Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 9970942, 14 pages
https://doi.org/10.1155/2021/9970942

WILEY | Hindawi

Research Article

Design and Performance Analysis for Edge Intelligence-Based F-PMIPv6 Mobility Support for Smart Manufacturing

Donghyun Kim, ByungJun Park, Junhyung Moon, Jaeen Lee, and Jongpil Jeong

Department of Smart Factory Convergence and Physical Science Research Institute, Sungkyunkwan University, Suwon 16419, Republic of Korea

Correspondence should be addressed to Jongpil Jeong; jpjeong@skku.edu

Received 14 March 2021; Accepted 31 May 2021; Published 24 June 2021

Academic Editor: Yong Zhang

In this paper, we propose a new mobility management network, i-FP, to be used in the smart factory that continues to develop in the Fourth Industrial Revolution. i-FP was created to solve the current local mobility management problem of legacy frameworks. MN (mobile node) refers to a mobile device in a manufacturing environment that includes workers, production facilities, and AGV. To allow mobile nodes (MNs) to move from one domain to another, i-FP uses three network entities: LFA (Local Factory Anchor), FAG (Factory Access Gateway), and MN, as an extended concept of PMIPv6. Among the three network entities in i-FP, LFA and FAG can act as edge intelligence devices to reduce the handover latency of the MNs. i-FP also uses IP header-swapping mechanisms to prevent traffic overhead and enhance network throughput. We evaluate new framework i-FP, PMIPv6, and HMIPv6, which are legacy protocols of local mobility management, in various ways and evaluate three schemes. We confirm that i-FP works better than do the other network methods used in the smart factory.

1. Introduction

Globally, countries are rapidly changing in the Fourth Industrial Revolution. The governments of major countries are striving to become leaders of the Fourth Industrial Revolution by means of differentiated policy support. In particular, manufacturing-based companies are focusing on changes to upgrade their general factories to smart factories. Various research attempts are made on existing manufacturing processes, such as Cyber Physics System (CPS) [1, 2], robotics, 3D printing, edge computing, and cyber-security technologies [3]. Because these key technologies are applied across all manufacturing areas, innovations are emerging that dramatically increase the competitiveness of manufacturing.

Edge computing has become an integral part of the smart factory that emerged with the development of cloud computing. Edge computing became edge intelligence, where research was conducted on how AI (Artificial Intelligence) delivers data analysis [4]. Accordingly, data gathering uses wired and wireless methods for data analysis, and it is a recent trend that it is designed wirelessly to allow flexible movement of workers, mobile shelves, and production facilities in the smart factory [5, 6]. Thus, in the manufacturing industry, wireless network connectivity continues to be a challenge. Wireless and mobile communication network technologies play a major role in creating diverse environments in manufacturing industries. With the growing importance for new wireless networks for the smart factory, new technologies have been developed, leading to the emergence of a variety of hierarchical mobility frameworks.

In wireless network frameworks, the mobility of users is typically divided into intradomain and interdomain movements. These mobilities correspond to the global mobility protocol [7] and the local mobility [8, 9] of the wireless network. Whereas the global mobility protocols maintain the connectivity to the factory beyond the scope of the domain as a user's movement, local mobility protocols operate through a distribution of the restricted region within the domain.

When a network user, who accesses and receives from a mobile network with IPv6 [10–12], accesses another network, the network transmits traffic from the original domain using the global mobility protocol to manage the network

that first access from the outside. It uses a local mobility protocol delivering traffic within a domain in succession, and enabling users can successfully communicate. Global and local mobility enables users to leverage seamless and flexible communication.

Global mobility protocols used to manage user mobility include F-PMIPv6 (Fast Proxy Mobile) [13, 14], HMIPv6 [15], TeleMIP [16], and HIP [17]. This paper focuses on the processes of global mobility and local mobility. Among the global mobility protocols, PMIPv6 [18, 19] and HMIPv6 [20] use traffic to locate target addresses in the network and to access top-level gateways. This is applied to the smart factory [21–24], which is divided into connecting the factory with the factory and connecting the mobile with the mobile. However, when applying the global mobility protocol to communications between adjacent mobile devices, the traffic is less efficient. We propose a new mobile network protocol to improve the problem of protocols in smart factories. The protocol to be used in the smart factory is i-FP, an acronym for "Intelligent Factory PMIPv6."

i-FP has three main objectives in total. (i) It provides routing services optimized for traffic in the domain. The routing optimization (RO) service enables rapid retrieval of communication paths between peers to deliver optimized traffic in the domain. (ii) It utilizes wireless links to reduce network traffic overhead. Efficient traffic management by wireless links can improve the performance of wireless networks, as the existing limited bandwidth overloads wireless applications. (iii) We introduce i-FP to reduce the cost to reduce the domain topology. We apply i-FP to the smart factory to improve the performance of existing applied local mobility protocols when connecting to the web. It adds IP header swap technology to prevent traffic overhead in the network. To evaluate the performance of i-FP, we compare the newly proposed framework with other frameworks related to the local mobility protocol. Based on the result, we prove that i-FP is an effective technique in the local domain of the smart factory.

In short, the key contributions of the study are provided as follows.

(i) Propose a new effective architecture, including gateways with edge intelligence capabilities within a smart factory environment

(ii) The proposed i-FP incorporates the architecture of HMIPv6 and PMIPv6, while leveraging IP swapping mechanisms to effectively reduce tunneling costs and latency

(iii) It is possible to effectively respond to mobility processing by performing what mobile nodes need to do directly on the gateway

(iv) Since protocol data is only transmitted over wired networks, i-FP does not generate signaling costs on wireless links, minimizing data loss and data costs on wireless links

(v) Finally, interactive connection of the factory cloud and the factory anchor within domains allows flexible management of the mobile nodes in the integrated system

In this paper, Section 2 introduces associated research, Section 3 discusses the architecture and procedures of the proposed framework, Section 4 evaluates the performance of the proposed technique, and Section 5 provides a conclusion based on performance evaluation results.

2. Related Work

In this section, we review existing research work related to our research to help readers understand the importance of mobile communication management and the latest technology trends in the smart factory. Convergence of IT and OT technologies is discussed in Smart Manufacturing Overview. In Edge Intelligence, we describe the edge computing that is the key technology applied to i-FP. Finally, we explain the FPMIPv6 and HMIPv6 which were used for mobility support in smart manufacturing.

2.1. Smart Manufacturing Overview. During the Fourth Industrial Revolution, the smart factory is becoming a very important element. General factories, consisting of production facilities, control systems, and factory management systems, are automated methods of the Third Industrial Revolution. With the advent of the Fourth Industrial Revolution, general factories are becoming smarter. Automation has been made intelligent by means of the fusion of IT and OT technologies [25], and intensive research is being conducted on data generation and analysis in terms of production facilities and production management by adding sensors and IoT technologies to production facilities [26, 27].

As illustrated in Figure 1, hyperconnections, digital integration, automation, integration, and data are keywords in smart factory fields. The collected big data is analyzed by AI technology or applied to machine learning. Robots cooperate with workers to add productivity, and IoT is used as a data collector. Based on technologies, the smart factory has been developed into an intelligent system that can achieve strategic goals, such as productivity, quality, and customer service in the entire production process, including design, development, manufacturing, distribution, and logistics [28]. To this end, various information exchanges by means of communication between devices and between devices and humans are essential for a smart factory, since the factory has centralized control over production facilities so far.

In order to establish a flexible production system of a smart factory, an organic response of production facilities is essential. Modular production equipment, as well as IoT technologies, can be changed according to the production process, so that production can be customized to meet consumer demands [29]. Development of mobile communication is essential for data communication and data analysis of this modular equipment.

2.2. Edge Intelligence. Edge intelligence (EI) is a concept that defines the communication, computing, and storage capabilities of a particular infrastructure that are closest to local unit users on a distributed network. The term "edge intelligence"

