

Article

Intellectual Property Theft Protection in IoT Based Precision Agriculture Using SDN

Md. Selim Hossain ¹, Md. Habibur Rahman ², Md. Sazzadur Rahman ^{3,*}, A. S. M. Sanwar Hosen ⁴,
Changho Seo ⁵ and Gi Hwan Cho ^{4,*}

¹ Department of Computing and Information System (CIS), Daffodil International University, Dhaka 1207, Bangladesh; selimtee@gmail.com

² Department of Information and Communication Technology, Bangabandhu Sheikh Mujibur Rahman Digital University, Gazipur 1750, Bangladesh; habibur@ict.bdu.ac.bd

³ Institute of Information Technology, Jahangirnagar University, Savar, Dhaka 1342, Bangladesh

⁴ Division of Computer Science and Engineering, Jeonbuk National University, Jeonju 54896, Korea; sanwar@jbnu.ac.kr

⁵ Department of Convergence Science, Kongju National University, Gongju 32588, Korea; chseo@kongju.ac.kr

* Correspondence: sazzad@juniv.edu (M.S.R.); ghcho@jbnu.ac.kr (G.H.C.)

Abstract: In this work, we examine the privacy and safety issues of Internet of Things (IoT)-based Precision Agriculture (PA), which could lead to the problem that industry is currently experiencing as a result of Intellectual Property Theft (IPT). Increasing IoT-based information flow in PA will make a system less secure if a proper security mechanism is not ensured. Shortly, IoT will transform everyday lives with its applications. Intellectual Property (IP) is another important concept of an intelligent farming system. If the IP of a wise farming system leaks, it damages all intellectual ideas like cultivation patterns, plant variety rights, and IoT generated information of IoT-based PA. Thus, we proposed an IoT enabled SDN gateway regulatory system that ensures control of a foreign device without having access to sensitive farm information. Most of the farm uses its devices without the use of its integrated management and memory unit. An SDN-based structure to solve IP theft in precision farming has been proposed. In our proposed concept, a control system integrates with the cloud server, which is called the control hub. This hub will carry out the overall PA monitoring system. By hiring the farm devices in the agricultural system, these devices must be tailored according to our systems. Therefore, our proposed PA is a management system for all controllable inputs. The overall goal is to increase the probability of profit and reduce the likelihood of IPT. It does not only give more information but also improves information securely by enhancing the overall performance of PA. Our proposed PA architecture has been measured based on the throughput, round trip time, jitter, packet error rate, and the cumulative distribution function. Our achieved results reduced around (1.66–6.46)% compared to the previous research. In the future, blockchain will be integrated with this proposed architecture for further implementation.

Keywords: intellectual property; precision agriculture; IoT; SDN; gateway; smart control



Citation: Hossain, M.S.; Rahman, M.H.; Rahman, M.S.; Hosen, A.S.M.S.; Seo, C.; Cho, G.H. Intellectual Property Theft Protection in IoT Based Precision Agriculture Using SDN. *Electronics* **2021**, *10*, 1987. <https://doi.org/10.3390/electronics10161987>

Academic Editors: Rashid Mehmood and Domenico Ursino

Received: 15 July 2021

Accepted: 13 August 2021

Published: 18 August 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Agriculture is tremendously important throughout the world. To provide the conversion on the road to exploiting efficiency, sustainable production, and actual time, reliable evidence about crop progress is vital today. PA can be seen as a new era of agriculture that makes agriculture a more skillful and accurate way of utilizing expertise to raise cattle and grow crops. This is the farm management method, the critical component of ICT is the usage of sensors, regulator systems, robotics, stand-alone vehicles, automatic hardware, Software Defined Network (SDN), Internet of Things (IoT), and variable technology. Precision agriculture based on IoT provides valuable insight into crop growth, development, transformation, farming, and so on [1,2]. The IoT-based system for radar monitoring allows

for high-cloud weather-based analysis. At the same time, the optical sensors discriminate between crop type, soil pH, water level, and health and maturity. Hands-on crop nursing is now possible through the latest information satellite and a scalable high-speed cloud computation system for agricultural insurance resolutions. We can gain competitive insights with advanced crop performance analytics, and advantages compare to the previous ones. Receiving early warnings about cultivation failure or agriculture helps a farmer make decisions.

Expositions of data relations and responses to potential threats or diseases, nutrients or water deficiencies, crop production drought, risk mitigation, and infrastructure sustainability provide proper predication in smart farming [3]. Farmers with a wealth of information are also supplied with PA to build up their farm records, improve decision-making, foster more traceability, increase agricultural products marketing, improve rental arrangements and landowners' relationships, improve farming quality inherently, and so forth. The agricultural sector must adopt new technologies to achieve a much-needed edge to meet the needs of the increasing population. Thus, SDN and IoT [4,5] enable the industry to raise operational efficiency, reduce costs, and cut waste. It also manages delivery issues and improves yield quality in new agricultural applications in smart agriculture and IoT precision having an SDN enabled smart network. Farmers can also monitor the conditions on the field from anywhere, which means remote monitoring. IoT's intelligent agriculture is highly efficient compared to the traditional method. In addition to the conventional, large-scale farming processes involved in SDN and IoT-smart farming, the applications may also provide new levers to uplift other crop and common trends in farming such as organics, family agriculture (completive or small-scale areas, particular crops, high-quality crops, etc.), and enhance the highly transparent system of agriculture [6,7]. The use of IoT-SDN based intelligent farming means that a system with sensor aids (light, humidity, temp, soil humidity, etc.) for monitoring crop fields is developed, and an irrigation system is automated. When these external or foreign devices are employed temporarily in our PA system, our proposed system by the intelligent hub will control the intelligent farming system. These plans are also effort based on monitoring, based on intelligent farming systems. The connection scheme of the farm system is a vital concern of these external devices. These devices can generally work in the network system or can be customized to operate.

1.1. Scientific Progression in IoT Based PA

IoT is playing a role in transforming our everyday lives with different types of applications. There are already 31 billion connected IoT [8] devices around the globe that help us to carry out daily tasks with added ease. When devices monitor our activities and know what we need to achieve, we have less to worry about. Thus, the expansion of IoT products has spread worldwide [9]. The use of IoT has boosted many industries by using low-cost sensors and IoT platforms, data collection, real-time insight, and process automation. In this way, the agriculture and agriculture industry, in general, can truly take advantage of the IoT solution [10]. It is also a key solution to the growing concern over the global population's food and environmental impact, not only a smart agricultural approach but also today's innovative agricultural technique.

PA is one of today's most curved issues. IoT-based PA covers various technologies, including sensors, Media Access Control (MAC), Global Positioning System (GPS), drones, satellite images, and big data. IoT-based PA covers a range of technologies. The use of IoT in farm machinery enables farmers to practice compared with fewer inputs that reduce costs rather than produce higher amounts. IoT also comprises hardware, such as sensors, machine-to-machine and long-range, decision support software, and web-based software. The most advantageous point of using this technology is that it can be combined at a very affordable price, allowing countries to stop precision farming approaches. The production concerns farmers' special and results-oriented efforts. By using IoT, farmers can assess the aspects of agriculture and take appropriate steps to obtain results. The production of

farmers with IoT using sensors, robotics, control systems, and more to forecast the results is guaranteed if they follow the analysis results and instructions. PA helps farmers determine where the problem is by providing the best services and forecasts of what to plant and regular seeding updates, analysis, and delivery of highly advanced combined sensors to soil moisture specifications.

1.2. Current Situation of Intellectual Property in PA

IP contains intangible human intellect conceptions. Many forms and some countries identify more than others as IP. Copyrights, patents, trademarks, and business secrets are the most well-known kind. The existing IoT-based farming is limited to hiring foreign devices when these devices are required in smart agriculture. It is like a usual process. When we engage these foreign agents, these devices can quickly look up every system of an intelligent farming system. It is very easy to steal any information or intellectual property such as plant patterns, employee skills, or farming policies for these foreign agents. It was only in the late 20th century that intellectual property was employed in most legal schemes worldwide. IP is primarily aimed at inspiring the development of an extensive range of IP rights. Intellectual property gives individuals and companies the right of information and intellectual property, usually for only a limited time. Intellectual Capital (IC) means a change in the value of knowledge for a company. Thus, the debit and IC are the credit or share of intellectual property such as people, patents, processes, brand names, etc. If this IP idea is shared or accessed somehow, then the concept could easily be implemented in another smart farming system. As a result, the goal of that farming system may not be adequately obtained. Now, there is no control hub procedure of the current smart farming system. If we hire a device in a smart farming system, it can easily access my farming information due to the existing IoT-based PA infrastructure.

