applied sciences

MDPI

Article

Secure and Efficient Multicast-Enabled Handover Scheme Pertaining to Vehicular Ad Hoc Networks in PMIPv6

Amit Kumar Goyal [1], Gaurav Agarwal [1], Arun Kumar Tripathi [2] and Mangal Sain [3,*]

[1] Department of Computer Science and Engineering, Invertis University Bareilly, Bareilly 243123, India
[2] Department of Computer Applications, KIET Group of Institutions, Delhi-NCR, Ghaziabad 201206, India
[3] Division of Computer and Information Engineering, Dongseo University, Busan 47011, Republic of Korea
* Correspondence: mangalsain1@gmail.com

Abstract: In VANET, mobility management and handover management are two of the most intriguing and challenging research topics. The existing mobility management infrastructures are unable to provide seamless secure mobility and handover management. It is very common in a vehicular network that when a vehicle roams between two domains, its reachability status may be compromised. The main reason for this is the higher handover latency and packet loss during the handover process. In the last decade, IP-based mobility protocols have been proposed for interoperable handover management systems. There has been a great deal of interest in providing IP multicast to mobile nodes such as vehicles, and numerous strategies have been put forth thus far. This research article proposes an IP multicast-enabled handover architecture for VANET in PMIPv6. Adding the IP multicast facility to the authentication server allows handover management that is both intra-domain and inter-domain, which originally was not supported by PMIPv6. This makes it possible for the IP service of a vehicle to maintain a connection from any location, without changing the earlier application. Additionally, a secure architecture with authentication capabilities built on top of PMIPv6 is suggested for VANET to address the authentication problem. Finally, the article compares the performance of the proposed architecture with that of the ones currently in use by varying several factors, including the vehicle's density, the setup costs required, and the unit transmission costs on wired and wireless links, and it shows that our proposed solution ensures the handover process with a minimal cost change.

Keywords: IP multicasting; mobility management; PMIPv6; VANET

Citation: Goyal, A.K.; Agarwal, G.; Tripathi, A.K.; Sain, M. Secure and Efficient Multicast-Enabled Handover Scheme Pertaining to Vehicular Ad Hoc Networks in PMIPv6. *Appl. Sci.* **2023**, *13*, 2624. https://doi.org/10.3390/app13042624

Academic Editors: Christos L. Stergiou and Konstantinos E. Psannis

Received: 27 December 2022
Revised: 27 January 2023
Accepted: 14 February 2023
Published: 17 February 2023

1. Introduction

The vehicular ad hoc network (VANET) has enthralled automobile manufacturing companies by adopting next-generation low-cost wireless technologies to make vehicles intelligent. VANETs are crucial for the creation of vehicle-centered applications, in which individual vehicles produce and gather data, disseminate these data locally, and use local data from nearby vehicles, even without the intervention of any other object. VANET [1] is an infrastructure-neutral, distributed heterogenous wireless network that offers a significant advancement; it can improve the ease of efficacy of roadside traffic and traffic control. The applications of VANET may include those that allow users to share data on road safety, traffic congestion, impending tolls, location detection, meteorology, parking, and facilities such as supermarkets, theaters, and cafes. When no support from a fixed infrastructure is needed, vehicles in a VANET can connect with one another directly or through the use of multi-hop communication (V2V). Applications concerning security, safety, and dissemination may be some examples where V2V communication is helpful. On the other hand, vehicle-to-infrastructure (V2I) communication is mostly used for information and data collection applications and allows for communication between vehicles and fixed infrastructure, such as base stations and access points (AP). Depending upon the