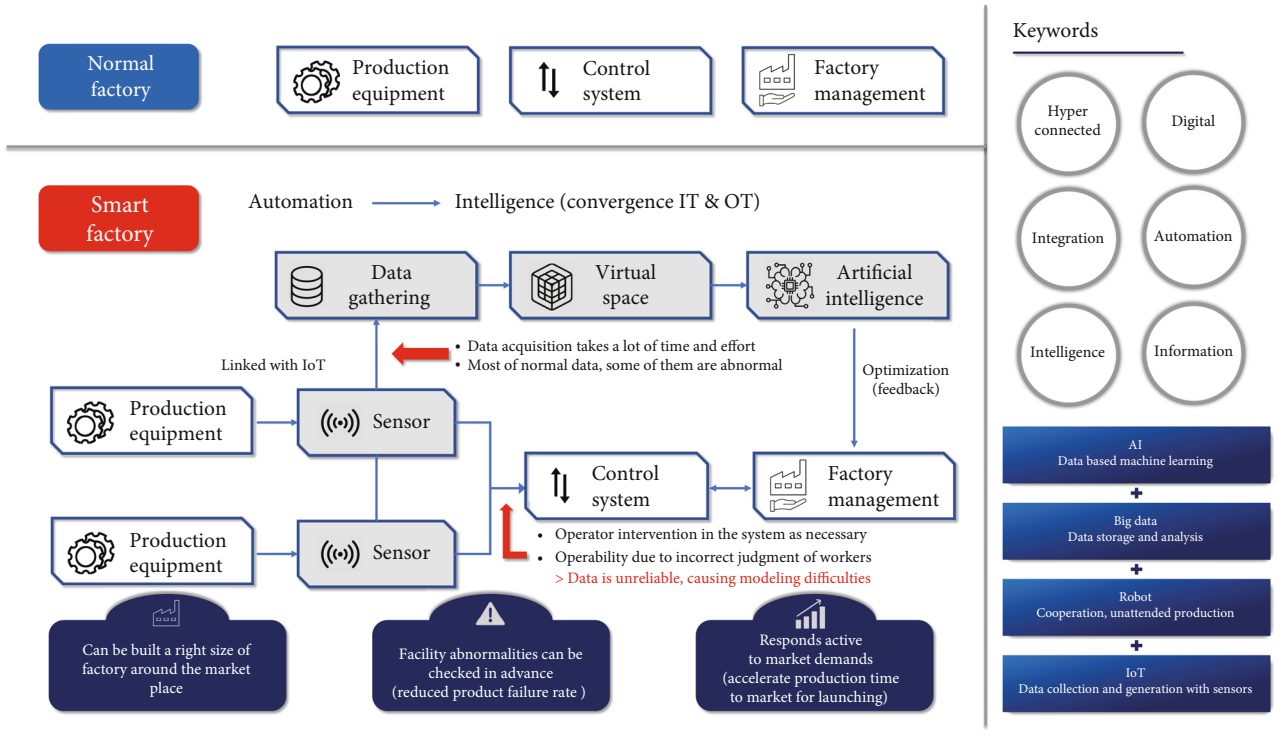


Figure 1: i-FP Architecture of Smart Factory.

was represented by Zhou et al.'s [4] research. "Edge" is a physical location representation in which data is generated and processed. In other words, an edge means that there is a control device and computing device. Recent research has shown that devices equipped with small computers are changing to IoT and IIoT. These devices operate with AI capabilities. Data processing devices in edge fields are used for intelligent collection of data, analysis, aggregation, and application. Edge intelligence uses edge computing [30] to support these edge devices in analysis performed on AI and ML models. Intelligent edges break traditional client-server models that are typically "double or thin" for clients, and servers are those that have the ability to process, analyze, and protect data.

Edge intelligence has three main entities: connectivity, computation, and control. This edge intelligence allows manufacturing systems to connect to each other over a wireless or wired network. This computing approach interconnects a specific range of workers, managers, smart facilities, robots, sensors, and AGVs and also applies to a wide range of connections, such as smart factory [31].

Fully connected edge intelligence systems can collect, manage, analyze, and archive large amounts of data through interdistributed computing. This local unit of computing can be combined with the cloud system to improve or replace computing power. Edge computing is performed mostly by edge servers (or IIoT gateways) that are part of IT equipment [32]. These servers can be half racks, two blades, or industrial embedded PCs. It is applicable to certain business services that require control of calculated insights from these local units and can also be extended to the cloud. Intelligent edges can perform control mechanisms for these local units and devices on the edges.

Cloud computing is a powerful solution if you want an Internet connection, but its use is very limited if it requires real-time data processing and communicating restrictions exist. Edge intelligence lets you keep some or all data close to where it was created, rather than sending it to a remote data center or cloud server for processing. Therefore, we want to intelligently manage communication to mobile devices moving within the smart factory by leveraging edge-computable entities [33].

2.3. Mobility Support for Smart Manufacturing. The FPMIPv6 is the "Fast Proxy Mobile IPv6" implementation of FMIPv6 in PMIPv6 environments, enabling high-speed handover. The mobile node (MN) detects mobile signals and preemptive Mobile Access Gateway (pMAG) for transport and prepares the MN's handover via HI (Handover Initiation) and HAck (Handover-Acknowledgement) messages. In the preparation phase, a bidirectional tunnel is formed between the pMAG and the new Mobility Access Gateway (nMAG). During the time when communication with MN is lost, data from LMA is buffered from pMAG to nMAG. When MN is connected to nMAG, packet data buffered by nMAG is sent to MN to prevent packet data loss due to separation during handover to facilitate communication. The mode of FPMIPv6 is divided into two: prediction and response.

In predictive handovers, the full handover begins by the MN detecting the need for handovers and delivering a handover indication message to the pMAG on its own. In reactive handover, on the other handovers, MN detects the need for handovers and performs a network reentry process directly into the target network, and handovers are initiated by

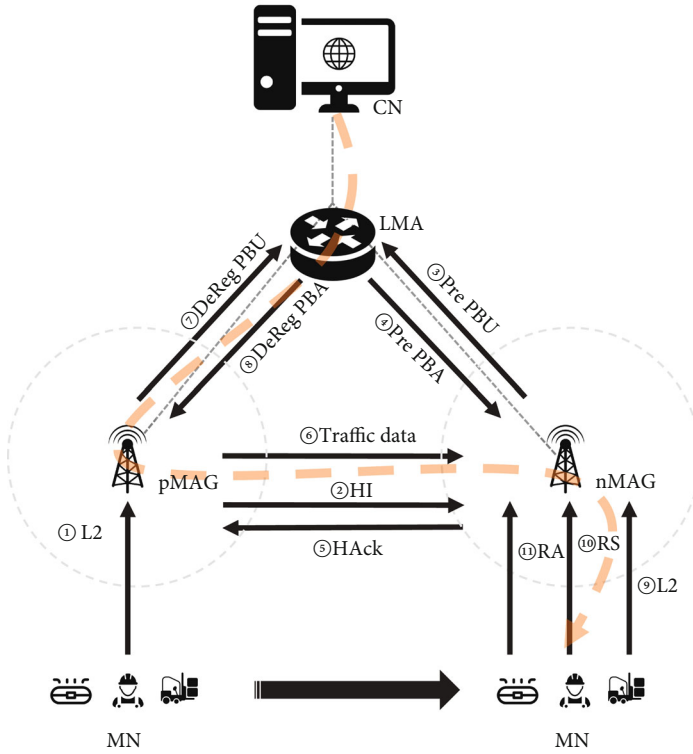


Figure 2: Handover process of FPMIPv6.

nMAG before pMAG recognizes the need for handovers. In a handover scenario, the MN basically uses a previable access network (pAN).

It is assumed that the situation is communicating with the pMAG. Before the MN moves, it sends a side message about moving to the pAN, including the information nAN MN-ID. Upon receipt of the message, the pAN sends HI messages, including MN-ID and nAN-ID, to the pMAG to inform the MN movement.

The pMAG transmits HI messages (including information from MN and LMA) to the nMAG. Upon receiving the HI message, the nMAG sends a HAck (Handover-Acknowledgement) to the pMAG. Upon receiving HAck messages, the pMAG forms a two-way tunnel with the nMAG. When a two-way tunnel is formed, the pMAG transmits packets stored in the MN to the nMAG and is stored in the nMAG buffer.

After the handover (L2), when the MN is connected to the nMAG, the MN sends packets from the nMAG and the nMAG binds the MN by sending a Proxy Binding Update (PBU) message to the LMA. After LMA receives a PBU message, it registers the status information of the MN in the Binding Cache Entry (BCE) and sends a Proxy Binding Acknowledgement (PBA) message to the nMAG. The binding process of MN is completed after the LMA has received a full PBA message over the nMAG. This content is schematized in Figure 2.

PMIPv6 is an IPv6-based mobility-enabled protocol for mobile nodes. The signal and routing state settings of the mobility node are performed by entities in the network. The main entities of PMIPv6 are MAG (Mobility Access Gateway) and LMA (Local Mobility Anchor). The role of LMA is responsible for the reachability of topology anchor points on mobile nodes and mobile node home network prefixes (HNP). The LMA manages information about MNs and has the right to manage topology anchor points for home network prefix information to be assigned to MN. MAG is the access link to which the mobile node is connected, and on behalf of the mobile node, it performs mobility management of the MN through the LMA and bidirectional passageways. MAG detects MN's entry and exit within the network and recommends binding registration tasks for LMA. The technique for supporting the mobility of MN in the network using the PMIPv6 protocol is shown in Figure 3.

Hierarchical Mobile IPv6 (HMIPv6) is a method proposed by the IETF (Internet Engineering Task Force) as a way to reduce the handover delay that occurs when a mobile node moves in MIPv6. HMIPv6 is a protocol that reduces signaling caused by handover of a mobile node by locally managing the movement of the mobile node and reduces the delay and signaling overhead caused by HMIPv6 during binding update. HMIPv6 requires a binding update to HA (home agent) and CN (Corresponding Node) when MN moves to another subnet.

If the MN is far from HA or CN, the binding update procedure causes unnecessary delay and signaling overhead. The access network is hierarchically structured in HMIPv6 to solve this problem. HMIPv6 can reduce signaling costs caused by user mobility and scalability in the growing network in managing local mobility and has separated global mobility management and local mobility. Global mobility is still managed by HMIPv6, but local mobility within the local

domain is managed from the MAP, which is a local mobility management agent. Therefore, since movement in the MAP region is unnecessary in HA and CN, the delay and signaling overhead in HMIPv6 needed to maintain or manage information about it can be greatly reduced. The contents are shown in Figure 4.