1.3. Impact of Intellectual Capital Theft in PA

IP theft includes removing an individual or company from trade secrets or soft products, known as ‘cultural property’, from ideas, inventions, or creative expressions. From new crop production and farm equipment design, commercializing and labelling of farm products are essential. Intellectual goods have a long-term effect and significant importance in the many agricultural sectors. However, the interaction between intellectual property law and agriculture has had comparatively less interest or attention. The situation has reformed over the past decade mainly because of increasing awareness of the role of IP law in food safety. If the business secret or policy is publicly disclosed, there will be a massive impact on this particular enterprise. The corporate competition might also be a public structure. If IP theft takes place in a specific agricultural system, a catastrophic drawback from that agricultural system will be imposed. The adoption of nano-based biomarkers to trace patented products through new scientific and technical innovations throughout the food chain uses molecular markers in breeding. To track proprietary products or data-based intelligent agriculture information, the adoption of nano-based biomarkers might be communicated throughout the world. The guardian of IP is serious about promoting innovation. Innovation, farms, and individuals would not benefit from the full support of their inventions without protecting ideas and would focus less on research and growth. Artists would therefore not be fully paid for their creations, and their cultural strength would suffer. Intellectual property is a category of property that includes intangible creations of the human intellect in a PA. It has a direct impact on a smart farming system. Cultivation patterns, plant variety rights, and IoT generated information from a smart farming system are the intellectual properties that are protected by the IoT-SDN gateway hub.

When foreign devices are hired in a PA, these devices must load the IoT-SDN operating system. The foreign devices are operated by the direction of this IoT-SDN intelligent hub.

IoT based precision agriculture is a new era of technology for smart farming systems. In the previous research works, intellectual property theft has not been protected. In our research work, firstly, we have proposed an SDN-IoT framework to protect intellectual

property. In our proposed framework, we have approached an SDN-GW connection hub that will manage the foreign devices. Secondly, in this research, we have proposed an algorithm that will control the apparatus according to the PA criteria. Finally, foreign device mobility management has been simulated and executes better performance than other mobility management.

The structure of this paper has been described as follows. In Section 2, literature survey is described. Section 3 describes the architecture of the proposed framework. In Section 4, evaluation and result analysis are illustrated. Section 5 presented the overall conclusions of the paper relating to the future work.

2. Literature Survey

Agriculture is the essential sector for sustainable development in the fourth industrial (4I) revolution [10]. Since technology is rapidly growing rationally with modern civilization, the agriculture sector has also adopted intelligent tools and techniques [11]. As a result, IoT is facilitating better and faster services in recent agriculture. Another new technology, SDN, has also been introduced in several sectors, including agriculture [12]. SDN has also been implemented to manage the network traffic in multipath routing [13]. SDN has also been inaugurated in IoT based monitoring in 5G networks [14]. The use of smart devices, especially IoT in agriculture, is termed as PA and provides valuable information on crop growth, development, processing, cultivation, etc. Satellite and scalable high-speed cloud and edge computing systems are also used for proactive crop cultivation [15]. They can also provide competitive insights with advanced crop performance analytics and advantages from previous information. Early warnings of cultivation failure help a farmer to make decisions accordingly. Expositions of data relations and responses to potential threats to gas or diseases, nutrients or water deficiencies, and crop production drought. If the farmer can establish a sustainable infrastructure of a firm, then they can mitigate the risk and forecast the market viability.

To store farm records, improve decision-making, promote traceability, and enhance agricultural products' marketing, IoT can oversee the challenges [16]. To improve the rental arrangements and the relationship of landowners, improve farming quality and so forth, farmers will also receive a wealth of information. According to the current growing population, it is now expected to reach 9.6 billion by 2050 [17]. Agriculture must grow its demand, irrespective of environmental challenges, including unpleasant conditions and climate change. The agricultural sector has to adopt new technologies to achieve an extended production edge to meet the needs of the increasing population. IoT might be a suitable addition to agriculture to enable the agricultural industry to raise operational efficiency, reduce costs, cut waste, manage its delivery, and improve yield quality in new agricultural applications [18].

SDN-enabled IoT's intelligent agriculture is highly efficient compared to the traditional method [18]. The application of SDN and IoT-oriented smart farming could target the conventional, large-scale farming processes and ensure the secured and scalable precision agriculture. Preserving high-quality varieties and improving the highly transparent agriculture system SDN and IoT integration have been studied in intelligent homes and industries. However, the integration of SDN in IoT based PA is an entirely new concept and more challenging issue. Thus, we have proposed precision agriculture compiled with IoT and SDN. Most of the researchers have researched SDN to outperform IoT devices and make them more secure. Some also work on NFV and blockchain technology. Their focus is on building, city, network and mobility management. Very few have done security concern in precision agriculture. Thus, we have focused on the security aspects of the IP in precision agriculture. We have also shown a comparison of our proposed model along with the other researchers in Table 1.

Table 1. Qualitative comparison of our proposed model along with previous work.

Authors	Focus	Technology	Platform	Protocol	QoS	Throughput
T. Maksymyuk, et al. [14]	Network Monitoring	5G, SDN and IoT	–	MQTT	Signal Strength compared among small and macro cell	–
P. K. Sharma et al. [19]	Distributed Network Management	IoT, SDN and Blockchain	Mininet 2.1.0	OpenFlow DistFlow	Compared Bandwidth of OpenFlow with DistSoft	–
B. K. Mukherjee et al. [20]	Smart City Management	IoT, SDN and NFV	Mininet WiFi	OpenFlow	Compared RTT with OpenFlow Protocol for three cluster	Compared with OpenFlow Protocol for three cluster
Y. Wang et al. [21]	Mobility Management	SDN	Mininet 2.1.0	Network Layer-3	Compared RTT for 3 different protocols with handover	–
A. Rahman et al. [22]	Smart City Management	IoT, SDN and NFV	Mininet 2.2.1	OpenFlow	Compared RTT with OpenFlow Protocol	Compared with OpenFlow Protocol
A. Rahman et al. [23]	Building Management	IoT, SDN and Blockchain	Mininet WiFi	OpenFlow	Compared RTT for 3 different size networks with OpenFlow Protocol	Compared with extended MINA architecture
D. Sinh, et al. [24]	Network Management	SDN, NFV and IoT	Mininet 2.0.0	OpenFlow	Reachability and network slicing	–
F. Cauteruccio, et al. [25]	Smart City Management	IoT	MIoT	IPSO	Average running time	Anomaly degree and percentage
Proposed	Security in Precision Agriculture	IoT and SDN	Mininet WiFi	OpenFlow	Compared RTT, Jitter, PER with mobility	Compared with OF protocol and 3 different clusters

A comprehensive analysis has been highlighted in the table. The key focus features along with the implemented protocol and the measurement matrices have been analyzed. Most researchers have studied structural and network management using SDN, NFV, IoT, and blockchain. Researchers have clarified their work as having QoS throughput measurement. SDN and IoT based OpenFlow and MQTT protocol have been considered for the implementation. We have considered LoRa and OpenFlow protocols in our proposed framework, and Mininet Wi-Fi have been chosen for simulation. We have also compared our obtained results and the previous research evaluating PER, CDF, Jitter, RTT, and throughput.

SDN and IoT-based intelligent farming means that a system with sensor aids (light, humidity, temp, soil humidity, etc.) for monitoring crop fields is developed, and an irrigation system is automated. Traditionally, any automatic farm consists of its native intelligent devices. Sometimes, farmers need to hire some foreign devices occasionally for strip cropping, large scale irrigation and so on, which can expose the farming information, production mechanism, intellectual property, and some other confidential resources. External or foreign devices are vulnerable threats for security purposes. Handle foreign devices are the critical concerns of the researcher. To the best of our knowledge, no one introduces SDN in IoT to facilitate the farmers for better and qualified PA. Hence, we have proposed a framework to provide a better quality of service in PA and network management. We have also proposed an algorithm to efficiently handle the foreign devices and manage the intellectual assets of any precision agriculture. In the end, to control the foreign mobile devices, we have also compared the improved quality of service (QoS) of our proposed model along with previously implemented mobile architecture in multiple controllers' domains [26].

3. Architecture of the Proposed Framework

Hereby, this framework mainly contributes to reducing IPT in precision farming presented in Figure 1.

