more packets and collects more data from the typical sensor nodes as the residual energy level rises. The on-demand routing protocol is designed to hold data in local storage for retransmission during link failure to achieve reliable data transfer. Performance metrics for the proposed technique include throughput, packet drop rate, packet delivery ratio, normalized overhead, and residual energy. The effectiveness of the proposed strategy was compared to a cluster-based data aggregation scheme. A novel intelligent routing protocol was proposed in [36] to increase the network lifetime and offer energy efficiency in the routing process, which is used to deliver data to the irrigation system. The protocol is known as terrain-based routing using fuzzy rules for precision agriculture and it uses fuzzy rules to provide a revolutionary intelligent energy-efficient routing scheme. The routing decisions were made using the fuzzy inference method described in this work. The equalized cluster head election routing protocol and region-based routing are two routing algorithms that were constructed and compared with the system. The experimental findings demonstrate that the suggested algorithm outperforms the other available algorithms. For an Agriculture Internet of Things (AG-IoT) network, the authors proposed a supervised machine learning multipath and administrative-distance-based load balancing algorithm [37]. The proposed algorithm, also known as AI-enabled multi-hop and administrative-distance-based opportunistic routing (MHADBOR), processes the collected data from source to destination using the network's multi-hop count and administrative-distance-based communication infrastructure. In addition, the authors frequently used CHs, microbase, and macrobase stations in the network to efficiently manage the deployed network traffic in a communication environment without congestion. In [38], the authors proposed an optimization of resource utilization in smart agriculture systems using IoT (SMAIoT) that can monitor several low-cost IoT sensor types. This framework gathers information from the soil, air, water, and insects and uses them to produce suitable decisions. The innovative aspect of the proposed framework is the scientific automation of functions such as irrigation, fertigation, pest detection, and pesticide spraying with efficient productivity. In [39], the authors provide an inter planetary file system (IPFS) storage for protecting agricultural sampling data based on the double-blockchain method for IoT networks. It stores the content of the sampled data using the IPFS network, and the proposed system can obtain the entire data segment using an oracle technique. Then, the authors developed a consortium blockchain, Agricultural Sample Data Chain (ASDC) by using Ethereum technology, and enhanced the Merkle Patricia Trie (MPT)-based accounts for all categories of sampled data. To retain a public record in the case of malicious attacks, block hashes are generated and uploaded on Ethereum's main chain after storing the data in ASDC blocks.

Limitations of the Existing Schemes

The summary of relevant studies shows that the IoT has grown significantly in creating and developing smart agriculture systems. It aids the farmers in monitoring soil conditions and water supply and increases productivity with the management of costs. It gathers the agricultural data and sends them to cloud databases to take the necessary actions accordingly. Numerous solutions have recently been proposed to deal with intelligent data monitoring with improved latency using machine learning techniques. However, many of the existing systems do not make it apparent how different connections are handled when there are redundant data. Moreover, efficient load balancing with the collaboration of mobile sensors is another significant research challenge [40,41]. Although many solutions have offered security for remote monitoring, this has been at the cost of computation and

complexity. As a result, we need a framework to handle the timely supply of monitoring data using some smart and intelligent behaviors.

3. Material and Methods

This section presents a detailed discussion of the proposed framework with the system model. Additionally, its algorithm and developed components are explained.

3.1. System Model and Background of the Proposed Framework

The system model consists of sensors, fog nodes, and the sink node. They are deployed at random positions and the sink node is mobile. The fog nodes are considered more intelligent and have sufficient resources as compared to ordinary sensors. The mobile sink has a direct association with cloud systems. Initially, IoT sensors are arranged in an undirected graph G with finite vertices N and edges E. Each node has enough memory to hold and maintain its neighbors' information. Similarly, neighbors in the fog system's proximity are arranged in the form list based on a particular score. Fog systems not only aggregate the agricultural data for transmission towards the sink node but also offer a security layer among sensors and cloud services. Each node has a prefixed transmission range, and in case the sink node is far away from it, the proposed framework adopts a multi-hop forwarding decision. We show the scenario for the proposed framework in Figure 1. A robust routing strategy was built with the identification of the redundant nodes, and agricultural sensors are installed in the field to sense the various situations. In the case of redundant nodes, such information is not permitted for transmission. Later, fog layers are made up of numerous fog nodes to initiate communication with sink nodes. Agriculture users may simply obtain the data from their smart devices with the support of cloud platforms. Our proposed framework also ensures data privacy and security in an unpredictable environment.
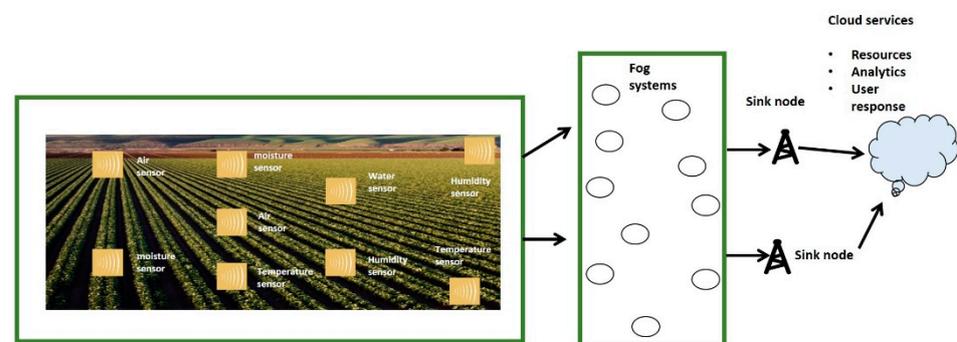

Figure 1. Scenario for fog-based IoT agricultural system.