However, there are many protocols, such as CIP [34], HAWAII [35], HMIPv6, Tele MIP, RDMA [36], and PMIPv6. For example, CIP and HAWAII force a strict tree structure in the domain topology. The hierarchical structure is based on a mobility agent, and all routers must be involved in mobility signaling. Therefore, CIP and HAWAII are expensive to implement, because all routers in the domain need to be upgraded. Other protocols, such as HMIPv6, TeleMIP, RDMA, and PMIPv6, do not require the participation of all routers in mobility signaling. Instead, a mobility agent as a topology anchor point and an access router as an external agent are introduced. By means of the cooperation of the mobility agent and the access router, the above protocols can deliver traffic to the moving users in the local domain. Even though these protocols do not require much functionality within the domain topology, they suffer from severe routing problems with intradomain traffic. If a user attempts to send a packet to a peer communicating in the same domain, the packet is first delivered to the domain gateway router and forwarded to the peer with which the user is communicating.

Multimedia applications such as online games are popular nowadays, and triangular routing paths cause additional transmission delays and waste bandwidth resources. HMIPv6, RDMA, and TeleMIP share similar delivery procedures and mobility signaling. These protocols use the domain's special address for global mobility and binding of network-specific addresses for domain forwarding. HMIPv6, RDMA, TeleMIP, and PMIPv6 are not network-enabled mobility, and they use only one address for domain routing and binding. Network support schemes can help PMIPv6 to reduce signal cost.

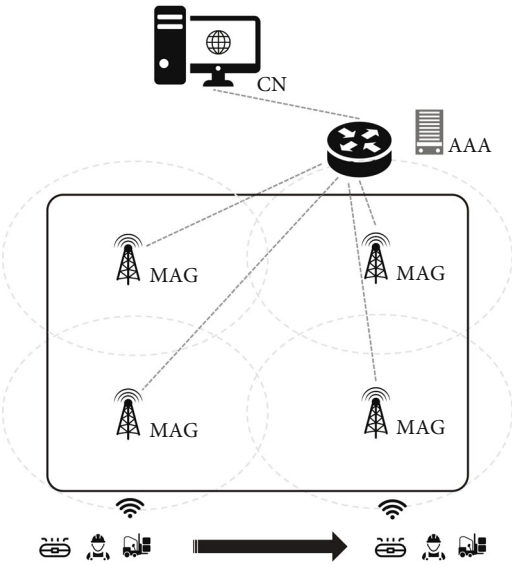


Figure 3: Handover Process of the PMIPv6.

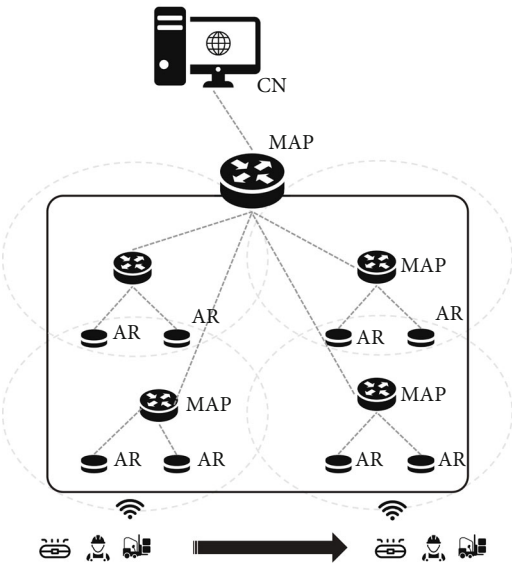


Figure 4: Concept of HMIPv6.

3. Edge Intelligence-Based Hierarchical Mobility Support for Smart Manufacturing

3.1. System Architecture. i-FP has four main entities, including the features of HMIPv6 and PMIPv6 to work better. i-FP contains four entities to enhance the network environment and performance of smart manufacturing using LFA, FAG, MN, and cloud. MN refers to mobile devices that include workers, production facilities, and AGV in the manufacturing environment, and LFA and FAG include the functions of edge intelligence. We propose the i-FP of a smart factory containing these major entities. The overall architecture can be found in Figure 5.

Various messages related to i-FP mobility support are used in the mobility management protocol. When analyzing mobility models, the following message sizes should be considered: MAG and LMA used in FPMIPv6 are used as the basis for FAG and LFA in i-FP. The first entity is LFA. The LFA performs the same role as the proxy home agent (HA) for MN. When MN is moved to the local domain, FAG receives traffic on behalf of MN and sends traffic to the link where MN is located. FAGs with edge computing function receive traffic on behalf of MN when MN is moved to the local domain and send traffic to MN's location link.

To make this possible, i-FP uses two types of addresses, RCoA (Regional Care of Address) and LCoA (Link Care of Address), which are the same way as HMIPv6 manages the MN. RCoA is the address obtained from MN when MN first enters the local domain. The address obtained from MN, RCoA, serves as the ID card for MN in the local domain. The MN also displays the location via the RCoA and updates HA or peers in communicating. If the MN moves within the local domain, the RCoA remains fixed. Therefore, it is not necessary for MN to send once binding update messages to HA or peers during communicating that does not deviate from the local domain. However, for this reason, RCoA can identify the domain in which MN is located but is not

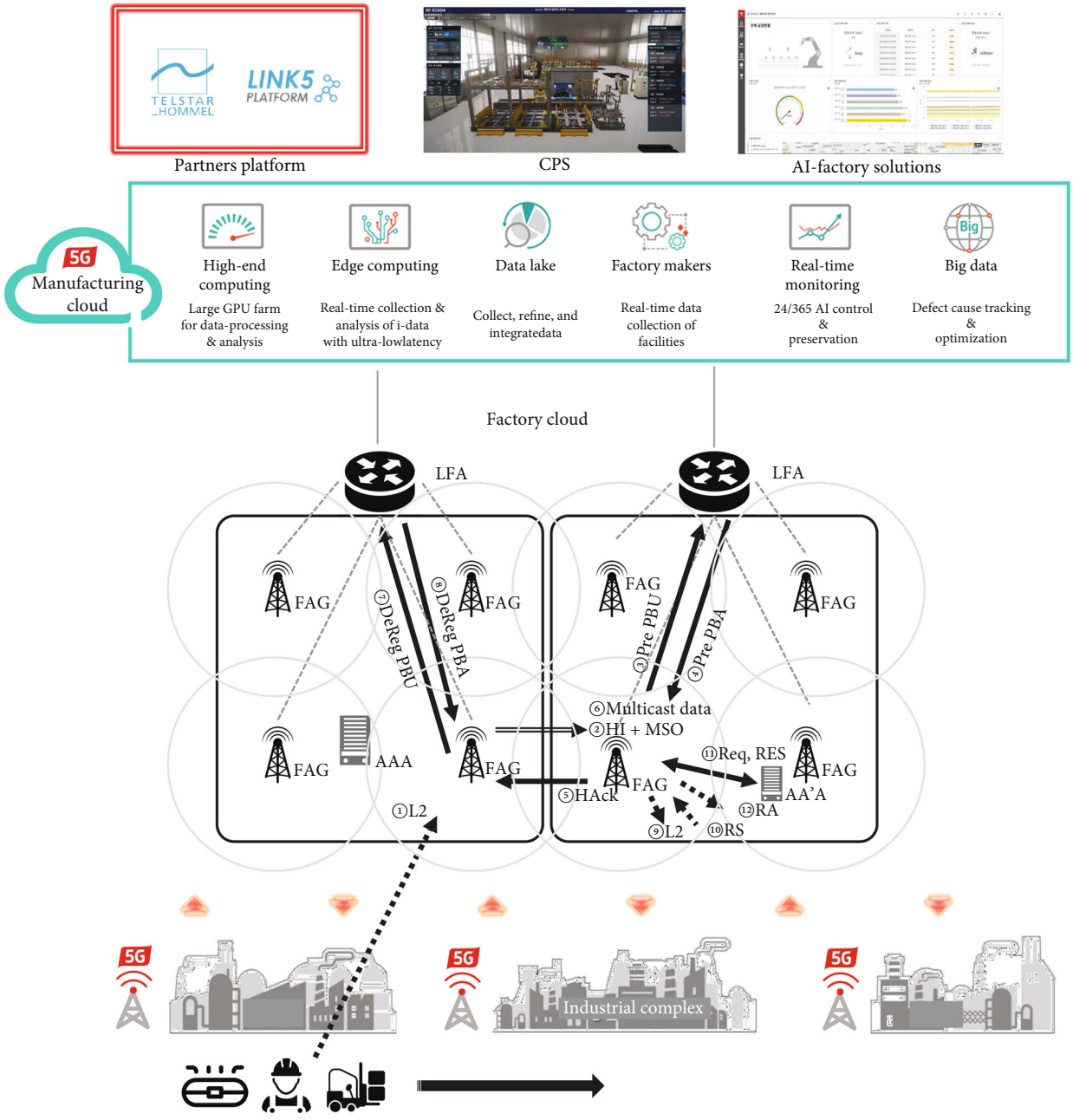


Figure 5: Concept of the smart factory.

affected by updates in intradomain movements. This means that it is not known whether the RCoA is connected to the FAG. Therefore, i-FP uses the address LCoA to obtain a more detailed location. LCoA is the same address as MN's location and is updated whenever MN is repositioned so that it always has accurate location information.