distance, or whether it can directly communicate with the roadside unit or not, a vehicle can connect with the roadside infrastructure in this situation, either in a multi-hop or single-hop method. This makes it possible to connect remote vehicles or the Internet over wide areas. Three different types of communication topologies are feasible in VANET: full ad hoc communication used in V2V communication, full cellular/WLAN communication in V2I, and hybrid communication occurs in V2I mode, whereby other vehicles can serve as gateways and use multi-hop routing to connect vehicles to roadside units (RSUs) [2]. Due to the highly mobile nature of vehicles, the vehicles in a VANET can frequently change their points of attachment. Additionally, vehicles must be reachable by hosts on the Internet, regardless of where they are at the current time. One of VANET's greatest and most challenging issues is mobility management [3,4]. In order to locate a vehicle's point of attachment for location management [5], serving networks may use mobility management and, by using the facilities provided by handover management, maintain a vehicle's connection while it is moving [6]. As a result, mobility management must adhere to the following specifications.

Seamless Mobility: The VANET should appear translucent, hiding the vehicles' ability to move about freely. Independent of the vehicle's present location, vehicles must be able to communicate with other vehicles and/or RSUs. The handoffs between access routers are also included in this, and a minimum delay should be ensured in the handoff process at the cost of authentication.

Scalability and Efficiency: VANETs have the possibility of growing significantly, incorporating possibly hundreds of vehicles on a regular basis. As a result, the protocol methods/mechanisms need to be extremely scalable, and they must be efficient enough in terms of the overhead brought about by mobility management.

VANET Properties: The mobility management must handle IPv6-based multi-hop communications along with various driving traits, such as the highly mobile nature of nodes.

Secure: The handover process should be secure enough so that no unauthenticated vehicle can enter into the network.

The Internet Engineering Task Force (IETF) has established several specifications that have been utilized to create several mobility management protocols. These protocols can be divided into two categories: host-based mobility management protocols and network-based mobility management protocols. While network-based mobility management protocols handle localized mobility, host-based mobility management protocols provide global mobility by allowing hosts to send mobility signaling. MIPv4 and MIPv6 [7–9], variants of the IP mobility protocol, permit the use of two distinct IP addresses, known as a fixed home address (HoA) and care of-address (CoA). MIPs (v4/v6) both encounter the problems of high packet losses and a high handover delay [9], which makes mobility inefficient. Host-based mobility management refers to several protocols, including MIPv6 and Hierarchical Mobile IPv6 (HMIPv6), which aims to reduce the signaling traffic issue between the home agent and correspondent node and regulate the excessive overhead, and Fast Mobile IPv6 (FMIPv6), which handles the issue of Quality of Service (QoS) for interactive program service applications that may be decreased by the packet loss and handover latency problems of MIPv6. The well-known mobility protocols for localized mobility are Fast Handover Proxy Mobile IPv6 (FPMIPv6) and Network-Based Proxy Mobile IPv6 (PMIPv6) [10,11], standardized by the IETF NETLMM working group, and the telecommunication and Internet communities have started to pay close attention to it. The aim of this article is to describe a secure and efficient PMIPv6 architecture that can be used to provide the intra-domain and inter-domain mobility handover of vehicles in a VANET. Originally, PMIPv6-supported schemes provided mobility in a localized domain. The proposed architecture, which is based on IP multicasting, can provide both inter- and intra-domain handoff. The remaining parts of the work are structured as follows. Relevant work in the mobility management of vehicles is reviewed in Section 2. Section 3 discusses the model for the estimation of the total cost during intra-domain handoff and inter-domain handoff and proposes the multicast-enabled mobility handover strategy. Section 4 emphasizes the mathematical

analysis of costs for inter-domain handoff, along with the costs of intra-domain handoff, whereas Section 5 presents a qualitative outcome analysis based on several metrics, and a comparison with the current mobility management program with the proposed architecture is discussed. Lastly, Section 6 closes the work by mentioning future directions in mobility management.