Figure 2 depicts the block diagram of the proposed framework. It is comprised of three sub-blocks, i.e., network structure, machine learning system, and fog-based secured communication. Firstly, sensors, actuators, gateways, and other communication devices initialized themselves for sensing and forwarding agricultural data. The sensors continuously record environmental information, which is then sent to sink nodes via local coordinators or gateways. Second, a machine learning-based technique was created to reduce the communication overheads of the sensor nodes. Finally, the proposed system adopts the distributed regression function to assess the various attributes of the system and achieves efficient node management [42]. Moreover, the machine learning approach not only balances the load over the multiple routes, but the proposed framework can also identify the redundant nodes. Duplicate data are therefore prohibited from entering in proximity to fog nodes. In the end, a fog-based secured scheme is developed with the intelligence of fog nodes and cryptographic techniques. Fog nodes perform dual functionalities for communication with both the IoT system and cloud platform. This validates the authenticity of incoming packets, and accordingly, appropriate actions are taken. In the case of authorized nodes,

they are allowed to send the data towards the cloud system or the request packets are dropped by the fog nodes. The information is recorded in the table about false messages and non-authentic devices.
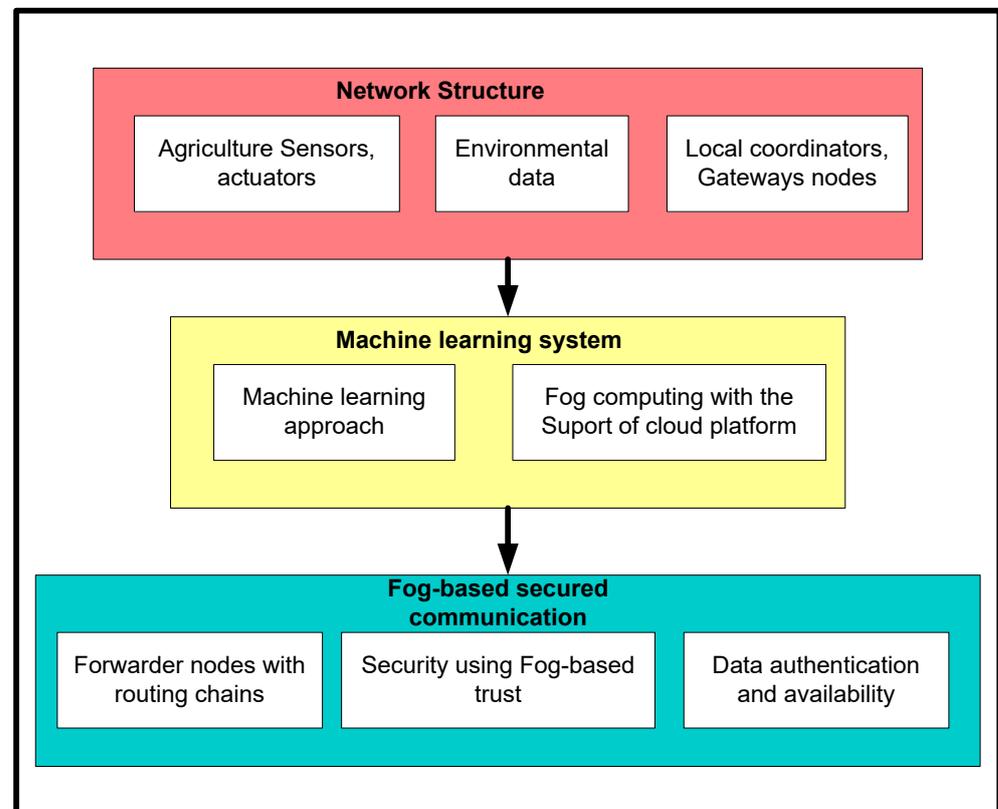

Figure 2. Block diagram of the proposed methodology.

3.2. Machine Learning-Based Distributed Regressional Analysis

Based on the undirected graph, the proposed framework identifies the initial and temporary routes $R(r_1, r_2, \ldots, r_n)$. The selected routes are based on the distance factor and each node maintains its neighbor table in a controlled manner. By exploring the neighbor table, each node formulates a route to the sink node for data transmission. To attain an efficient routing scheme with balances the load and bandwidth utilization, the proposed framework initiates the nodes management activity on the routes r_i. Let us consider that N_i has a data D_i to transmit to the sink node. Then, the proposed framework first identified the overlapping nodes that lay in the same transmission range. If any such nodes exist, then set their flag's value in the routing table. The flag value indicates the forwarding status of the nodes. Let us suppose that D_t is the distance threshold of the node NDs, and r is the predefined radius. To determine the overlapping nodes, the proposed framework exploits the search zone candidate nodes C_N based on the D_t and r, as given below

$$NDs\ (C_N,\ D_t) \leq r \tag{1}$$

After determining the candidate nodes, the proposed framework updates the routing table of source node *i* with the latest statistical values of neighbors. Table 1 describes the format of the routing table. It comprised node identity, transmission power, flag value, computing score, and distance. The node identity which is one byte long is unique. The next field is one byte long and contains the value of preset transmission power. The flag field is just a Boolean parameter to indicate whether the node can be silent or not, and it is one bit long. Finally, the scoring factor is two bytes long and depends on the captured information

about the nodes. In the end, the distance is 1 byte long and contains information about the space toward the fog system.