The LFA manages the RCoA and LCoA for MN. When the LFA receives traffic on the direction of MN, the LFA changes the target of the packet from RCoA to LCoA. The reason for using LCoA is that MN can quickly and accurately identify the stationary gateway in the domain. When the target of the packet changes to LCoA, the LFA sends the updated packet to the FAG with the MN connected. Because LCoA contains accurate location information for MN, MN can successfully receive packets. The binding of the RCoA and LCoA in LFA allows the i-FP to accurately and quickly transfer traffic from the MN to the domain. However, LFA cannot manage the local mobility of the domain.

Therefore, i-FP uses FAG, a second entity, to manage the transfer of MN. FAG is the access router (AR) of the local domain and is responsible for the i-FP's wireless network. FAG interconnects various APs that provide wireless links to the network. When the MN is connected to the FAG network, the FAG sends a Request Registration (RR) message to the MN to the LFA. If the MN is an authorized user, the FAG grants MN the authority to allow access. For example, the FAG specifies a new LCoA for MN and forwards MN's traffic to the corresponding radio link. If an MN attempts to send a

packet to another MN located in the i-FP domain, the FAG updates the packet's destination address and ensures that the packet is routed to the peer of the MN over the optimal path. Packet delivery procedures are described in detail in the following sections.

The third entity in i-FP is MN. MN is a roaming wireless device that includes workers, production facilities, and AGV included in the factory local domain. HMIPv6 and PMIPv6 use IP tunneling techniques in the local domain, while i-FP uses IP swapping mechanisms. IP switching agents are located between the data layer and the network layer on all MNs in the i-FP domain. This agent is used to process IP headers for MN traffic.

The IP swapping agent changes the packet target LCoA to RCoA when MN receives the packet and then sends the packet to the network layer. When a packet is sent to a network layer, the IP swapping agent simultaneously updates the source address of the packet to the LCoA of the MN. In this way, MN can maintain connectivity even if the domain is moved to a different network. Detailed operating procedures for IP swapping mechanisms can be found in "TMSP: Terminal Mobility Support Protocol" [37]. i-FP uses IP swapping technology, so there is no need for additional IP headers as there are no tunneling cost and latency.

i-FP uses the same LMA and MAG and MN as PMIPv6 to manage mobility. Although i-FP uses more IP addresses than PIMPv6, IPv6 is not a big problem because it has enough IP addresses. While HMIPv6 generates protocol signal costs on wired and wireless links, PMIPv6 and i-FP do not generate signal costs on wireless links, and protocol data is transmitted only on wired networks. Therefore, PMIPv6 and i-FP do not generate wireless bandwidth overhead on handover.

The last entity, factory cloud, is associated with the LFA in each domain. MN's mobility information is stored within the integrated system, cloud. A two-way bridge is formed between factory cloud and LFA. A formed bridge provides a flexible connection of information between each domain, which groups LFAs located in each domain. Nonprocessable computational processing with FAG and edge computing applied to the LFA within the local domain is sent to factory cloud via the LFA. The transmitted data is processed and analyzed through high-end computing in cloud. This facilitates the handling of handovers of i-FPs within the local domain.

3.2. Operation Procedure. Adding the concept of cloud to the smart factory, we configure the system structure in Figure 5. We have configured systems that connect to the cloud to construct cloud-based edge computing and have preconditions for applications that correspond to the configured network to be provided. Cloud servers are configured using OpenStack, and edge computing is located in local units to form cloud-based edge computing. IoT data is also stored on cloud storage in real time. When configuring gateways and servers between real-time storage, you configure nodes at the end of the application to act as controllers. Finally, IoT detection data is stored through the gateway and analyzed by the server. The application layer to which storage and analytics data are applied configures servers by node for real-time processing.

3.3. Registration Procedure. It acquires RCoA when the MN first accesses the network before performing the registration procedure on the i-FP network. When MN acquires RCoA, DHCP or Stateless Configuration (SC) is used. The following RCoA is registered with the global mobility agent. RCoA does not change while MN is in the domain. Thus, a global mobility protocol is maintained within the domain. Figure 5 shows the registration procedure since MN obtained RCoA.

As the MN proceeds with the handover, the newly connected FAG sends a Router Advertisement (RA) message to the MN. RA messages serve as keys for MN to acquire LCoA in the new FAG. The FAG then binds the RCoA and LCoA obtained from the MN within the local domain and sends the information to the LFA with the binding information to the Local Binding Update (LBU) message. If LFA allows LBU messages, the binding entry is set between RCoA and LCoA. This information is used for the domain and domain communication. The LFA sends a Local Binding Acknowledgement (LBA) message to the FAG. As soon as the FAG receives the LBA, the registration process is completed and the MN is able to transmit packets from a new location. i-FP is divided into traffic between domains and traffic within the domain. If MNs are in different local domains, their traffic is between domains. Otherwise, the traffic is within the domain. Traffic handover in i-FP is described as follows.

3.4. Intradomain Handover. The traffic delivery within a domain involves address management at the FAG. When MN1 transmits a packet to MN2, the IP swapping agent (ISM) of MN1 updates the original source to the LCoA and sends the packet to the FAG1. The FAG1, which is the first hop on the transmission path, updates the destination of the packet to the LCoA of the MN2. Because it is a packet transmission within the domain, it does not pass through the LFA and sends the packet directly to the FAG2 by referring to the LCoA. The FAG2 that receives the packet through the LCoA recognizes that the destination of the packet is the MN that is connected to it, so the FAG2 changes the address of the packet source into the RCoA that is the original address. Last, if the packet is sent to the MN2, the IP swapping agent of the MN2 changes the destination of the packet to the RCoA. Then, the packet is transmitted to the MN2. If the MN2 processes the transmitted packet and then again transmits the response message to the MN1, the IP swapping mechanism of the wireless link changes the address of the MN2 to the LCoA and transmits the packet to the FAG2.

Because the FAG2 is a packet movement in the domain, the MAG2 changes the destination address to the LCoA and transmits the packet to the FAG1. Because the FAG1 to which the packet is delivered recognizes that the destination indicates the MN that manages itself, it changes the destination source address to the RCoA that is the original address and delivers the packet to the MN1. Before the MN1 receives the packet, the IP swapping mechanism of the wireless link changes the destination address, which is the address of the MN1, to the RCoA that is the original address and delivers

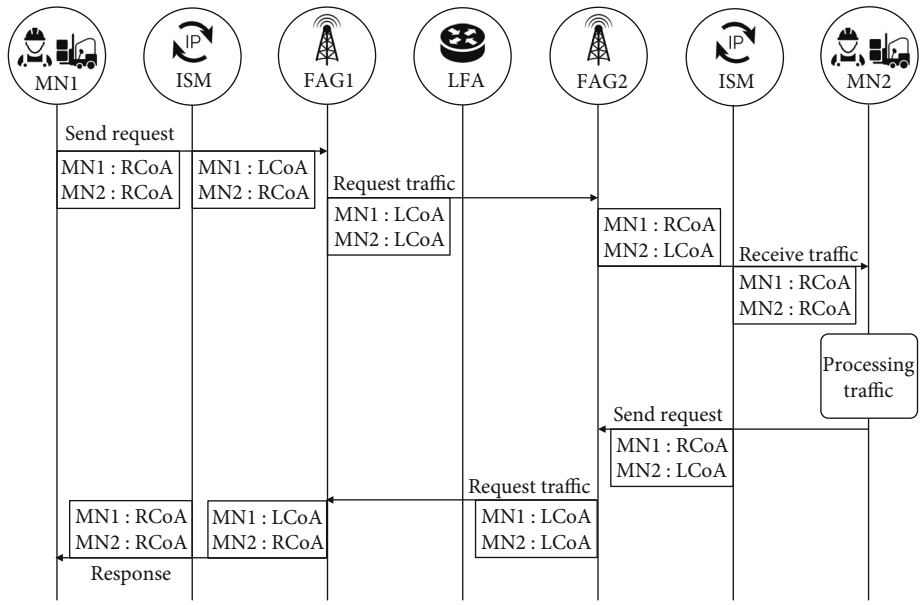


Figure 6: Flow of i-FP within the domain.

the packet. Because of this procedure, if the mobile node, such as MN1 or MN2, knows only the original address, it can exchange the packet without other functional requirements with the packet address management mechanism in the domain. This procedure is shown in Figure 6.

The handover of the MN in the domain sends an L2 signal, which means that the MN is about to do a handover to the pFAG to which it is first connected. The pFAG recognizes this signal sent to nFAG, which is expected to hand over the HI message to prepare the handover with the LCoA of the MN. The nFAG that delivers the MI message generates nLCoA, which will be newly assigned, and puts the LCoA and nLCoA in the message, which demands to be preregistered to the LFA, and transmits it. If the LFA receives the pre-BU message, it carries out the user certification to the AAA server, so that it maps the certified users with the RCoA and nLCoA information and preregisters them temporarily. Then, the LFA sends the pre-BA message to the nFAG to complete the registration. The nFAG that receives the message transmits the HAck message to pFAG to show that the handover is ready.

The pFAG that receives the HAck transmits the traffic that is transmitted to it to the nFAG and carries out the buffering. The pFAG puts the DeReg BU messages in the LCoA and sends them to the LMA in order to cancel the registration of the MN immediately; then, the LFA identifies it and updates the LCoA to nLCoA, so that it formally registers the MN, which is preregistered to the nFAG. As the response to it, the DeReg BU message is delivered to the pFAG, which transmits the response message to the L2 message to the MN. The MN transmits the RS message to the nFAG to demand the access. Because the nFAG registers the MN in advance, it can immediately put the nLCoA, which is the new LCoA address, in the RA and send it and then transmits the traffic that has just been buffered. The handover in the domain is completed by this procedure, and the MN can communicate with the nFAG. This procedure is shown in Figure 7.