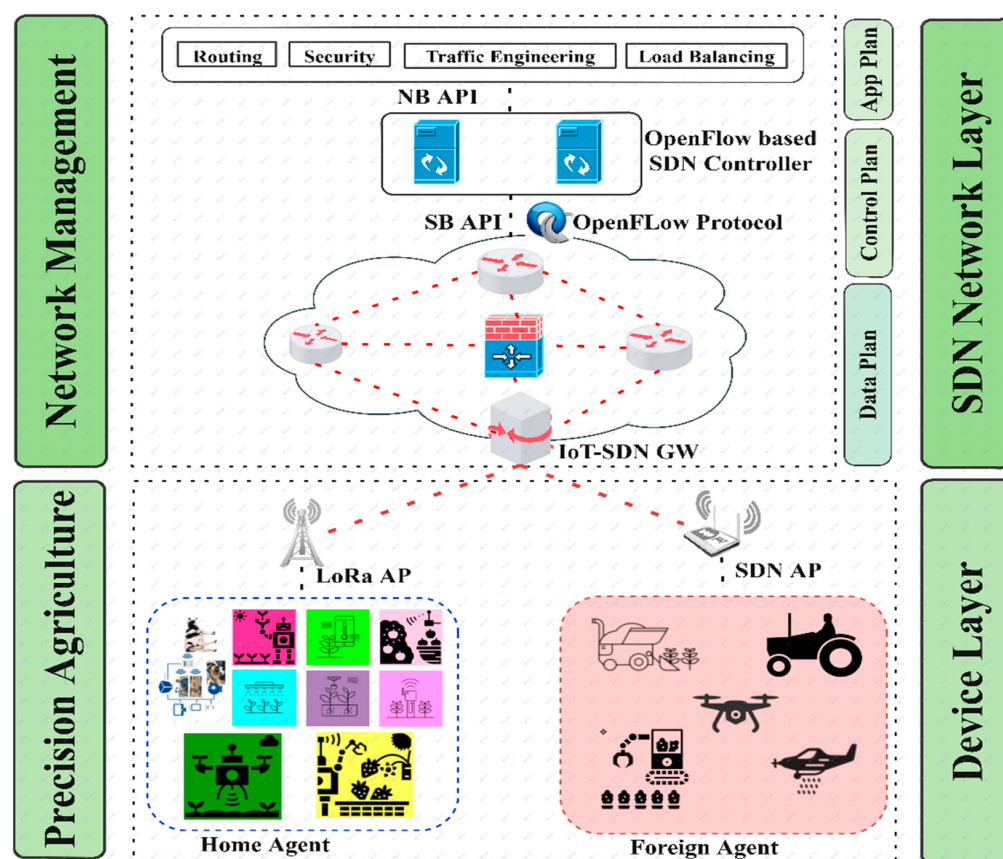


Figure 1. System workflow of the proposed framework.

The entire PA monitoring system will be implemented according to this proposed system. The framework is divided into two different device and network layers. An IoT-SDN gateway connected the layers to provide consistent remote control of the smart farming devices. Based on the operational behavior, devices are separated into the home and foreign agent. Native devices are termed home agents that are managed by home access points operated with LoRa protocol. SDN is used to manage the external devices that are called the foreign agent. Since SDN offers dynamical modification according to the user's expectation, agricultural information can be protected from the outside world. OpenFlow protocol based SDN access points can handle the foreign agent. The home and foreign agent can be inclined with the IoT-SDN gateway for network management. In this work, the devices are perfectly in line with our gateway hub system and enhance the efficiency of the intelligent farming system. SDN operational functionality, modified mechanical strategy, and proposed framework algorithm are described below.

3.1. Precision Agricultural Network

In PA, most smart devices are assigned with their specific tasks like moisture, GPS, temperature, smoke, pH sensors, sprinkler, camera, drone, etc. Some smart devices occasionally need the same tractor, irrigator, harvester etc. These types of devices are called foreign devices and are hired once or twice in an agricultural session. These devices are varied in number based on the size of a PA. In a small farm, almost 15–30 smart devices are installed, including networking devices. This number is increased to 30–60 for a medium-size PA. More than 70 numbers of devices are installed for large size PA. Thus, we have considered three different size network clusters containing 25, 50, and 100 nodes respectively for small, medium, and large size in our proposed PA architecture.

3.2. Management of IP Rights and Foreign Agents

Today, several different analog farming methods exist. For every farmer, agricultural store, and agronomic, technology has become an integral part of their company. Farming requires a lot of techniques and efforts to develop smart farming. Agriculturists utilize technology to enhance efficiency and control expenses. With the development and modernization of digital technology, IoT-based smart farming concepts have emerged. Application of IoT in agriculture promises previously unavailable efficiency, reduced resources and cost, automation, and data-driven processes. In agriculture, these benefits act as improvements, but the solutions for the whole industry turn into a range of dangerous problems such as IP theft. Cultivation patterns, plant variety, copyright, trademarks, internal database management, employee competence, and IoT device generated information from a smart farming system are examples of IP rights.

The core of smart farming is derived from the ability to extract value from IP data. When foreign agents know the IP data, such as internal database management, it must possibly leak these IP rights. To protect this leakage, we have proposed the foreign agents' management policy which has been shown in Figure 2. When these IoT-based foreign agents are hired, we have a customized setting to control these agents. These devices are loaded and operated according to the criteria of PA. Since we customize the setting for foreign agents, these foreign agents have strong restriction to accessing all PA things. Since these devices are controlled by an IoT-SDN control hub, data generated from these devices are stored in separate cloud servers. As a result, IP rights can be easily protected.

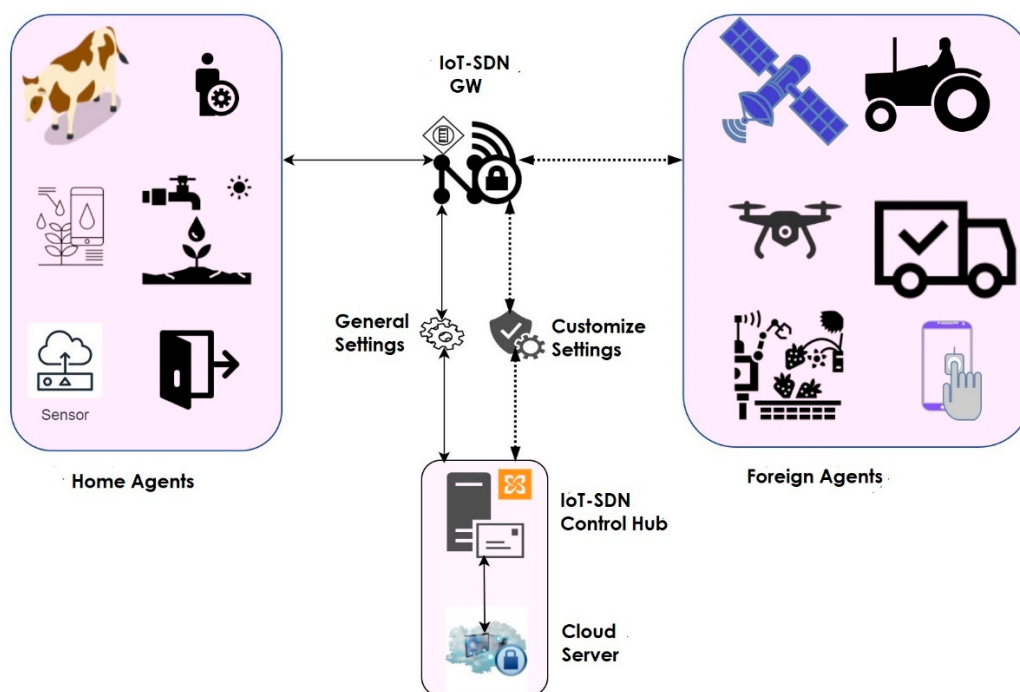


Figure 2. Foreign agent selection for IP rights management.

3.3. IoT-SDN Gateway Integration

A smart SDN based gateway is a server to manage both the home and foreign agents outside the network. The computer system within the IoT based agricultural networks are portal nodes in the big intelligent farming system. The general insight architecture of the IoT-SDN gateway is presented in Figure 3. A gateway-based connection hub with internal networks is embedded by an operating system. A portal is the complete form of a number of devices essential for the system's interoperability as system translators. Sensing [27] devices connected with this gateway are smartly controlled by defining the devices' functionality.