Table 1. Format of a routing table.

1 Byte	1 Byte	1 Bit	2 Bytes	1 Byte
Node identity, *id*	Transmission power t_x	Flag value, f_i	Score, sc_i	Distance to fog nodes, Df_i

The proposed framework only allows one node in the transmission radius for sensing and forwarding the agricultural data. To achieve this, it determines the node score sc_i with w_i weighted coefficient using distributed weighted regression function $X(i)$, and based on the maximum score, the flag value of the nodes *i* is set to either "*True*" or "*False*", as given below:

$$\begin{cases} if \ sc_i == max \\ \quad f_i \ is \ True \\ false, \ otherwise \end{cases} \tag{2}$$

$$X(i) = w_i \cdot sc_i \tag{3}$$

The sc_i value for node *i* is determined by exploring the residual energy e_i, packets load PL_i, distance Df_i, as given below:

$$sc_i = e_i + 1/PL_i + \frac{1}{Df_i} \tag{4}$$

where PL_i defines in terms of transmitted packets *N* at time interval *T*, as defined below.

$$PL_i = \frac{N}{T} \tag{5}$$

3.3. Fog Systems-Based Security Maintenance

In the proposed framework, the fog nodes performed the role of the intermediate system between the data originating network and cloud services. Firstly, it received all the data and stores it in memory for further analysis and processing. It then confirms the data authenticity to forward it towards the cloud system in the multi-hop discipline. Then, the aggregated data D_A is encrypted *En* using the secret key *k* of the node *i*. Additionally, it is integrated with the identity ID_i as given below.

$$En(k) \ (D_A + ID_i) \tag{6}$$

Upon receiving, fog nodes decrypt it to retrieve the aggregated data and the identity of the data-originated node. After the decryption process, the fog nodes verify the identity of the nodes with their stored information, and if it matches positively, then it will look up its routing table for the selection of the next hop among the neighboring fogs. Moreover, the cloud system *c* authenticates the receiving data using digital signatures. To achieve this, the fog node *FG* first digitally signs the aggregated data D_A using its private key p_r to generate a secret value *S*, as given below.

$$FG_c = S + D_A \tag{7}$$

where

$$E_{p_r}(D_A) = S \tag{8}$$

On the other side, the cloud system first authenticates the digital signature using the public key of the fog nodes and upon successful verification, it is further forwarded to the connected end users with the IoT system. The flow between the developed techniques for intelligent agricultural routing is shown in Figure 3. Initial routes are formulated using the

greedy method and exploited for optimizing the routing process. It can detect redundant nodes in the proximity of a predefined radius and accordingly, it sets the flag value by exploring the intelligent technique of machine learning. The flag value indicates the status of neighbors and whether they can transmit the data or keep them in silent mode. Finally, agricultural data is transmitted towards the sink node using the fog-based IoT system.
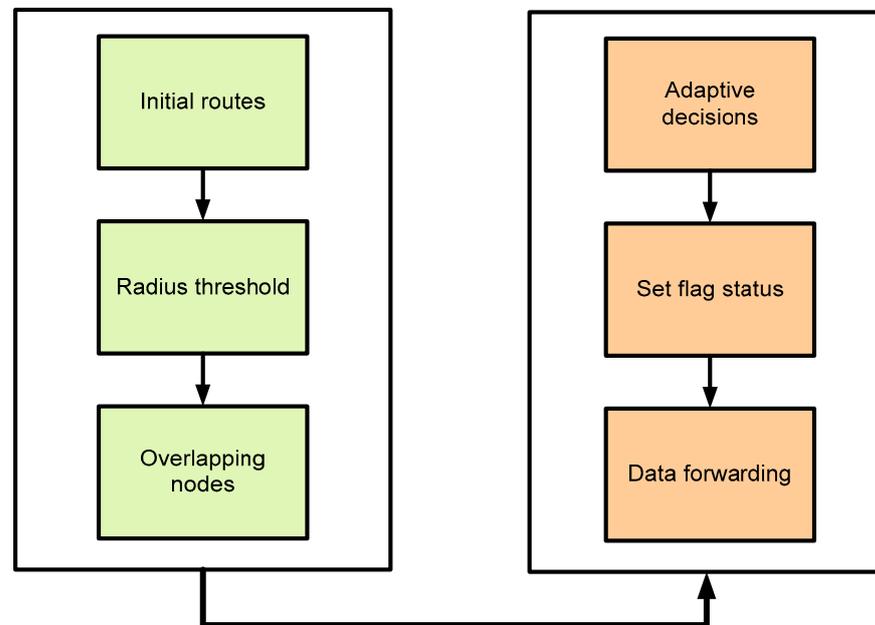

Figure 3. Developed methods for the proposed framework.