3.5. Intradomain Handover. The traffic movement between other domains, which is different from the traffic movement in a domain, operates as follows. If the original MN sends the CN by means of the wireless network in order to request data, the wireless link operates the IP swapping mechanism before the packet arrives and changes the source address of the packet to the RCoA, which can be recognized even by the external domain. The packet with the changed address arrives at the FAG, which sends the packet as is to the LFA that is the local domain gateway. Because the destination of the packet is the CN that is an external domain, the LFA again converts the source address of the packet to the RCoA and sends it the CN, which processes it and then sends the response message for it to the RCoA.

Next, the CN receives the packet from the LFA and converts it to the LCoA, which is topologically identical, in order to send it to the internal domain. Then, the CN transmits the packet to the MAG that has the corresponding MN. The FAG delivers the packet to the MN and converts the address, which has already become the LCoA for the IP swapping mechanism which is antecedently operated, to the original RCoA and transmits it to the MN. By means of the IP converting mechanism in the domain, in the i-FP, the MN is involved in the IP change, or while it does not have to know it, the MN can exchange the packet with external domains. This is shown in Figure 8.

The handover between domains sends the L2 message to the pFAG to which it is originally connected, which means that the connection is about to be discontinued. The pFAG that receives the message transmits the RCoA of the MN with the HI message to the nFAG of the domain that expects the connection. The nFAG, which identifies the message, transmits the pre-BU message with the RCoA and the nLCoA, which is the newly assigned address, in order to preregister the MN to the nLFA to which it belongs. The nLFA receives the pre-BU message and carries out the user certification at the AAA server. If the message passes the certification, the

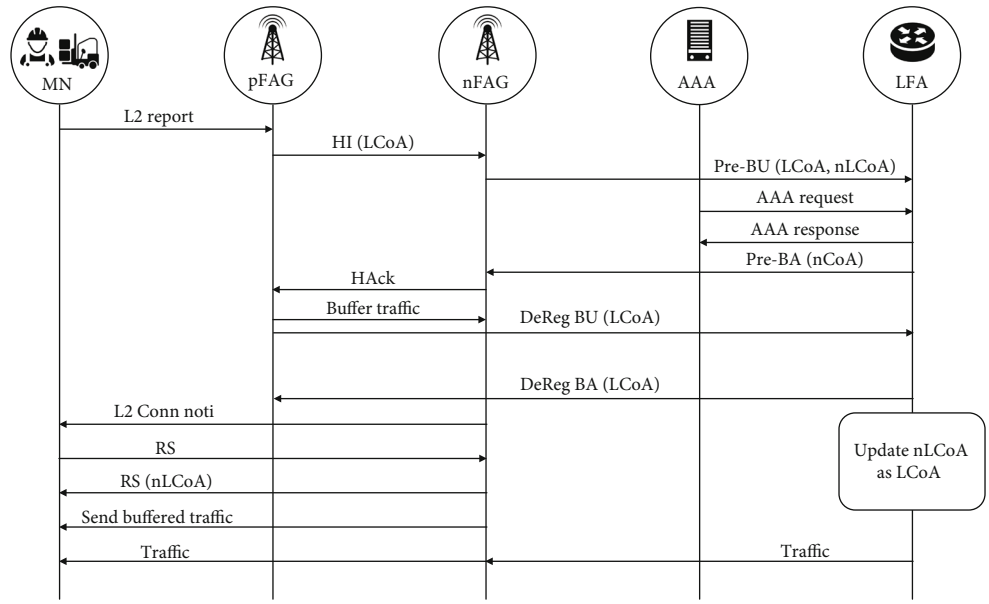


Figure 7: Flow of i-FP within the domain.

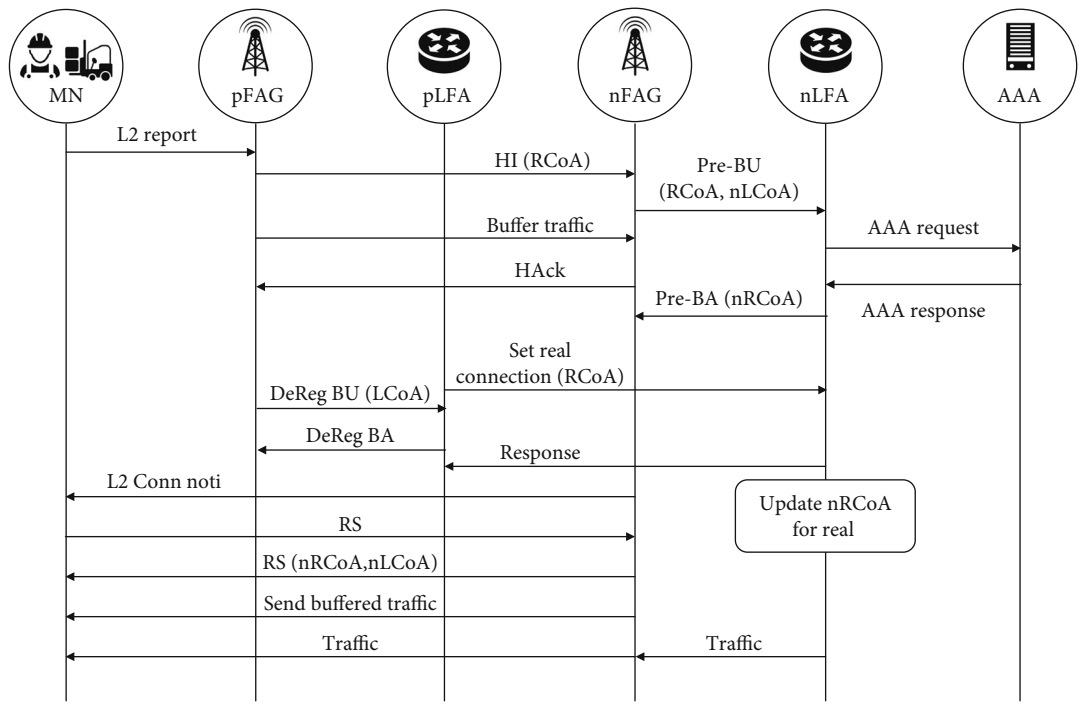


Figure 8: Handover of i-FP in the interdomain.

nLFA generates the nRCoA, saves it with the nLCoA, and lets it be preregistered. The LFA, as the response to it, transmits the pre-BA message with the nRCoA to the nFAG.

The nFAG that receives it then transmits the HAck message, which means that the handover is completely ready, to the pFAG. The pFAG that receives the message transmits the traffic that is delivered to it, and the nFAG buffers the transmitted traffic. After that, the pFAG, in order to cancel the connection of the MN, puts the LCoA in the DeReg-BU message and transmits it. The pLFA tells the nLFA to formally register the preaccessed MN, along with the RCoA. Then, the nLFA identifies the nRCoA by using the mapped RCoA and nRCoA, registers the nRCoA formally, and then sends the response message to the pLFA. The pLFA that receives the response message sends the DeReg BA message to the pFAG and informs the cancellation of the registration.

The nFAG transmits the response message to the L2 message, in which the MN transmits for the first time and then transmits the RS message to request the access to the nFAG. The nFAG receives the message, puts the newly assigned address of nRCoA and nLCoA in the RA message, and transmits them to the MN. After that, the nFAG transmits the

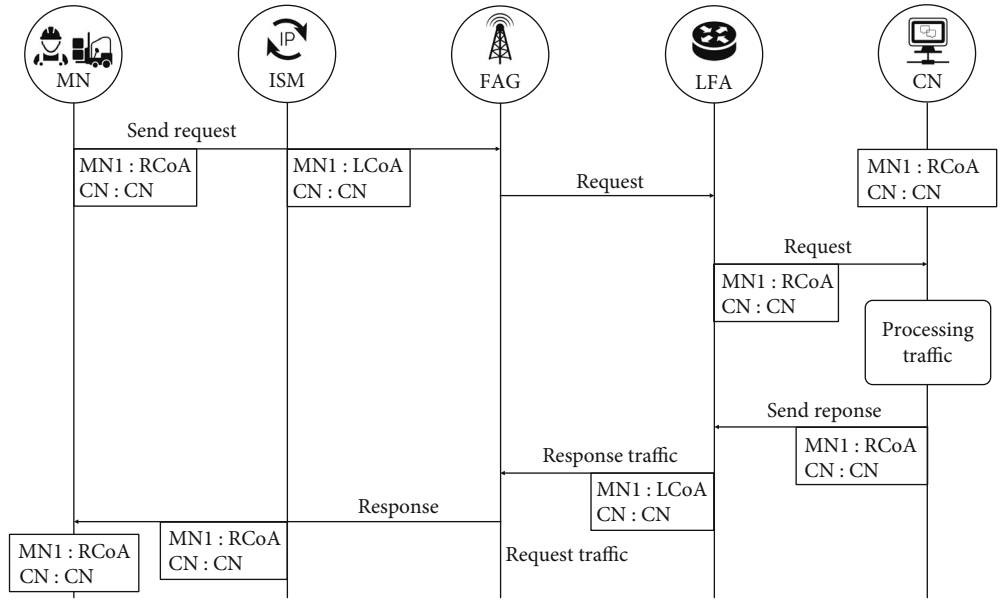


Figure 9: Traffic movement path between domains of i-FP.

buffered traffic data to the MN. The handover between domains is completed in these processes, and the fast connection and communication of the MN and the nFAG become possible. This is shown in Figure 9.