OpenFlow as an SDN and LoRa as IoT communication protocols describe the routing rule system [28,29]. These protocols permit the transfer of information through any physical quantity between two or more communication nodes. If one device communicates with the others, they comply with the gateway protocol rules. The tracking module monitors the entire system with its operating system. The external devices are connected to the home network according to the algorithmic structure. All of the communication among the IoT-based smart devices and the network information management is stored in the database. SDN is deployed with the IoT devices for the foreign device's control [30,31]. Thus, the SDN based IoT gateway has been established, where SDN plays a network management role over the IoT devices [32]. The foreign devices are managed based on this intelligent farming gateway system. When the foreign devices are hired in the smart farming system, the devices are joined according to the algorithm structure setting based on that farming system. If these devices are not joined by a proper method, these devices will be rejected or released to load the embedded operating system. Completing the registration process, the foreign devices load the embedded operating system with smart farming. Since a farming loaded operating system is enabled in these foreign devices, it must be controlled by a farming system. The monitoring module monitors the foreign with the help of a tracking module. The gateway module will help to exchange data among the foreign devices and home devices.

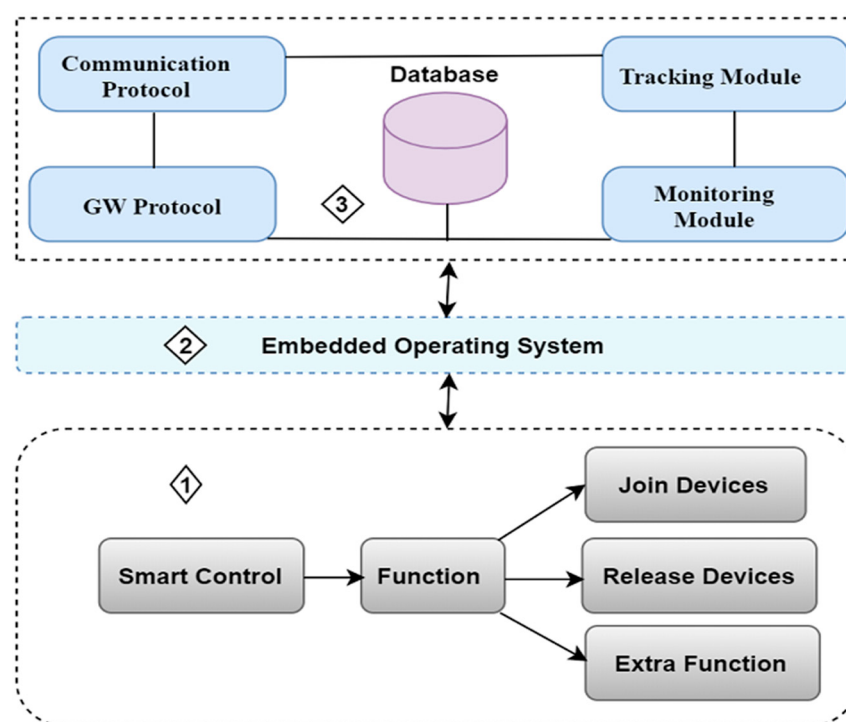


Figure 3. Architectural view of the IoT-SDN smart gateway.

3.4. Proposed Algorithm

Since the intelligent gateway is designed to manage the foreign agent, we have to set the operational functionality. The administrator of the PA defines the rules to access resources inside the farm. The Algorithm 1 has been integrated with the IoT-SDN gateway. The network administrator defines the execution time, speed, and acceptable delay of each foreign device. The Algorithm 1 is described as follows:

Algorithm 1: Proposed Foreign Agent Selection Algorithm

Input: Number of External Devices (E), Registered with Password (R), Operational Time (T), Operational Speed (S) and Acceptable Delay (D)

Output: Foreign Agent Selection, Time and Delay

```

1: Initialize the Variables
2: while (1) do
3:   T[0] ← T //Initialize Time
4:   S[0] ← S //Initialize Speed
5:   D[0] ← D //Initialize Acceptable Delay
6:   Time = 0 //Initial total execution time
7:   Delay = 0 //Initial total delay
8:   for i ← 1 to E do
9:     if (PW[i] != R) then
10:      PW[i] ← R
11:     end if
12:     if (T[i] != T[0] and S[i] != S[0] and D[i] != D[0]) then
13:      T[i] ← T //Update Time
14:      S[i] ← S //Update Speed
15:      D[i] ← D //Update Acceptable Delay
16:      FA [i] ← E[i] //Foreign Agent Selection
17:      PA[i] ← PA[i] + E[i]
18:     else
19:      FA [i] ← E[i] //Foreign Agent Selection
20:      PA[i] ← PA[i] + E[i]
21:     end if
22:     Time ← Time + T[i] * S[i]
23:     Delay ← Delay + D[i]
24:   return FA[i] //Return Selected Foreign Agent
25: end for
26: Timeavg = Time/E
27: Delayavg = Delay/E
28: end while

```

At first, the algorithm initializes the measurement criteria like time, speed, and acceptable delay for the foreign devices. Then, it checks whether the external device is registered or not. If it is already registered, the password has been discarded for loading existing resources. Otherwise, it provides the suggestion of foreign devices for completing the registration and loading the operating system of existing PA farming. When these devices are loaded with the operating system of PA farming, it successfully allowed for accessing the farming information and returning the selected foreign agent. Otherwise, the rejection function will be active for these foreign agents. It also checks the criteria for successful attachment with the PA. Cumulative time and delay have been stored and averaged to measure the network performance. Based on the implementation of this algorithm, the overall network performance has been discussed in the Results section.

3.5. Mechanical Modification

We proposed a model that was described in Figure 1 to solve intellectual property theft in precision farming. Figure 1 shows that the device is controlled by the IoT-SDN gateway. This control hub carries out the overall PA monitoring system. If a foreign device needs to be employed in the farming system, this device must be adapted based on the owner's need. Consequently, these devices work due to the control plate system perfectly, and there is no information leakage. Therefore, our proposed PA is a management system for all controllable foreign devices depicted in Figure 4. The functional requirements are imposed on the guest device through the proposed algorithm whenever the algorithm executes the operational behavior that is stored in the memory. Thus, the explosion probability of the information is reduced. It can rarely guarantee a positive outcome by securely determining the overall system performance.

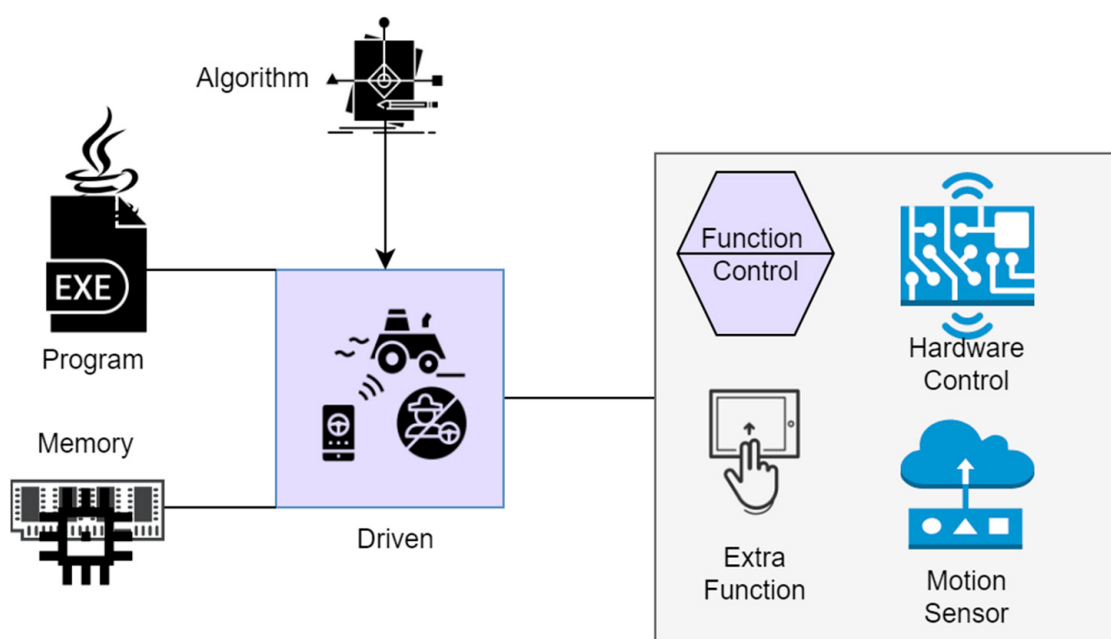


Figure 4. Modified mechanical design of PA.