Figure 4 explains the security algorithm for transmitting agricultural data with the support of fog nodes. It clarifies the fog-based trust mechanism with privacy concerns and reliability. Accordingly, the proposed security algorithm decreases the probabilities of network attacks and stabilizes the communication system. Fog nodes are utilized as a bridge to facilitate both the IoT and cloud systems. Firstly, fog nodes verified the incoming agricultural data, and upon its validation, authentication and session agreement are established. The session agreement is valid for a particular time and needs to be refreshed later for further communication. In case verification is unsuccessful, then the error message is generated towards the data originating node. Additionally, fog nodes construct routing paths for data forwarding by exploring the routing table. The routing information is updated and evaluated each time that data transmission is needed. In the end, fog and cloud ensure data security using cryptography-based digital signature and encryption techniques. Such a technique provides high-level security measures to the upper layers.
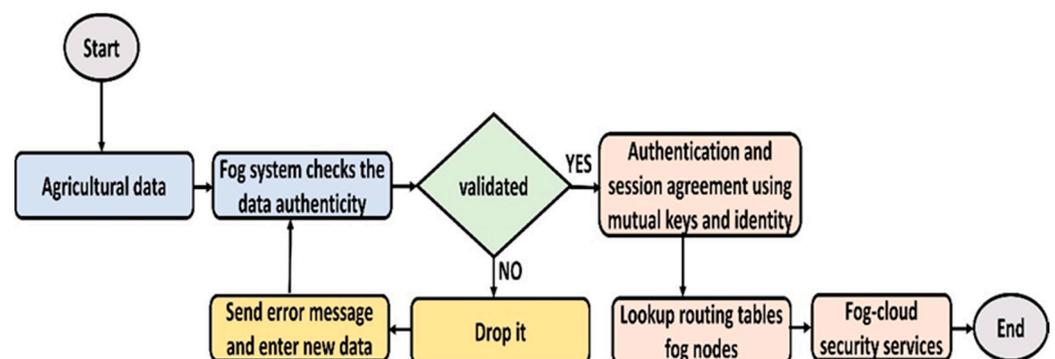

Figure 4. Flowchart of the proposed security algorithm.

Moreover, the functioning of the proposed framework consists of many states, as depicted in Figure 5. The system will be in a specific state at a given time, and it will change states when a particular trigger is called. The objectives of the states are defined below.

- *Sensor's deployment:* In this state, agriculture nodes are randomly dispersed in the targeted area. They have limited constraints and not enough memory, transmissions, and processing resources. They are not able to communicate with the sink node directly;
- *Data sense:* All the deployed sensors, actuators, and IoT devices collaborate in collecting the data. In addition, the data are transferred to the sink nodes through integrating fog systems. The fog nodes are explored for reducing communication delays;
- *Relay node:* The data are obtained from the deployed sensors and forwarded towards the relay node. The roles for relay nodes are not predefined, they are chosen using quality-aware parameters;
- *Decision making:* In this state, a distributed machine learning technique is applied using network statistics to offer the optimal results for attaining a reliable communication system;
- *Data security:* In this end, security actions are performed in this state. It identifies faulty nodes and false messages to detect the comprised data using private values. It increases the reliability of remote users that are connected to cloud systems.
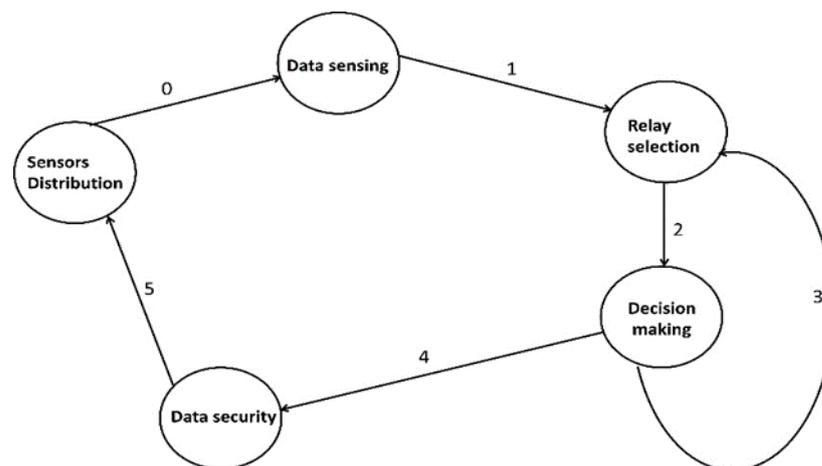

Figure 5. States of the proposed framework.

4. Simulations

This section presents the simulation environment and a discussion of the various tests. We ran the simulations of a core i7 laptop with 64 GB RAM and 1 TB hard drive. 20 trials of the simulations were performed. Between 150 and 750 sensor nodes were used in each simulation experiment. Zigbee technologies were used in the testing, and experiments were carried out in 1000 m × 1000 m area with a variety of configuration settings. For sensing the agricultural environment, numerous sensor categories were utilized, including temperature, air humidity, soil moisture, and water quality. Two sink nodes, between ten and fifteen 15 fog nodes, and various relay nodes were also deployed. Sensor nodes collected the agriculture data and forwarded them to the relay nodes for aggregation and data routing. The fog nodes existed between sensors and sink nodes. The duration of the experiments was 2000 rounds and each round had a time interval of 20 s. The sensors were equipped with GPS. Communication channels were scattered with certain malicious nodes to test the system's security. The results analysis was obtained based on the packet delivery, energy efficiency, network connectivity, and reliability metrics. All the network metrics were evaluated under scenarios of varying sensors and distances from the sink node. Table 2 contains the various parameters for simulations.

Table 2. Simulation parameters.