4. Performance Analysis

In this section, we conducted performance evaluations with mathematical modeling of the newly proposed i-FP, HMIPv6, and PMIPv6. This analysis objective is to minimize the costs arising from the network. Network costs are defined by message size and hop distance (bandwidth aspect). Each modeling was analyzed under the same conditions and ignored router processing costs. Table 1 shows parameters for mobile protocols used in performance analysis.

4.1. The Number of Routing Hops. We measure the number of traffic routing hops in the first performance analysis. The primary goal of i-FP is to provide the best routing route for intradomain traffic. This analysis compares the number of routing hops for intradomain traffic of the three protocols. At the same time, we compare and evaluate the transmission delay of intradomain traffic. The GR (Global Router) for the domain is located in the factory cloud (FC).

The number of routing hops of the three protocols is similarly set for domain internal traffic. When a packet is sent from CN, the FC in the domain receives the packet list. FC then forwards the packet to the new MN-connected AR. The AR sends packets over the radio link to the MN. Therefore, the number of routing hops can be expressed as 5, in which H_{X-Y} means the number of routing hops for node X and node Y. HMIPv6 and PMIPv6 require packets to be forwarded by FC. The FC encapsulates the packet and forwards it to the MN's current location.

Therefore, traffic inside the HMIPv6 and PMIPv6 domains causes triangular routing problems. However, the number of routing hops in the domain in i-FP is different from the traditional method. If an i-FP MN tries to forward a packet to another MN, the packet arrives at AR1 and forwards the traffic to AR2, where AR2 is located. Finally, AR2 forwards the packet with MN2. i-FP has fewer routing hops than HMIPv6 and PMIPv6 because packets are forwarded on the shortest path. Equations (1)–(3) represent the number of interdomain routing hops for HMIPv6, PMIPv6, and i-FP, and (4)–(6) represent the number of routing hops for the domain. FAGs for PMIPv6 can be configured as bridges for mobile nodes if MN1 and MN2 are on the same FAG network. The local routing optimization mechanism reduces forwarding delays.

$$H_{\text{Inter}}^{\text{HMIPv6}} = H_{\text{CN-FC}} + H_{\text{FC-AR}} + H_{\text{AR-MN}}, \quad (1)$$

$$H_{\text{Inter}}^{\text{P}_{\text{MIP}}\text{v6}} = H_{\text{CN-FC}} + H_{\text{FC-AR}} + H_{\text{AR-MN}}, \quad (2)$$

$$H_{\text{Inter}}^{\text{i-FP}} = H_{\text{CN-FC}} + H_{\text{FC-AR}} + H_{\text{AR-MN}}, \quad (3)$$

$$H_{\text{Intra}}^{\text{HMIPv6}} = H_{\text{MN1-AR1}} + H_{\text{AR1-FC1}} + H_{\text{FC1-AR2}} + H_{\text{AR2-MN2}}, \quad (4)$$

$$H_{\text{Intra}}^{\text{PMIPv6}} = H_{\text{MN1-AR1}} + H_{\text{AR1-FC1}} + H_{\text{FC1-AR2}} + H_{\text{AR2-MN2}}, \quad (5)$$

$$H_{\text{Intra}}^{\text{i-FP}} = H_{\text{MN1-AR1}} + H_{\text{AR1-FC1}} + H_{\text{AR2-MN2}}. \quad (6)$$

4.2. The Number of Routing Hops. The protocol signal cost is incurred in updating location information as MN moves, and usage is proportional to the amount of packets. Signal costs include RS (Router Solicitation) messages, BU (Binding Update) messages, and BA (Binding Acknowledgement) messages. The cost of the protocol signal, which is the cost of the handover procedure, is expressed as C_s. C_s is expressed as (7). P is the probability of one handover per t unit time.

Table 1: Parameter values for performance analysis.

Variable name	Value	Variable name	Value
H_{CN-FC}	2	$H_{AR1-AR2}$	1
H_{FC-AR}	1	i-FP_{BU}	96
H_{AR-MN}	1	i-FP_{BA}	96
$H_{MN1-AR1}$	1	i-$FP_{RouterSol}$	44
$H_{AR1-FC1}$	1	i-$FP_{RouterAdv}$	68
$H_{FC1-AR2}$	1	i-FP_{REU}	142
$H_{AR2-MN2}$	1	$HMIPv6_{RBU}$	80
$HMIPv6_{RBA}$	60	$PMIPv6_{PBA}$	88
$HMIPv6_{RouterSol}$	44	$PMIPv6_{RouterSol}$	44
$HMIPv6_{RouterAdv}$	68	$PMIPv6_{RouterAdv}$	68
$PMIPv6_{PBU}$	88	$T_{MAG-LMA}$	100
D_{L2}	100	$W_{MAG-LMA}$	300
A	10	T_{MN-LFA}	200
T_{MN-MAP}	100	$L1_{P\_Header}$	100
W_{MN-MAP}	300	H_{MAP-MN}	2
$H_{LMA-MAG}$	1	U	10000
R	1000		

H_{mn} is expressed as $H_{mn} = 1 - p$ with the probability of a handover to the MN. s is the total size of the protocol packets used for the handover procedure. m is the number of mobile nodes that exist in a domain per hour. The cost of HMIPv6, PMIPv6, and i-FP signals can be calculated by (8)–(10).

$$C_S = \sum_{n=1}^{\infty} n^* p^n * (1-p) * m * \frac{s}{t}, \tag{7}$$

$$C_S^{HMIPv6} = \sum_{n=1}^{\infty} n^* p^{n*} (1-p)^* m^* \frac{RBU + RBA + RS + RA}{t}, \tag{8}$$

$$C_S^{PMIPv6} = \sum_{n=1}^{\infty} n^* p^{n*} (1-p) * m * \frac{PBU + PBA + RS + RA}{t}, \tag{9}$$

$$C_S^{i\text{-}FP} = \sum_{n=1}^{\infty} n^* p^{n*} (1-p)^* m * \frac{RS + RA}{t}. \tag{10}$$

4.3. Handover Delay. If an MN handover is transmitted from one network to another, the MN may not be able to receive traffic. When the MN handover is moving through the network, MN's information is transmitted and MN cannot receive traffic. The time during which traffic is not received is called a handover delay. There are usually three possible causes of handovers. First, the MN's previously connected communication is broken when the MN moves to a different network. The MN should then be connected to a different radio link than before. Thus, D_{L2} represents the handover delay that occurs during the L2 link switching phase. MN gets a new IP address after being linked to a new network. D_{IP} indicates the time it takes for MN to acquire a new IP address. The time generated during the IP acquisition phase has a significant impact on the handover delay. There is a prestudied mechanism to solve these problems [38–41]. Specifying an optimized IP address allows the MN to obtain an IP address without the need for Duplicate Address Detection (DAD). i-FP is designed to leverage these mechanisms to allow MN to establish optimized IP addresses in new networks. Finally, MN gets a new IP address and sends an LU message. D_{LU} is the time spent completing a location information update. D_{LU} is primarily affected by the physical distance between MN and the agent. Thus, D_{LU} is managed by a local mobility protocol that uses proxy HA in the domain. The handover delay is based on these variables and is expressed as expression (11).

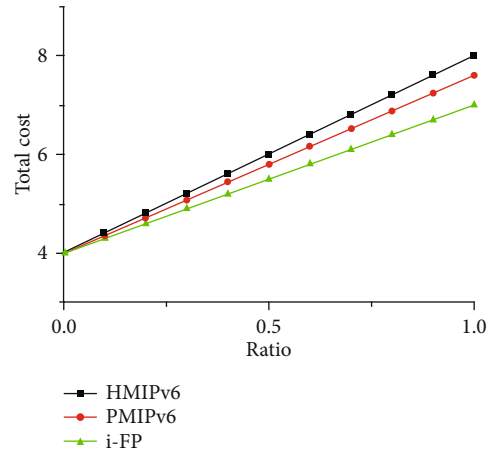


Figure 10: Average number of routing hops.