3.6. SDN Implementation

Whenever the IoT-SDN gateway forwards the information toward the network layer, it deals with further remote monitoring, traffic control, routing, and so on. Apart from this, SDN decouples the data plane from the control plane compared to the traditional network scheme [19,20]. The data plane forwards the packet according to the instruction from the control plane. The control plane consists of the network operating system (NOS). This controller is integrated with northbound API for traffic control, routing table, and security concerns. The upper layer of the control plane is known as the application plane. Applications are applied for future network virtualization. Figure 5 presents the visual representation of the overall operational functionality of SDN. Since SDN decouples the control plane from the data plane, the networking devices are performing as forwarders. They only execute the instructions from the control plane. The control plane consists of the network operating system installed in a network controller. Well defined API is used to execute the required operation of the end user. The API is placed in the application plane. It acts as a bridge among the users and the SDN network. Packet monitoring, routing, mobility, accounting, authentication, and security operations are done by the API.

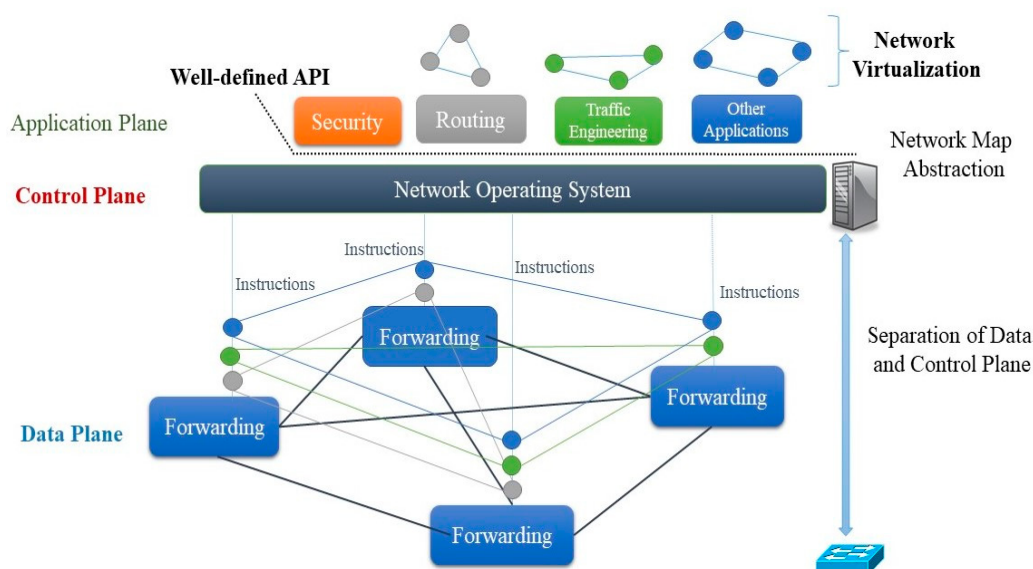


Figure 5. General architecture of a software defined network.

4. Evaluation and Results Analysis

This section describes the simulation and result analysis of the proposed framework. It will cover the simulation environment, architecture, and performance measurement metrics.

4.1. Environmental Setup

An Intel Core-i5 based Central Processing Unit (CPU) with 2.11 GHz processing speed and 8 GB RAM has been used to set up the simulation environment. In addition, a 64-bit Ubuntu (18.04) operating system was used for virtually designing the network architecture. Three different sizes of network clusters are considered for the performance analysis. At first, 25 nodes were used for deploying the proposed network architecture. Then, the network added another 25 nodes as a medium-size network. Finally, the network performance has been analyzed for 100 nodes. Mininet Wi-Fi as a simulator and Ryu as a controller are used for the simulation to create the virtual network. OpenFlow is used as a two-way communication protocol. After deploying the network, Wireshark was used to capture the packets of the virtual network. Then, the network performance is visually represented by using MATLAB (2020a). The remaining simulation parameters are shown in Table 2.

Table 2. Simulated parameters setting for the network architecture.

Parameters	Parameter Values
Simulator	Mininet WiFi
Simulation Area	300 m × 300 m
Number of Nodes	1–100
SDN Controller	1
OpenFlow Switches	5
Gateway	1
Simulation Times	120 s
Data Rate	110 Kbps
Routing Protocol	OpenFlow
Measurement Metrics	Throughput, Round Trip Time (RTT), Cumulative Distribution Function (CDF), Jitter and Packet Error Rate (PER)

4.2. Network Configuration

To analyze the proposed framework, a small size single controller-based PA has been considered for first tire simulation. Figure 6 presents the topological view of a small smart farm installed with some basic sensors and monitoring control. Three access points are connected with the internet. The SDN controller is set to the network administration building. The farm owner can monitor the PA system from his own residence.

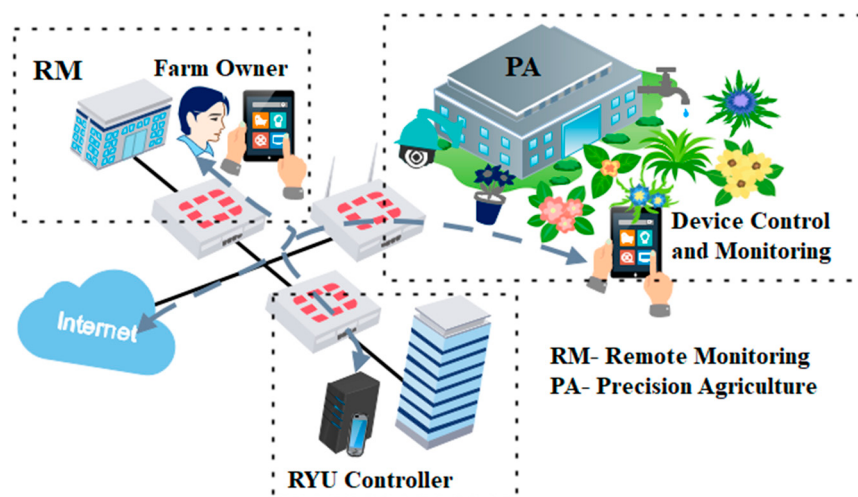


Figure 6. Single controller based network topology of precision agriculture.

Figure 7 presents the graphical visualization of the simulated network. Access point 2 is connected with the controller depicted by sta1. The mobile monitoring host inside the farm is associated with access point 4, indicated by sta2. Since the network nodes are mobile, mobility frequency has been set to 0.1, 0.25, 0.50, and 0.75 in several time simulations. Only two mobilities 0.25 and 0.50 have been presented in Figure 6 concerning a and b.

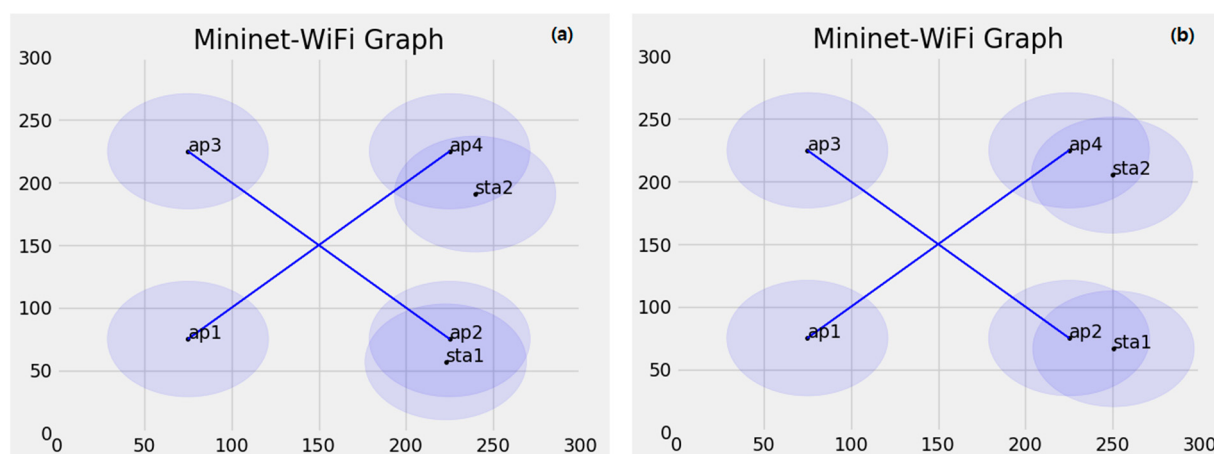


Figure 7. Simulation of SDN network along with mobility. (a) mobility frequency 0.25 and (b) mobility frequency 0.50.