Parameter	Value
Agriculture sensors	Varying 150–750
Sensor's type	Temperature, air humidity, water quality, soil moisture
Fog nodes	10–15
Interface	IEEE 802.15.4
Round step	20 s
Sink nodes	2
Number of rounds	2000
Initial energy	5 J
Field dimension	1000×1000
Simulations	20

5. Results with Discussion

We evaluated the performance of the proposed framework with other studies in terms of energy efficiency. The performance evaluation of the proposed framework against those of related works is shown in Figure 6a,b for varied IoT sensors and the distance from the sink node. It was found that the proposed framework, even in the presence of malfunctioning nodes, considerably improves the delivery rate of data packets by an average of 20% for varying nodes, and 22% for varying distances from the sink. It results from exploring security approaches, key generation, and mutual trust. In the proposed paradigm, the intelligent system achieves sustainability and effectively identifies harmful activities by utilizing the secret and personal data of devices. Furthermore, the sink nodes are more powerful than IoT sensors and verify each activity before sending it to the end users. Unlike the majority of the proposed research, our framework explicitly provides intelligent decision modules for enhancing packet delivery performance with the aid of machine learning and sustains the network load with improved throughput. Figure 7a,b demonstrate the comparison of the proposed framework in the literature and it was discovered that it notably improves the network reliability by an average of 18% and 23% for both scenarios. This is due to the exposure of machine learning techniques to identify the optimal IoT nodes and intelligently interact with cloud systems. Moreover, the proposed framework can tackle redundant information and decreases the chances of data unavailability and congestion. Additionally, the security solution decreases unwanted traffic across the open transmission system and stops malicious devices from sending false route request packets. As a result, the proposed framework lengthens the response time for critical situations with a nominal delay rate. The comparison of the proposed and existing solutions is revealed in Figure 8a,b in terms of varying nodes and distances from the sink. The statistical analysis demonstrated that the proposed framework increased energy usage by 15% and 24%, respectively. Energy efficiency was found to be negatively impacted when the number of devices increased. On the other hand, the proposed framework provides a smart energy solution based on a distributed machine learning technique and smoothly selects the updated routes by utilizing the optimum solution. Additionally, the proposed framework effectively defends against multiple attacks and minimizes the consumption of network bandwidth by employing a security algorithm. Consequently, the nodes' energy is increased, which improves the performance of the entire network. By finding the redundant nodes in the routing table, the flag status is modified. Nodes whose flag value is false are therefore prohibited from participating in data routing. The performance comparison of the proposed framework to the existing solutions for network connectivity is illustrated in Figure 9a,b. Network connectivity indicates the active time at which nodes use particular communication links. The connectivity ratio for the proposed framework against various IoT devices and varied distances is remarkably enhanced by an average of 16% for varying distances from the sink and 20% in terms of varying nodes. This is due to the ability of the proposed framework to efficiently manage power distribution across the sensors and investigate the machine learning principles for accomplishing forwarding decisions.

Moreover, the proposed framework directs the routing module to formulate the routes by re-evaluating the decisions whenever any disrupted intermediate links are discovered or frequent re-transmissions. The proposed framework successfully manages the transmission overheads by including the least computational cost function.
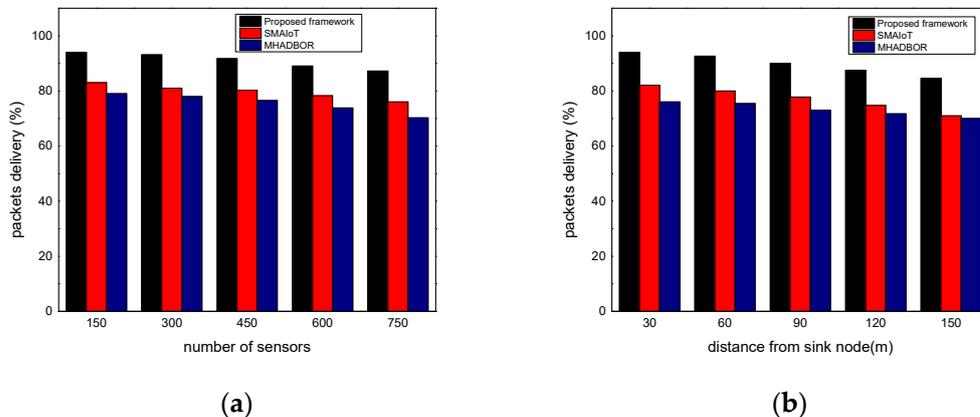

Figure 6. (**a**) Packets delivery with varying sensors and (**b**) Packets delivery with varying distance.
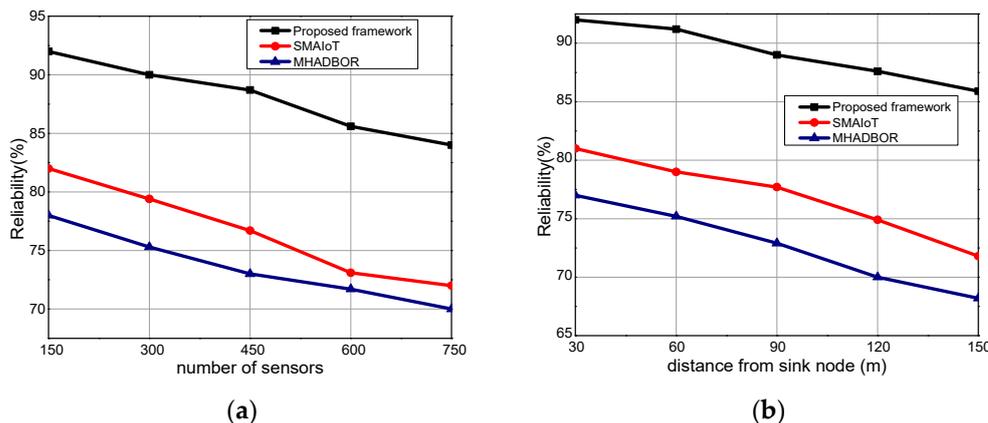