We compared and evaluated the performance of PMIPv6, HMIPv6, and i-FP on the same network with D_{L2}. The three protocols have different D_{IP}s. PMIPv6 does not change the IP address of MN in the new network, so the value of D_{IP} is zero. However, the values of D_{IP} for i-FP and HMIPv6 are larger than 0 because MN must set a new address. In both protocols, MN takes time to automatically set MN's address according to RA messages when it moves to a new network. RA messages are sent by the AP at every interval. D_{IP}^{HMIPv6} has a random value. If the time is the same mobile time, then the average value of D_{IP}^{HMIPv6} becomes $A/2$. $D_{IP}^{i\text{-}FP}$ has the same value as D_{IP}^{HMIPv6}. The three protocols D_{LU} are also different. HMIPv6 changes the location message between MN and MAP, creating a tunnel after the handover procedure. The tunnel generation time W_{MN-MAP} between MN and MAP is the same as the one-way transmission time T_{MN-MAP} of MN and MAP. Therefore, in HMIPv6, D_{LU} is equal to $2 * T_{MN-MAP} + W_{MN-MAP}$. In PMIPv6, D_{LU} is used to change update messages between MAG and LMA. In PMIPv6, a tunnel is formed between MAG and LMA in PMIPv6, just as a tunnel is created between MN and MAP in HMIPv6. The time required to create a tunnel between MAG and LMA is $W_{FAG-LMA}$. The update message transfer time from MAG to LMA is $T_{FAG-LFA}$. In PMIPv6, D_{LU} is

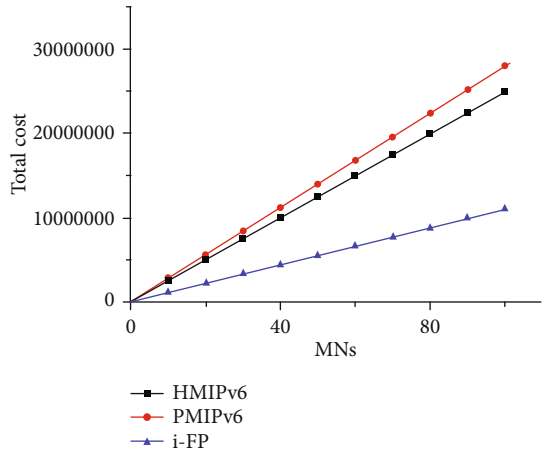


Figure 11: Traffic signaling cost.

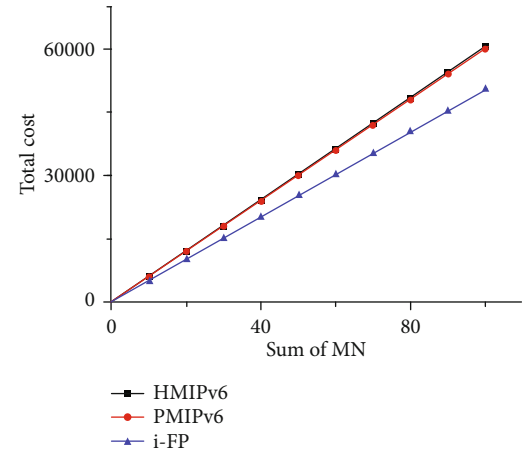


Figure 12: Handover delay.

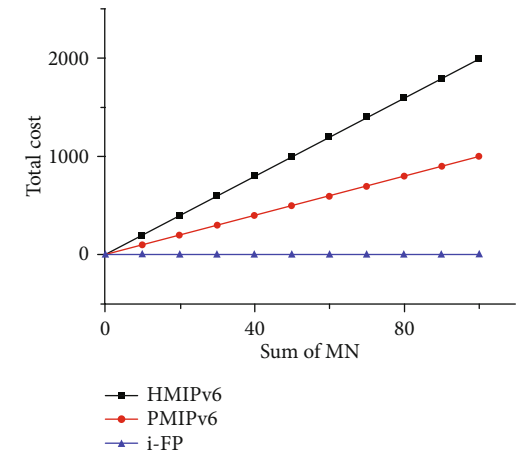


Figure 13: Traffic overhead.

defined as $2 * T_{\text{FAG–LFA}} + W_{\text{FAG–LFA}}$. For i-FP, no tunnel creation between MN and LFA is required. Thus, $D_{\text{IP}}^{\text{i-FP}}$ is represented by $2 * T_{\text{MN–LFA}}$ which is the MN and LFA bidirectional communication time. The handover latency of the three protocols is expressed in expressions (12)–(14), respectively. A is the interval between adjacent response messages.

$$D_{\text{HO}} = D_{\text{L2}} + D_{\text{IP}} + D_{\text{LU}}, \tag{11}$$

$$D_{\text{HO}}^{\text{HMIPv6}} = D_{\text{L2}} + \frac{A}{2} + 2 * T_{\text{MN–MAP}} + W_{\text{MN–MAP}}, \tag{12}$$

$$D_{\text{HO}}^{\text{PMIPv6}} = D_{\text{L2}} + 0 + 2 * T_{\text{FAG–LFA}} + W_{\text{FAG–LFA}}, \tag{13}$$

$$D_{\text{HO}}^{\text{i-FP}} = D_{\text{L2}} + \frac{A}{2} + 2 * T_{\text{MN–LFA}}. \tag{14}$$

4.4. Traffic Overhead. Finally, we compare the results by measuring the traffic overhead of HMIPv6, PMIPV6, and i-FP. HMIPv6 and PMIPv6 send traffic by IP tunneling technology. Tunneling headers cause overhead of user data in the network. C_{overhead} is the value of traffic overhead. $C_{\text{overhead}} = L_{\text{IPHeader}} * H$ denotes the traffic overhead of the three protocols. The length of the IP tunnel is defined as L_{IPHeader}. H is the number of hops the packet traverses in the local domain. The data rate is R bps and the packet size of user data is U; the overhead cost of HMIPv6, PMIPv6, and i-FP can be expressed as

$$C_{\text{overhead}}^{\text{HMIPv6}} = L_{\text{IPHeader}} * H_{\text{MAP–MN}} * \frac{R}{U}, \tag{15}$$

$$C_{\text{overhead}}^{\text{PMIPv6}} = L_{\text{IPHeader}} * H_{\text{LFA–FAG}} * \frac{R}{U}, \tag{16}$$

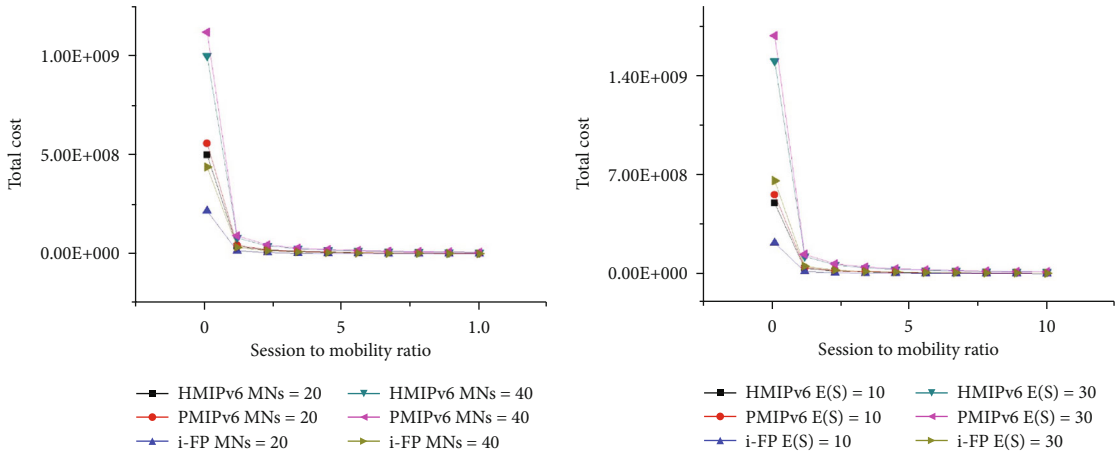
$$C_{\text{overhead}}^{\text{i-FP}} = 0. \tag{17}$$

4.5. Numerical Results. We evaluated the difference in performance between HMIPv6, PMIPv6, and i-FP with various conditions and obtained numerical results for routing hops, traffic signaling cost, handover delay, and traffic overhead. We analyze the numerical results of each evaluation method in the order mentioned. i-FP has the fewest routing hops, and the average number of routing hops of PMIPv6 is smaller than that of HMIPv6. δ represents the ratio of the intradomain traffic F_{intra} divided by the sum of the intradomain traffic F_{intra} and the interdomain traffic F_{inter}, which means $\delta = F_{\text{intra}}/(F_{\text{inter}} + F_{\text{intra}})$. In Figure 10, we can see that the average number of routing hops of i-FP is lower than the other two protocols.

Figure 11 shows the total signal cost as MN increases. As a number of MNs initiated by handover increase, all three protocols increase the signal cost. However, i-FP increases to a slower slope than PMIPv6 and HMIPv6. Therefore, i-FP is more cost-effective because of its lower signal cost than PMIPv6 and HMIPv6.

The performance of the handover delay for each protocol is evaluated according to the total cost of the MN. The larger the handover delay, the greater the packet loss in the handover procedure. The total cost until packet reception is complete is used to measure the handover delay of the three protocols. In Figure 12, we can see that the latency of PMIPv6 and HMIPv6 is more than doubled as MN increases compared to the incidence cost of i-FP.

To measure the total cost of traffic overhead for each technique, we evaluated a number of MNs performing handover as variables. From the traffic overhead evaluation, we see



(a) A type (b) B type

Figure 14: Total cost by SMR.

that i-FP is maintained regardless of the number of MNs performing handovers, because it uses the IP swapping mechanism without IP tunneling, and HMIPv6 and PMIPv6 perform IP tunneling. Therefore, it can be confirmed that the overhead increases as a number of MNs performing handover increase. Since a number of MNs increase compared to those of HMIPv6, PMIPv6 increases rapidly. The contents are shown in Figure 13.

Session-to-mobility ratio (SMR) was utilized to evaluate the total cost of the network. SMR is calculated by dividing the session arrival rate by the head-off rate. We classified SMR into two types, increasing the accuracy of the evaluation. If the value of SMR is large, the session activity is higher than the hand off speed. It is shown that i-FP has had little impact on the increase in SMR compared to other networks and has the lowest total cost. This is shown in Figure 14.