2. Existing Work

PMIPv6, the localized network-based mobility management standard introduced by the IETF, does not include mobile nodes such as vehicles in mobility-related signals. Instead, the network entity assigns the vehicle a special home network prefix (HNP) when it enters the PMIPv6 mobility domain. This prefix will be used to identify the vehicle consistently inside a mobility domain. As a result, the vehicle considers the PMIPv6 domain to be its principal network. The two functional parts of the underlying PMIPv6 architecture are the mobile access gateway (MAG) and a local mobility anchor (LMA). The MAG or access router (AR) is concerned with monitoring the vehicle's movement, whereas the LMA is the anchor point of the PMIPv6 domain. As soon as the MAG notices the movement of the vehicle, it starts the procedures needed for handover with the LMA. It accomplishes this by sending a proxy binding update (PBU) message to the LMA. Additionally, a tunnel connects the LMA and MAG so that they may use the vehicle's HNP address [12,13]. All vehicular traffic passes via the LMA, which serves as a topological anchor point and is responsible for preserving the PMIPv6 domain's routing and vehicle accessibility. Through binding cache entry (BCE) [13,14], the LMA also keeps track of each registered vehicle's binding status. The established interface identification of the tunnel, the vehicle's HNP, a proxy registration flag, and other details are all contained in the BCE. When a vehicle's point of attachment changes, Layer 2 handovers, intra-domain handovers, and inter-domain handovers are all possible. When a vehicle switches access points while still in the same MAG, a Layer 2 handover takes place. This modification does not affect the LMA, since the MAG only affects the binding of the vehicle locally. An inter-domain handover takes place when a vehicle transitions between two MAGs connected to the same LMA. The MAGs maintain the vehicle attached to the LMA by switching PMIPv6's handoff signals. On the other hand, the vehicle's attachment points alternate between two MAGs connected to different LMAs during the inter-domain handover. Originally, the PMIPv6 protocol was only responsible for managing intra-domain mobility roaming. While assessing the total packet delivery cost for VANET in PMIPv6, none of the existing solutions consider authentication during handoff; however, we have considered the authentication cost during handover, along with the IP multicasting that enables the inter-domain handover for VANET in PMIPv6. Thus, neglecting this situation invariably results in a handover that is not secure and is inefficient. To solve these issues, we suggest a method that takes the authentication costs into account while evaluating the overall cost of packet delivery in PMIPv6 for a vehicular network, along with IP multicasting, which allows inter-domain handover for VANET in PMIPv6.

3. Proposed Work

The most important part of the proposed scheme is modifying the role of the trusted third-party server (TTP) that is responsible for the vehicle's and network entities' authentication and authorization. In the proposed scheme, the TTP server is allowed to multicast the authentication information to neighboring TTPs, as well as to the anchor point of the domain, i.e., the LMA, as shown in Figure 1. The authentication of vehicles involves following certain steps. In step 1, the access router, i.e., MAG, forwards the authentication request containing the vehicle ID and MAG ID to the TTP present in the local domain. It is the responsibility of the TTP to authenticate the vehicle. After authenticating the vehicle, the TTP server returns the authentication response (in terms of the vehicle profile, MAG profile) back to the MAG in step 2. During this, in step 3, the TTP multicasts the authentication information (vehicle and/or MAG profile) to the LMA present in the local PMIPv6 domain, as well as to the neighboring TTPs present in other PMIPv6 domains. The information

shared with neighboring TTPs can be used in case of inter-domain handover. Thus, the TTP of the local domain works as a multicast server for the authentication process. The addition of the multicast server maintains the Layer 4 connection in both the intra- and inter-domain regions and allows for vehicle handover, which PMIPv6 did not initially provide. The solution will minimize multicast forwarding delays to provide seamless and fast handovers for real-time services. It will eliminate lookup costs and binding update delays at the BCE.