Figure 7. (**a**) Reliability with varying sensors and (**b**) Reliability with varying distance.
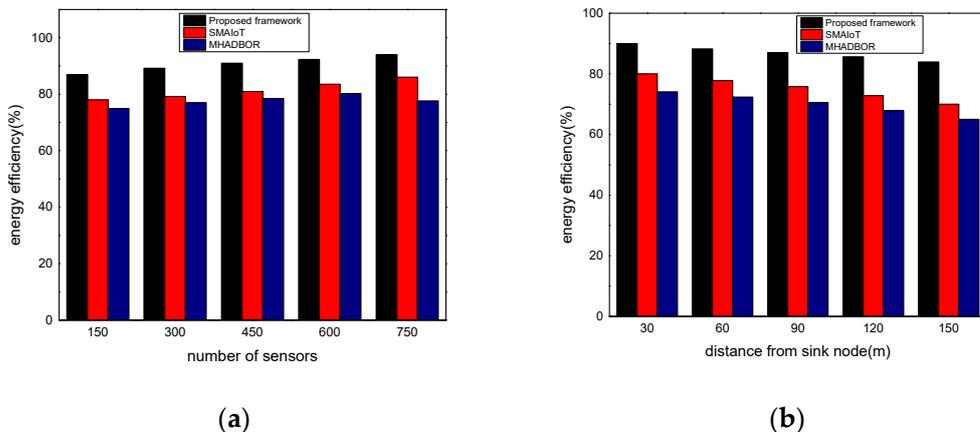

Figure 8. (**a**) Energy efficiency with varying sensors and (**b**) Energy efficiency with varying distance.
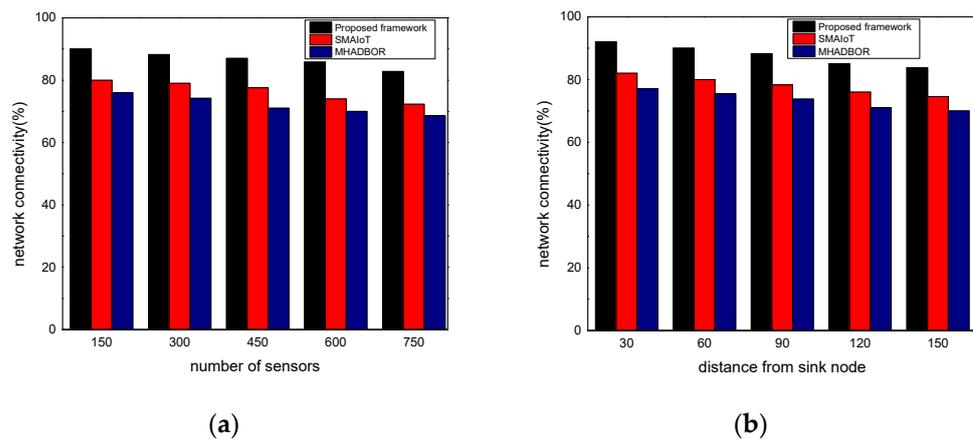
Figure 9. (**a**) Network connectivity with varying sensors and (**b**) Network connectivity with varying distance.

6. Conclusions

With an emphasis on green energy and remote monitoring, smart technologies and agricultural systems have grown significantly in recent years. It controls the plants, soil characteristics, water pressure, and weather-related information, which benefits farmers and increases production. However, limited solutions have been proposed to enhance production in precision agriculture while reducing latency and information disturbance. Furthermore, protecting agricultural data while utilizing the insecure Internet is another significant research challenge. In this study, we presented a framework for providing a farmer communication system to enhance timely delivery through the cooperation of fog systems. This system also incorporates redundant information detection, which reduces network bandwidth inefficiencies. Additionally, the proposed framework employs security methods to counter privacy attacks on sensing data. The performance results showed the good outcomes of the proposed framework with maximum energy efficiency and delivery ratio. Furthermore, its performance has proven the improved processing usage in the existence of malicious devices. In the future, we intend to cope with the proposed framework's scalability and load-balancing issues with the support of a multi-cloud architecture. Moreover, we would like to integrate security to maintain cloud integrity from the point of users' perspective.

Author Contributions: Conceptualization, A.R. and K.H.; methodology, A.R. and I.A.; software, I.A. and K.H.; validation, J.L., L.P. and A.R.; formal analysis, A.R. and J.L.; investigation, L.P. and I.A.; resources, A.R. and I.A.; data curation, J.L. and L.P.; writing—original draft preparation, I.A. and A.R.; writing—review and editing, K.H., J.L. and L.P.; visualization, A.R. and L.P.; supervision, J.L. and I.A.; project administration, A.R. and I.A.; funding acquisition, J.L. and I.A. All authors have read and agreed to the published version of the manuscript.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data are provided within the manuscript.