5. Conclusion

We proposed a new i-FP based on the features of HMIPv6 and PMIPv6 networks. We also address the cost issues arising from network architectures for MNs used in smart factory environments. Based on the proposed i-FP, HMIPv6, and PMIPv6 modeling, we analyzed and evaluated the network cost minimization. Comparing the cost and traffic overhead of packet data transmission, we demonstrate that i-FP, which appears to be the lowest in local units, is the enhanced technique. Therefore, we confirm that i-FP is the most suitable mobile network protocol framework for application in smart factory environments due to low data loss and low latency. Furthermore, through an optimization system of cross-domain handover via edge computing, the cost compared to existing techniques is also relatively low, which increases satisfaction. This can be the basis for judging that i-FP is the best solution for local mobile network environments in smart factory environments. Adding to the analysis of the cloud environment, the following work envisions additional research to build an integrated system to analyze performance compared to existing technologies.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request (jpjeong@skku.edu).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Industrial Cluster Program funded by the Ministry of Trade, Industry and Energy (MOTIE, Korea) and the Korea Industrial Complex Corporation (Project Number SKN19ED). And also, this research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ICT Creative Consilience program (IITP-2020-0-01821) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).

References

[1] E. A. Lee, "Cyber physical systems: design challenges," in *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, pp. 363–369, Orlando, FL, USA, 2008.

[2] J. Villalba-Diez and X. Zheng, "Quantum strategic organizational design: alignment in industry 4.0 complex networked cyber-physical lean management systems," *Sensors*, vol. 20, no. 20, p. 5856, 2020.

[3] S. Praptodiyono, T. Firmansyah, M. Alaydrus, M. I. Santoso, A. Osman, and R. Abdullah, "Mobile IPv6 vertical handover specifications, threats, and mitigation methods: a survey," *Security and Communication Networks*, vol. 2020, 18 pages, 2020.

[4] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, and J. Zhang, "Edge intelligence: paving the last mile of artificial intelligence with edge computing," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1738–1762, 2019.

[5] A. Rahman, J. Jin, A. L. Cricenti, A. Rahman, and A. Kulkarni, "Communication-aware cloud robotic task offloading with on-demand mobility for smart factory maintenance," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 5, pp. 2500–2511, 2018.

[6] A. Radziwon, A. Bilberg, M. Bogers, and E. S. Madsen, "The smart factory: exploring adaptive and flexible manufacturing solutions," *Procedia Engineering*, vol. 69, pp. 1184–1190, 2014.

[7] D. Saha, A. Mukherjee, I. S. Misra, and M. Chakraborty, "Mobility support in IP: a survey of related protocols," *IEEE Network*, vol. 18, no. 6, pp. 34–40, 2004.

[8] J. Kempf, "Problem statement for network-based localized mobility management (NETLMM)," Tech. rep., RFC 4830, 2007.

[9] J. Kempf, "Goals for network-based localized mobility management (NETLMM)," Tech. rep., RFC 4831, 2007.

[10] S. Deering and R. Hinden, "Internet protocol, version 6 (IPv6) specification," 1998.

[11] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in IPv6," 2004.

[12] A. S. Ahmed, R. Hassan, and N. E. Othman, "IPv6 neighbor discovery protocol specifications, threats and countermeasures: a survey," *IEEE Access*, vol. 5, pp. 18187–18210, 2017.

[13] D. K. Oh and S. W. Min, "A fast handover scheme of multicast traffics m PMIPv6," *The Journal of Korean Institute of Communications and Information Sciences*, vol. 36, no. 3B, pp. 208–213, 2011.

[14] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, and F. Xia, "Fast handovers for proxy mobile IPv6," *RFC 5949*, 2010.

[15] C. Castelluccia, "HMIPv6," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 4, no. 1, pp. 48–59, 2000.

[16] S. Das, A. Misra, and P. Agrawal, "TeleMIP: telecommunications-enhanced mobile IP architecture for fast intradomain mobility," *IEEE Personal Communications*, vol. 7, no. 4, pp. 50–58, 2000.

[17] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, *Host Identity Protocol*, Tech. rep., RFC 5201, 2008.

[18] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, *Proxy Mobile ipv6*, 2008.

[19] J. Lei and X. Fu, "Evaluating the benefits of introducing PMIPv6 for localized mobility management," in *2008 International Wireless Communications and Mobile Computing Conference*, pp. 74–80, Crete, Greece, 2008.

[20] H. Soliman, C. Castelluccia, K. Elmalki, and L. Bellier, "Hierarchical mobile IPv6 mobility management (HMIPv6)," *RFC 4140*, p. 5380, 2008.

[21] J. Kim and J. Jeong, "Design and performance analysis of an industrial IoT-based mobility management for smart manufacturing," in *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 0471–0476, Vancouver, BC, Canada, 2019.

[22] S. H. La, J. Jeong, J. Koo, and U. M. Kim, "On intelligent hierarchical F-PMIPv6 based mobility support for industrial mobile networks," *Procedia Computer Science*, vol. 155, pp. 169–176, 2019.

[23] D. G. Park, J. Lee, J. W. Oh, and J. Jeong, "A novel SDN-based cross handoff scheme in industrial mobile networks," *Procedia Computer Science*, vol. 155, pp. 642–647, 2019.

[24] J. A. Kim, D. G. Park, and J. Jeong, "Design and performance evaluation of cost-effective function-distributed mobility management scheme for software-defined smart factory networking," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 6, pp. 2291–2307, 2020.

[25] I. Heritage, "Protecting industry 4.0: challenges and solutions as IT, OT and IP converge," *Network Security*, vol. 2019, no. 10, pp. 6–9, 2019.

[26] M. Gohar, S. Anwar, M. Ali, J. G. Choi, H. Alquhayz, and S. J. Koh, "Partial bicasting with buffering for proxy mobile IPv6 mobility management in CoAP-based IoT networks," *Electronics*, vol. 9, no. 4, p. 598, 2020.

[27] A. Hussain, S. Nazir, F. Khan et al., "A resource efficient hybrid proxy mobile IPv6 extension for next generation IoT networks," *IEEE Internet of Things Journal*, 2021.

[28] B. Chen, J. Wan, L. Shu, P. Li, M. Mukherjee, and B. Yin, "Smart factory of industry 4.0: key technologies, application case, and challenges," *IEEE Access*, vol. 6, pp. 6505–6519, 2018.

[29] M. M. Mabkhot, A. M. Al-Ahmari, B. Salah, and H. Alkhalefah, "Requirements of the smart factory system: a survey and perspective," *Machines*, vol. 6, no. 2, p. 23, 2018.

[30] Y. Yuan, L. Qian, G. Jia, L. Yu, Z. Yu, and Q. Zhao, "Efficient computation offloading for service workflow of mobile applications in mobile edge computing," *Mobile Information Systems*, vol. 2021, p. 11, 2021.

[31] F. Sufyan and A. Banerjee, "Computation offloading for distributed mobile edge computing network: a multiobjective approach," *IEEE Access*, vol. 8, pp. 149915–149930, 2020.

[32] H. Wu, Y. Yan, D. Sun, H. Wu, and P. Liu, "Multi buffers multi objects optimal matching scheme for edge devices in IIoT," *IEEE Internet of Things Journal*, p. 1, 2021.

[33] Lanner America, Intelligent Edgehttps://www.lanner-america.com/knowledgebase/intelligent-edge/.

[34] A. G. Valk'o, "Cellular IP: a new approach to Internet host mobility," *ACM SIGCOMM computer communication review*, vol. 29, no. 1, pp. 50–65, 1999.

[35] R. Ramjee, T. La Porta, S. Thuel, K. Varadhan, and S. Y. Wang, "HAWAII: a domain-based approach for supporting mobility in wide-area wireless networks," *IEEE/ACM Transactions on Networking*, vol. 10, no. 3, pp. 396–410, 2002.

[36] A. Romanow, J. Mogul, T. Talpey, and S. Bailey, "Remote direct memory access (RDMA) over IP problem statement," *RFC 4290*, 2005.

[37] T. M. Lim, C. K. Yeo, F. B. S. Lee, and Q. V. Le, "TMSP: terminal mobility support protocol," *IEEE Transactions on Mobile Computing*, vol. 8, no. 6, pp. 849–863, 2008.

[38] S. Thomson, T. Narten, and T. Jinmei, "IPv6 stateless address autoconfiguration," *RFC 4862*, 2004.

[39] Y. Gvvon, J. Kempf, and A. Yegin, "Scalability and robustness analysis of mobile IPv6, fast mobile IPv6, hierarchical mobile IPv6, and hybrid IPv6 mobility protocols using a large-scale simulation," in *2004 IEEE International Conference on Communications*, vol. 7, pp. 4087–4091, Paris, France, 2004.

[40] X. Perez-Costa, M. Torrent-Moreno, and H. Hartenstein, "A performance comparison of mobile IPv6, hierarchical mobile IPv6, fast handovers for mobile IPv6 and their combination," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 7, no. 4, pp. 5–19, 2003.

[41] G. Kim, "Low latency cross layer handover scheme in proxy mobile IPv6 domain," in *International Conference on Next Generation Wired/Wireless Networking*, pp. 110–121, Berlin, Heidelberg, 2008.