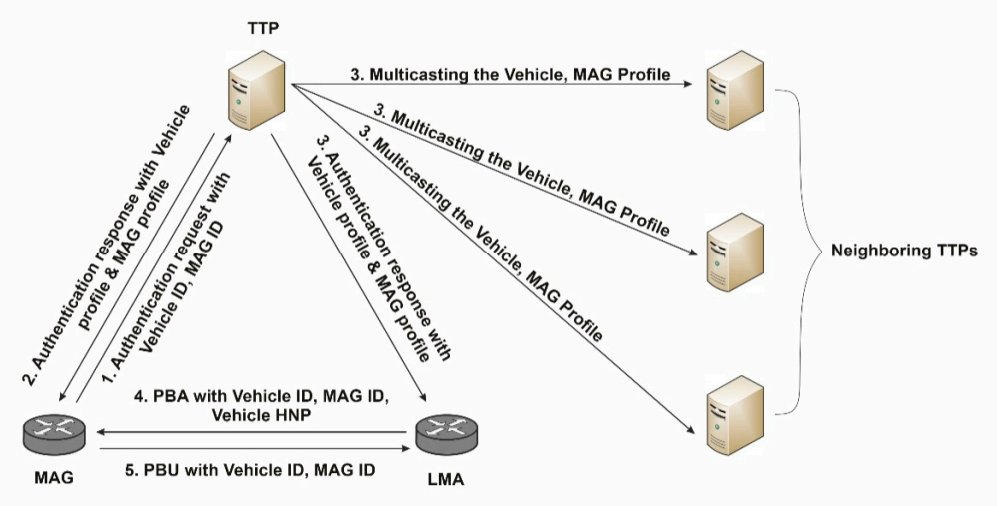


Figure 1. Multicast authentication information by TTP server.

Once the LMA has received the authentication information from the Trusted Third Part (TTP), the LMA can directly send the Proxy Binding Acknowledgement (PBA) message consisting of Vehicle-ID, MAG-ID and Home-network Prefix (HNP) to the MAG in step 4, without waiting for the MAG to send the Proxy Binding Update (PBU) message.

Current handover techniques [9] do not account for the authentication cost when calculating the overall packet delivery costs in the handoff of VANET in PMIPv6. To assess the entire cost of packet delivery during handover, our proposed architecture considers the authentication cost during handover. Figure 2 shows the architecture for handoff during intra-domain and inter-domain handover that uses the IP multicasting described above. Here, three proxy mobile IPv6 domains, namely PMIPv6domain1, PMIPv6domain2, and PMIPv6domain3, are considered. In each PMIPv6 domain, vehicles are connected to one of the MAGs, e.g., MAG1_D1, available via an access point, e.g., AP1_D1, which in turn are under the control of the topological anchor point of the domain, i.e., LMA1. The authentication and authorization of vehicles and MAGs are performed by the trusted third-party (TTP) server present in every domain. The role of the TTP server has been modified as described in Figure 2. Upon receiving the authentication request from an MAG, the TTP present in the local domain authenticates the vehicle by generating a vehicle profile and MAG profile. The TTP server then returns the authentication response back to the MAG, as well as to the LMA present in the local PMIPv6 domain. During the intra-domain handover, a vehicle changes its attachment from AP1_D1 of MAG1_D1 to the access point AP2_D1 of MAG2_D1 of LMA1. On the other hand, when a vehicle changes its point of attachment from AP2_D1 of MAG2_D1 to access point AP1_D2 of MAG1_D2, inter-domain handover occurs. The TTP server, upon authenticating the vehicle, multicasts the authentication information to the neighboring TTPs present in other PMIPv6 domains. Section 3.1 describes the message flow diagram of a vehicle when it first connects to domain, Section 3.2 explains the message flow diagram of a vehicle during intra-domain handover, and Section 3.3 describes the message flow diagram during inter-domain handover.