References

1. Zhou, I.; Makhdoom, I.; Shariati, N.; Raza, M.A.; Keshavarz, R.; Lipman, J.; Abolhasan, M.; Jamalipour, A. Internet of things 2.0: Concepts, applications, and future directions. *IEEE Access* **2021**, *9*, 70961–71012. [CrossRef]
2. Nguyen, V.-L.; Lin, P.-C.; Cheng, B.-C.; Hwang, R.-H.; Lin, Y.-D. Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2384–2428. [CrossRef]
3. Rehman, A.; Haseeb, K.; Saba, T.; Lloret, J.; Ahmed, Z. Mobility Support 5G Architecture with Real-Time Routing for Sustainable Smart Cities. *Sustainability* **2021**, *13*, 9092. [CrossRef]
4. Rehman, A.; Haseeb, K.; Saba, T.; Lloret, J.; Tariq, U. Secured Big Data Analytics for Decision-Oriented Medical System Using Internet of Things. *Electronics* **2021**, *10*, 1273. [CrossRef]
5. Quy, V.K.; Hau, N.V.; Anh, D.V.; Quy, N.M.; Ban, N.T.; Lanza, S.; Randazzo, G.; Muzirafuti, A. IoT-Enabled Smart Agriculture: Architecture, Applications, and Challenges. *Appl. Sci.* **2022**, *12*, 3396. [CrossRef]
6. Lloret, J.; Garcia, M.; Bri, D.; Sendra, S. A Wireless Sensor Network Deployment for Rural and Forest Fire Detection and Verification. *Sensors* **2009**, *9*, 8722–8747. [CrossRef] [PubMed]
7. Gavrilović, N.; Mishra, A. Software architecture of the internet of things (IoT) for smart city, healthcare and agriculture: Analysis and improvement directions. *J. Ambient Intell. Humaniz. Comput.* **2021**, *12*, 1315–1336. [CrossRef]
8. Raj, M.; Gupta, S.; Chamola, V.; Elhence, A.; Garg, T.; Atiquzzaman, M.; Niyato, D. A survey on the role of Internet of Things for adopting and promoting Agriculture 4.0. *J. Netw. Comput. Appl.* **2021**, *187*, 103107. [CrossRef]
9. Haseeb, K.; Saba, T.; Rehman, A.; Ahmed, Z.; Song, H.H.; Wang, H.H. Trust management with fault-tolerant supervised routing for smart cities using internet of things. *IEEE Internet Things J.* **2022**. [CrossRef]
10. Khan, A.I.; Alsolami, F.; Alqurashi, F.; Abushark, Y.B.; Sarker, I.H. Novel energy management scheme in IoT enabled smart irrigation system using optimized intelligence methods. *Eng. Appl. Artif. Intell.* **2022**, *114*, 104996. [CrossRef]
11. Singh, R.K.; Berkvens, R.; Weyn, M. AgriFusion: An Architecture for IoT and Emerging Technologies Based on a Precision Agriculture Survey. *IEEE Access* **2021**, *9*, 136253–136283. [CrossRef]
12. Maddikunta, P.K.R.; Hakak, S.; Alazab, M.; Bhattacharya, S.; Gadekallu, T.R.; Khan, W.Z.; Pham, Q.-V. Unmanned Aerial Vehicles in Smart Agriculture: Applications, Requirements, and Challenges. *IEEE Sens. J.* **2021**, *21*, 17608–17619. [CrossRef]
13. Farooq, M.S.; Riaz, S.; Abid, A.; Abid, K.; Naeem, M.A. A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. *IEEE Access* **2019**, *7*, 156237–156271. [CrossRef]
14. Johnson, N.; Kumar, M.S.; Dhannia, T. A study on the significance of smart IoT sensors and Data science in Digital agriculture. In Proceedings of the 2020 Advanced Computing and Communication Technologies for High Performance Applications (ACCTHPA), Cochin, India, 2–4 July 2020.
15. He, S.; Shi, K.; Liu, C.; Guo, B.; Chen, J.; Shi, Z. Collaborative Sensing in Internet of Things: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 1435–1474. [CrossRef]
16. Churcher, A.; Ullah, R.; Ahmad, J.; Rehman, S.U.; Masood, F.; Gogate, M.; Alqahtani, F.; Nour, B.; Buchanan, W. An Experimental Analysis of Attack Classification Using Machine Learning in IoT Networks. *Sensors* **2021**, *21*, 446. [CrossRef]
17. Bagaa, M.; Taleb, T.; Bernabe, J.B.; Skarmeta, A. A Machine Learning Security Framework for Iot Systems. *IEEE Access* **2020**, *8*, 114066–114077. [CrossRef]
18. Demestichas, K.; Peppes, N.; Alexakis, T. Survey on Security Threats in Agricultural IoT and Smart Farming. *Sensors* **2020**, *20*, 6458. [CrossRef]
19. Elijah, O.; Rahman, T.A.; Orikumhi, I.; Leow, C.Y.; Hindia, M.N. An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges. *IEEE Internet Things J.* **2018**, *5*, 3758–3773. [CrossRef]
20. Abunadi, I.; Mengash, H.A.; Alotaibi, S.S.; Asiri, M.M.; Hamza, M.A.; Zamani, A.S.; Motwakel, A.; Yaseen, I. Optimal Multikey Homomorphic Encryption with Steganography Approach for Multimedia Security in Internet of Everything Environment. *Appl. Sci.* **2022**, *12*, 4026. [CrossRef]
21. Ferrag, M.A.; Shu, L.; Yang, X.; Derhab, A.; Maglaras, L. Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. *IEEE Access* **2020**, *8*, 32031–32053. [CrossRef]
22. Vangala, A.; Das, A.K.; Chamola, V.; Korotaev, V.; Rodrigues, J.J. Security in IoT-enabled smart agriculture: Architecture, security solutions and challenges. *Clust. Comput.* **2022**. [CrossRef]
23. Haseeb, K.; Ud Din, I.; Almogren, A.; Islam, N. An Energy Efficient and Secure IoT-Based WSN Framework: An Application to Smart Agriculture. *Sensors* **2020**, *20*, 2081. [CrossRef] [PubMed]
24. Rao, P.M.; Deebak, B.D. Security and privacy issues in smart cities/industries: Technologies, applications, and challenges. *J. Ambient Intell. Humaniz. Comput.* **2022**. [CrossRef]
25. Singh, T.; Solanki, A.; Sharma, S.K.; Nayyar, A.; Paul, A. A Decade Review on Smart Cities: Paradigms, Challenges and Opportunities. *IEEE Access* **2022**, *10*, 68319–68364. [CrossRef]
26. Sodhro, A.H.; Pirbhulal, S.; Luo, Z.; de Albuquerque, V.H.C. Towards an optimal resource management for IoT based Green and sustainable smart cities. *J. Clean. Prod.* **2019**, *220*, 1167–1179. [CrossRef]