4.3. Performance Matrices

Analysis of the performance, i.e., throughput, RTT, CDF, jitter, and PER based on the mobility of the proposed framework, has been calculated and described as QoS matrices. Iperf (command) is used to measure the performance of the network. Based on our proposed algorithm, we have calculated the throughput and RTT for measuring the network performance. Drone and foreign devices are moveable in their operational behaviors.

Thus, we have to consider the impact of mobility on the network. As a result, we have measured the CDF, Jitter, and PER with another mobile network containing multiple controllers' domains [26]. Four different mobile frequencies, 0.1, 0.25, 0.5, and 0.75, have been considered for performance comparison.

A. Throughput

The successful data transfer rate from source to destination is known as throughput. We have simulated our proposed architecture based on small, medium, and large size of the network including 25, 50, and 100 nodes. Throughput is calculated by Equation (1):

$$\text{Throughput} = \text{Number of Packets/Time} \quad (1)$$

The higher the throughput and the lower the RTT complies, the better the network performance. Figure 8 represents the average throughput of the proposed network for three different clusters. Figure 7 shows that the smallest cluster gives the best throughput compared to the medium and the most extensive sized network. However, in the broader sense, the difference in the throughput is negligible. The throughput of medium and large size networks is almost identical. An acceptable throughput is slightly reduced for larger size network nodes in our architecture.

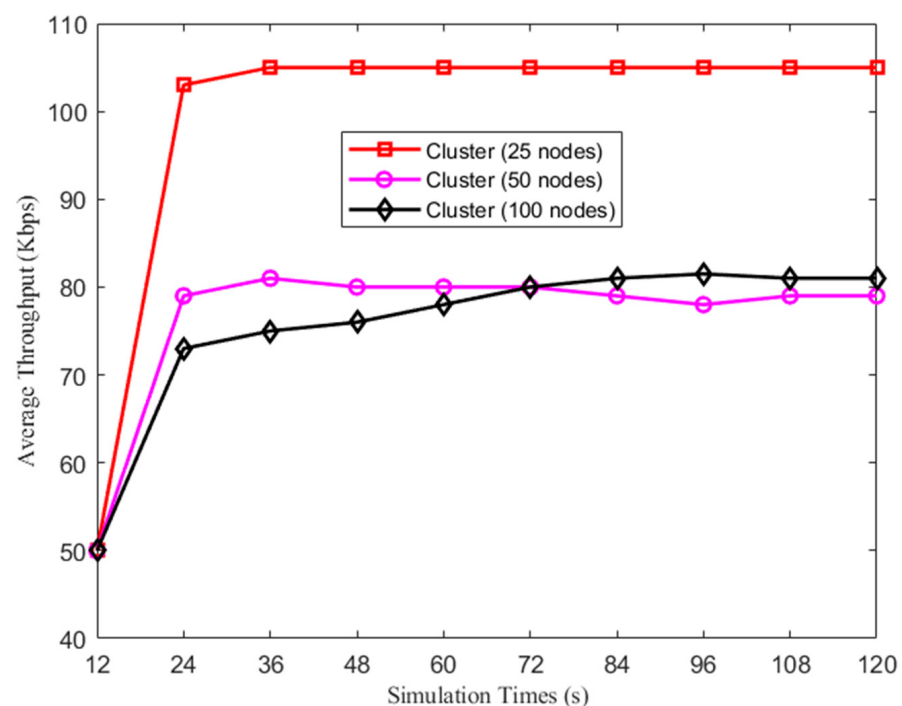


Figure 8. Average throughput comparison among 25, 50, and 100 nodes.

B. Round Trip Time

Round trip time is one of the significant measurements parameters of any network architecture. In our proposed framework, the session time between the home agents and the foreign agents have been considered for RTT. If any session has already been established before joining any foreign agent, the time has been marked as previous RTT. RTT is obtained as Equation (2):

$$RTT = (1 - \alpha) \times \text{previousRTT} + \alpha \times \text{PresentRTT} \quad (2)$$

where α is constant weight factor.

Figure 9 represents the RTT for 25, 50, and 100 node network architecture. RTT is the time calculated with the summation of the packet requested by the sender and

the acknowledgement provided by the receiver. RTT is increased proportionally with the simulation time. The RTT of the small and medium-size networks is nearly similar. However, the RTT is very high for an extensive sized network.

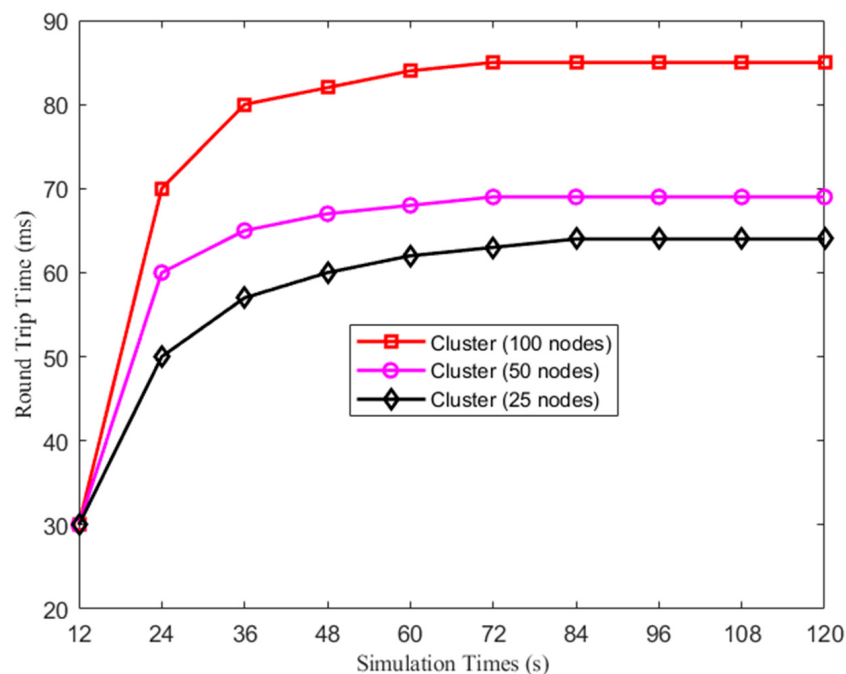


Figure 9. Round trip time comparison among 25, 50, and 100 nodes.

C. Cumulative Distribution

Since the foreign agent will be hired, mobility needs to be considered for performance measurement. Hence, the cumulative distribution function (CDF) represents the geometric distribution of the packet handled per second with the corresponding probabilities. Four different frequently used possibilities of mobility frequencies have been shown in Figure 10. The figure shows that the distribution's efficiency decreases with the increasing number of packets. CDF has been calculated using Equation (3):

$$y = F(x|p) = 1 - (1 - p)^{x+1} \quad (3)$$

$$x = 0, 1, 2 \dots n$$

where p is the probability of success.

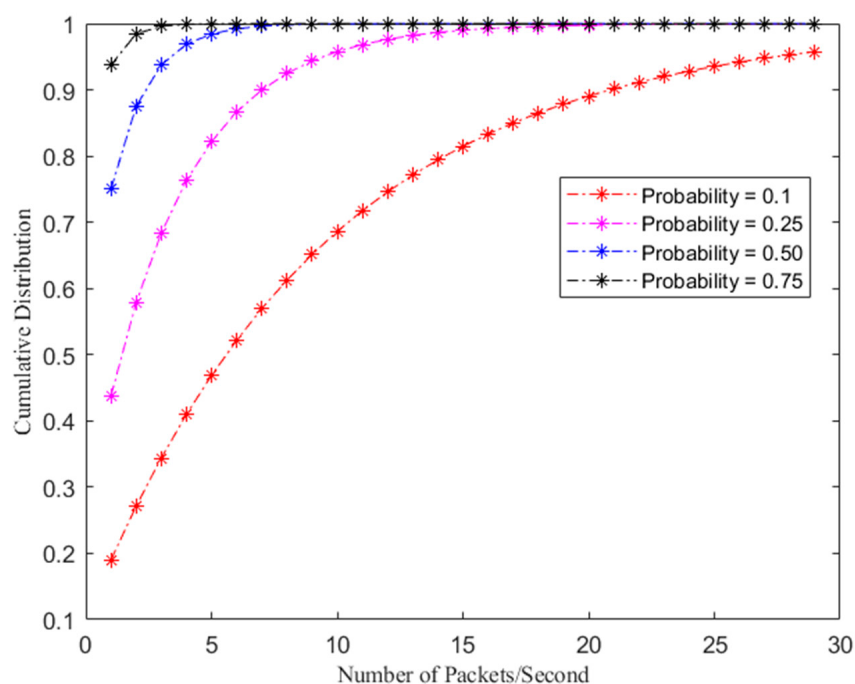


Figure 10. Cumulative distribution with probability 0.1, 0.25, 0.50, and 0.75.