27.	Abidoye, A.P.; Kabaso, B. Energy-efficient hierarchical routing in wireless sensor networks based on fog computing. *EURASIP J. Wirel. Commun. Netw.* **2021**, *2021*, 8. [CrossRef]

28.	Wang, T.; Zhang, G.; Alam Bhuiyan, Z.; Liu, A.; Jia, W.; Xie, M. A novel trust mechanism based on Fog Computing in Sensor–Cloud System. *Future Gener. Comput. Syst.* **2020**, *109*, 573–582. [CrossRef]

29.	Ahmed, S.; Hossain, F.; Kaiser, M.S.; Noor, M.B.T.; Mahmud, M.; Chakraborty, C. Artificial Intelligence and Machine Learning for Ensuring Security in Smart Cities. In *Data-Driven Mining, Learning and Analytics for Secured Smart Cities*; Springer: Cham, Switzerland, 2021; pp. 23–47. [CrossRef]

30.	Alam, T. Cloud-Based IoT Applications and Their Roles in Smart Cities. *Smart Cities* **2021**, *4*, 1196–1219. [CrossRef]

31.	Aldegheishem, A.; Alrajeh, N.; Garcia, L.; Lloret, J. SWAP: Smart WAter Protocol for the Irrigation of Urban Gardens in Smart Cities. *IEEE Access* **2022**, *10*, 39239–39247. [CrossRef]

32.	Zikria, Y.; Ali, R.; Afzal, M.; Kim, S. Next-Generation Internet of Things (IoT): Opportunities, Challenges, and Solutions. *Sensors* **2021**, *21*, 1174. [CrossRef]

33.	Maksimovic, M. Greening the future: Green Internet of Things (G-IoT) as a key technological enabler of sustainable develop-ment. In *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence*; Springer: Cham, Switzerland, 2018; pp. 283–313.

34.	Mahajan, B.H.; Badarla, A.; Junnarkar, A.A. CL-IoT: Cross-layer Internet of Things protocol for intelligent manufacturing of smart farming. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 7777–7791. [CrossRef]

35.	Tabassum, M.; Perumal, S.; Kashem, S.B.A.; Ponnan, S.; Chakraborty, C.; Chowdhury, M.E.H.; Khandakar, A. Enhance data availability and network consistency using artificial neural network for IoT. *Multimedia Tools Appl.* **2022**. [CrossRef]

36.	Pandiyaraju, V.; Logambigai, R.; Ganapathy, S.; Kannan, A. An Energy Efficient Routing Algorithm for WSNs Using Intelligent Fuzzy Rules in Precision Agriculture. *Wirel. Pers. Commun.* **2020**, *112*, 243–259. [CrossRef]

37.	Adil, M.; Khan, M.K.; Jamjoom, M.; Farouk, A. MHADBOR: AI-Enabled Administrative-Distance-Based Opportunistic Load Balancing Scheme for an Agriculture Internet of Things Network. *IEEE Micro* **2021**, *42*, 41–50. [CrossRef]

38.	Jani, K.A.; Chaubey, N.K. A Novel Model for Optimization of Resource Utilization in Smart Agriculture System Using IoT (SMAIoT). *IEEE Internet Things J.* **2021**, *9*, 11275–11282. [CrossRef]

39.	Ren, W.; Wan, X.; Gan, P. A double-blockchain solution for agricultural sampled data security in Internet of Things network. *Futur. Gener. Comput. Syst.* **2020**, *117*, 453–461. [CrossRef]

40.	Dilek, S.; Irgan, K.; Guzel, M.; Ozdemir, S.; Baydere, S.; Charnsripinyo, C. QoS-aware IoT networks and protocols: A comprehen-sive survey. *Int. J. Commun. Syst.* **2022**, *35*, e5156. [CrossRef]

41.	Khan, S.; Parkinson, S.; Qin, Y. Fog computing security: A review of current applications and security solutions. *J. Cloud Comput.* **2017**, *6*, 19. [CrossRef]

42.	Kumar, D.P.; Amgoth, T.; Annavarapu, C.S.R. Machine learning algorithms for wireless sensor networks: A survey. *Inf. Fusion* **2019**, *49*, 1–25. [CrossRef]