D. Jitter

The delay variations are known as jitter. The jitter of the network architecture has been presented in Figure 11. More than 150 packets have been captured and considered for jitter calculation in a microsecond. The y -axis represents the jitter corresponding to the packet number depicted on the x -axis. Since mobility was one of the challenging issues for the proposed architecture, we have shown the jitter comparison with [26]. Higher jitter is decreasing the network performance. The figure represents that our proposed network architecture facilitated lower jitter than the network simulated in [26].

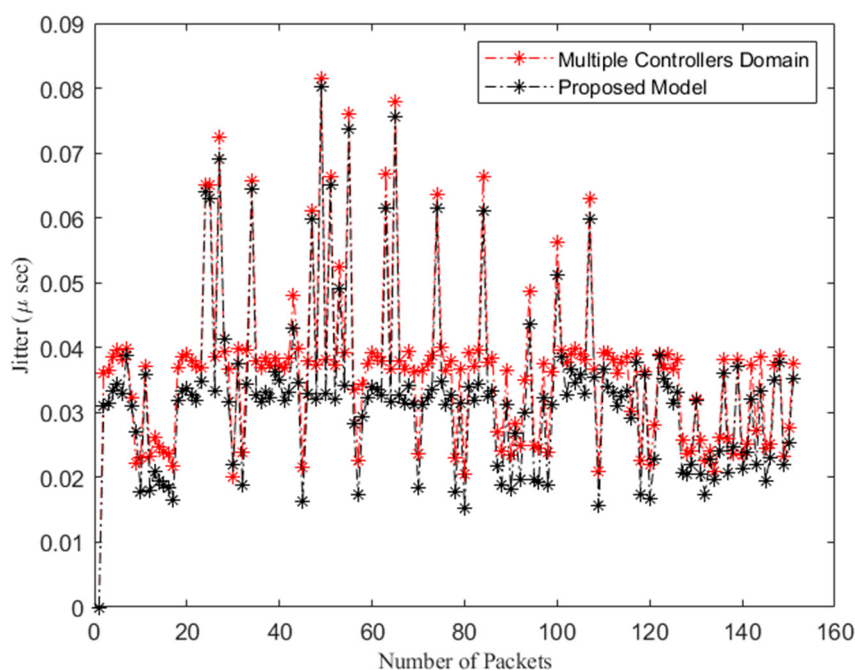


Figure 11. Jitter (packet delay variations) comparison of proposed architecture.

E. Packet Error Rate

The ratio of error packets over the total number of transmitted packets in a network is termed packet error rate (PER). Our proposed PA is implemented in a single IoT-SDN controller domain. Since foreign devices are moveable, the mobility frequencies of 0.1, 0.25, 0.50, and 0.75 PER have been compared with the multiple controllers' environment [26]. Figure 12 presented the comparative PER among single and various controllers. At the time of handling the session handover, PER increased with the increasing mobility frequency. The figure clearly shows that our proposed PA reduces the PER by around 3.53% compared to the multiple controllers. PER is calculated by Equation (4):

$$PER = \frac{\text{Error Packets}}{\text{Transmitted Packets}} \cdot 100\% \quad (4)$$

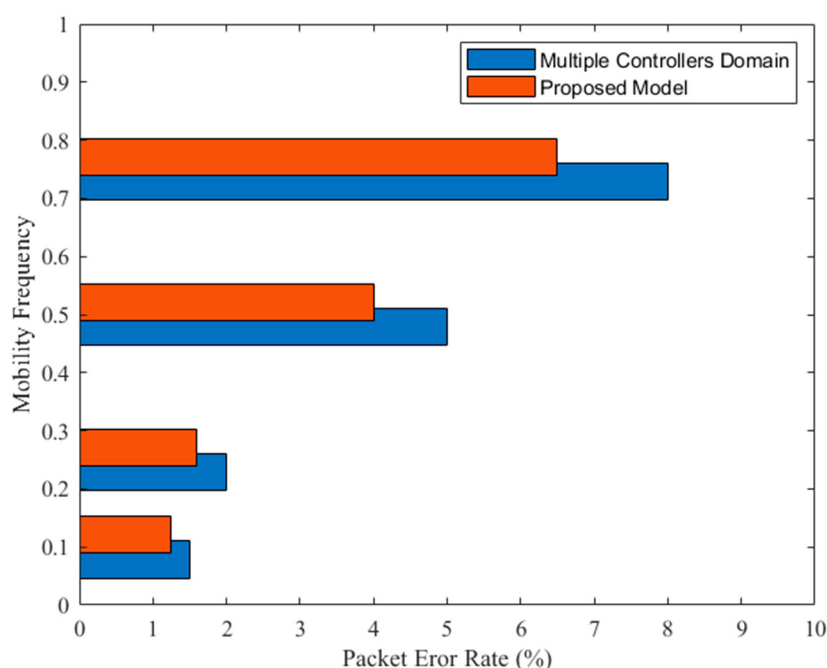


Figure 12. Packet error rate (PER) comparison of proposed architecture.

F. Quantitative Error Rate Comparison with Existing Works

Since mobility has been considered for handling the moveable devices, we have compared our proposed model with multiple controllers' domain. We have reduced the error rate 3.53% on average in four different mobile frequencies. The error rate varies with the implemented technology and the protocol. Several researchers have done their research on PA implementing both IoT and SDN. Frequently used OpenFlow, MQTT, EADC, CHP, and LoRa protocols have been considered for comparison with our proposed model. Our proposed model reduces the error rate (1.66~6.46)% compared to the other protocols. A comprehensive comparison of the error rate of our proposed model has been compared in Table 3.

Table 3. Comparison of error rate for the use of different protocol.

Author	Technology	Protocol	Error Type	Error Rate
M. H. Rahman et al. [26]	SDN	OpenFlow	Packet	6.87%
R. Shete et al. [33]	IoT	MQTT	Information	8.65%
A. S. Hosen et al. [34]	IoT	EADC	Packet	9.8%
		CHP		9.23%
J. Jin et al. [35]	IoT	LoRa	Information	5.7%
E. Boonchieng et al. [36]	IoT + NETPIE	MQTT	Information	5%
Proposed	IoT + SDN	LoRa + OpenFlow	Packet	3.34%

5. Conclusions and Future Work

Geospatial skills help to develop more efficient and effective methods of farming. They are used for the analysis of soil data and crop health from afar and cover large areas simultaneously. These technologies can contribute to the improvement of food production and safety throughout the world. Efficient management of resources and persistent and timely monitoring of crop health are more and more critical. Specific areas where PA may be at risk or vulnerable are increasingly connected to the Internet and other equipment. The final area of device corruption is now widely recognized as a danger in many institutions.

Consequently, we have proposed a smart IoT-SDN gateway control system that will ensure the authenticity of foreign devices since IP rights are very sensitive pieces of information in a PA system. A smart hub will be used to perform the overall PA monitoring system. If new guest equipment or external devices are to be hired for this agricultural system, they must be tailored to our needs. Therefore, these devices work following the control plate system perfectly, and there is no information leakage. Our plan is to add a blockchain to this research work.

Author Contributions: Conceptualization, M.S.H. and M.S.R.; methodology, M.S.H. and M.H.R.; software, M.S.H. and M.H.R.; validation, M.S.H., M.H.R. and M.S.R.; formal analysis, M.S.H., M.H.R. and M.S.R.; writing—original draft preparation, M.S.H., M.H.R. and M.S.R.; writing—review and editing, M.S.R. and A.S.M.S.H.; visualization, M.S.H. and M.H.R.; supervision, M.S.R.; project administration, C.S. and G.H.C.; funding acquisition, C.S. and G.H.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2021R1F1A1059840), and Institute of Information and Communications Technology Planning and Evaluation (IITP) grant by the Korea government through MSIT (No. 2021-0-00511, research on robust AI, and distributed attack detection for edge AI security).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.
2. Zhang, X.; Davidson, E.A. Improving nitrogen and water management in crop production on a national scale. *Am. Geophys. Union* **2018**, *2018*, B22B-01.
3. Mekala, M.S.; Viswanathan, P. A survey: Smart agriculture IoT with cloud computing. In Proceedings of the 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS), ICMDCS'17, Vellore, India, 10–12 August 2017; pp. 1–7.
4. Hossain, S.; Waheed, S.; Rahman, Z.; Shezan, A.; Hossain, M. Blockchain for the security of internet of things: A smart home use case using ethereum. *Int. J. Recent Technol. Eng.* **2020**, *8*, 4601–4608. [\[CrossRef\]](#)
5. Singh, S.; Hosen, A.S.; Yoon, B. Blockchain security attacks, challenges, and solutions for the future distributed IoT network. *IEEE Access* **2021**, *9*, 13938–13959. [\[CrossRef\]](#)
6. Rathee, G.; Sharma, A.; Iqbal, R.; Aloqaily, M.; Jaglan, N.; Kumar, R. A blockchain framework for securing connected and autonomous vehicles. *Sensors* **2019**, *19*, 3165. [\[CrossRef\]](#) [\[PubMed\]](#)

7. Hosen, A.S.M.S.; Sharma, P.K.; Cho, G.H. MSRM-IoT: A reliable resource management for cloud, fog and mist assisted IoT networks. *IEEE Internet Things J.* **2021**. [\[CrossRef\]](#)
8. Islam, N.; Farhin, F.; Sultana, I.; Kaiser, M.S.; Rahman, M.S. Towards machine learning based intrusion detection in IoT networks. *Comput. Mater. Contin.* **2021**, *69*, 1801–1821. [\[CrossRef\]](#)
9. Rahman, A.; Hossain, S.; Rahman, Z.; Shezan, S.A. Performance enhancement of the internet of things with the integrated blockchain technology using RSK sidechain. *Int. J. Adv. Technol. Eng. Explor.* **2019**, *6*, 257–266. [\[CrossRef\]](#)
10. Charania, I.; Li, X. Smart farming: Agriculture's shift from a labor intensive to technology native industry. *Internet Things* **2020**, *9*, 100142. [\[CrossRef\]](#)
11. Alexandratos, N.; Bruinsma, J. *World Agriculture towards 2030/2050: The 2012 Revision*; ESA Working Paper Rome; FAO: Rome, Italy, 2012.
12. Ahmed, N.; De, D.; Hussain, I. Internet of things (IoT) for smart precision agriculture and farming in rural areas. *IEEE Internet Things J.* **2018**, *5*, 4890–4899. [\[CrossRef\]](#)
13. Hossen, S.; Rahman, H.; Mustanjid, A.; Nobin, A.S.; Habib, A. Enhancing quality of service in SDN based on multi-path routing optimization with DFS. In Proceedings of the 2019 International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh, 24–25 December 2019.
14. Maksymyuk, T.; Dumych, S.; Brych, M.; Satria, D.; Jo, M. An IoT based monitoring framework for software defined 5G mobile networks. In Proceedings of the Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication, Beppu, Japan, 5–7 January 2017.
15. Psannis, K.E.; Stergiou, C.; Gupta, B.B. Advanced media-based smart big data on intelligent cloud systems. *IEEE Trans. Sustain. Comput.* **2018**, *4*, 77–87. [\[CrossRef\]](#)
16. Fastellini, G.; Schillaci, C. Precision farming and IoT case studies across the world. In *Agricultural Internet of Things and Decision Support for Precision Smart Farming*; Academic Press: Cambridge, MA, USA, 2020; pp. 331–415.
17. Song, H.; Zhang, D.; Jara, A.; Wan, J.; Boussetta, K. IEEE access special section editorial: Smart cities. *IEEE Access* **2016**, *4*, 3671–3674. [\[CrossRef\]](#)
18. Lee, M.; Hwang, J.; Yoe, H. Agricultural production system based on IoT. In Proceedings of the 2013 IEEE 16th International Conference on Computational Science and Engineering, Sydney, NSW, Australia, 3–5 December 2013; pp. 833–837.
19. Sharma, P.K.; Singh, S.; Jeong, Y.-S.; Park, J.H. DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks. *IEEE Commun. Mag.* **2017**, *55*, 78–85. [\[CrossRef\]](#)
20. Mukherjee, B.K. An SDN based distributed iot network with nfv implementation for smart cities. In *International Conference on Cyber Security and Computer Science*; Springer: Cham, Switzerland, 2020.
21. Wang, Y.; Bi, J. A solution for IP mobility support in software defined networks. In Proceedings of the 2014 23rd International Conference on Computer Communication and Networks (ICCCN), Shanghai, China, 4–7 August 2014.
22. Islam, M.J. Distblacknet: A distributed secure black sdn-iot architecture with nfv implementation for smart cities. In Proceedings of the 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox's Bazar, Bangladesh, 7–9 February 2019.
23. Rahman, A. Distblockbuilding: A distributed blockchain-based sdn-iot network for smart building management. *IEEE Access* **2020**, *8*, 140008–140018. [\[CrossRef\]](#)
24. Le, L.V.; Do, S.; Lin, B.-S.P.; Tung, L.-P. Big Data and Machine Learning Driven Open5GMEC for Vehicular Communications. *Trans. Networks Commun.* **2018**, *6*, 103. [\[CrossRef\]](#)
25. Cauteruccio, F.; Cinelli, L.; Corradini, E.; Terracina, G.; Ursino, D.; Virgili, L.; Savaglio, C.; Liotta, A.; Fortino, G. A framework for anomaly detection and classification in Multiple IoT scenarios. *Future Gener. Comput. Syst.* **2021**, *114*, 322–335. [\[CrossRef\]](#)
26. Rahman, H.; Islam, N.; Swapna, A.I.; Habib, A. Analysis of software defined wireless network with IP mobility in multiple controllers domain. In *International Conference on Cyber Security and Computer Science*; Springer: Cham, Switzerland, 2020.
27. Hosen, A.S.M.S.; Singh, S.; Mariappan, V.; Kaur, M.; Cho, G.H. A secure and privacy preserving partial deterministic RWP model to reduce overlapping in IoT sensing environment. *IEEE Access* **2019**, *7*, 39702–39716. [\[CrossRef\]](#)
28. Kim, H.; Feamster, N. Improving network management with software defined networking. *IEEE Commun. Mag.* **2013**, *51*, 114–119. [\[CrossRef\]](#)
29. McKeown, N. OpenFlow: Enabling innovation in campus networks. *ACM SIGCOMM Comput. Commun. Rev.* **2008**, *38*, 69–74. [\[CrossRef\]](#)
30. Bhandari, K.S.; Hosen, A.S.M.S.; Cho, G.H. CoAR: Congestion-aware routing protocol for low power and lossy networks for IoT applications. *Sensors* **2018**, *18*, 3838. [\[CrossRef\]](#) [\[PubMed\]](#)
31. Caraguay, V.; Leonardo, A. SDN: Evolution and opportunities in the development IoT applications. *Int. J. Distrib. Sens. Netw.* **2014**, *10*, 735142. [\[CrossRef\]](#)
32. Hosen, A.S.M.S.; Cho, G.H. An energy centric cluster-based routing protocol for wireless sensor networks. *Sensors* **2018**, *18*, 1520. [\[CrossRef\]](#) [\[PubMed\]](#)
33. Shete, R.; Agrawal, S. IoT based urban climate monitoring using Raspberry Pi. In Proceedings of the 2016 International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, India, 6–8 April 2016; pp. 2008–2012.
34. Hosen, A.S.; Singh, S.; Sharma, P.K.; Rahman, M.S.; Ra, I.H.; Cho, G.H.; Puthal, D. A QoS-aware data collection protocol for LLNs in fog-enabled internet of things. *IEEE Trans. Netw. Serv. Manag.* **2019**, *17*, 430–444. [\[CrossRef\]](#)

-
35. Jin, J.; Ma, Y.; Zhang, Y.; Huang, Q. Design and implementation of an agricultural IoT based on LoRa. In Proceedings of the MATEC Web of Conferences, Beijing, China, 18–25 May 2018; Volume 189, p. 04011.
 36. Boonchieng, E.; Chieochan, O.; Saokaew, A. Smart farm: Applying the use of NodeMCU, IOT, NETPIE and LINE API for a Lingzhi mushroom farm in Thailand. *IEICE Trans. Commun.* **2018**, *101*, 16–23. [[CrossRef](#)]