3.1. Message Flow Diagram of the Initial Connection in PMIPv6 for VANET

When a vehicle connects itself for the first time to the PMIPv6 domain, the sequence of messages that are exchanged among network entities MAG/LMA, TTP [15], and the

vehicle are as shown in Figure 3. For the first time, the vehicle connects to an access point that is affixed to one of the MAGs; the MAG forwards the authentication request to the TTP with the vehicle ID and MAG ID in step 2. Vehicle authentication and authorization, as well as that of network entities such as MAGs and LMAs, are handled by the TTP. After authentication is completed, in step 3, the TTP will send the authentication response consisting of the vehicle and MAG profiles to the MAG and LMA [16]. In addition to this, the TTP also multicasts this profile information to the neighboring TTPs so that, later, during the inter-domain handover, this information can be used. On receiving the router solicitation message from the vehicle in step 4, in step 5, the PBU message with the vehicle ID is sent by the MAG to the LMA. Following the updating of the binding cache entry (BCE) in step 6, the MAG is identified as being permitted to send PBU messages. The LMA in step 7 then transmits a PBA message along with the vehicle's HNP. Step 8 creates a bi-directional tunnel to the MAG [17,18], which makes it accessible for the vehicle. In step 9, the MAG transmits to the vehicle a router advertisement (RA) message. After obtaining the RA message, the vehicle produces its home address by fusing the HNP with its interface address. In PMIPv6, which only employs the per vehicle prefix technique, each vehicle is assigned a unique home network prefix. In contrast to MIPv6, a vehicle traveling within a PMIPv6 domain receives a distinctive home address. The bidirectional tunnel enables all messages sent by the vehicle to be forwarded to the LMA. The LMA, which serves as the topological anchor point for the domain, receives all communications meant for the vehicle. The LMA then transmits the received message through the tunnel to the MAG. After the outer header is removed, the message is sent to the vehicle via the MAG at the opposite end of the tunnel.

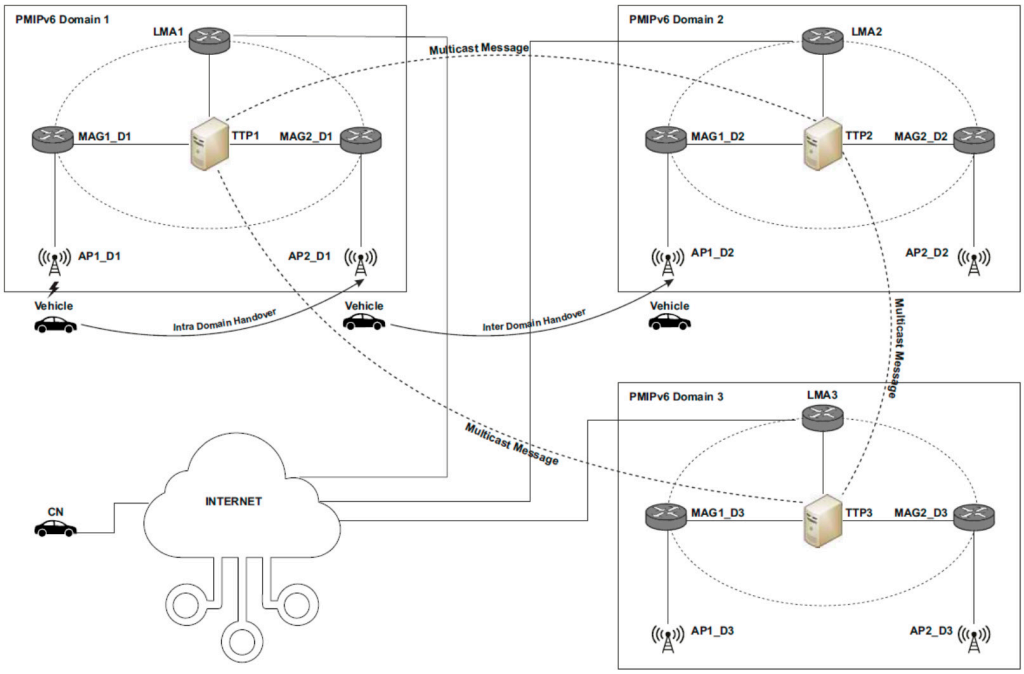
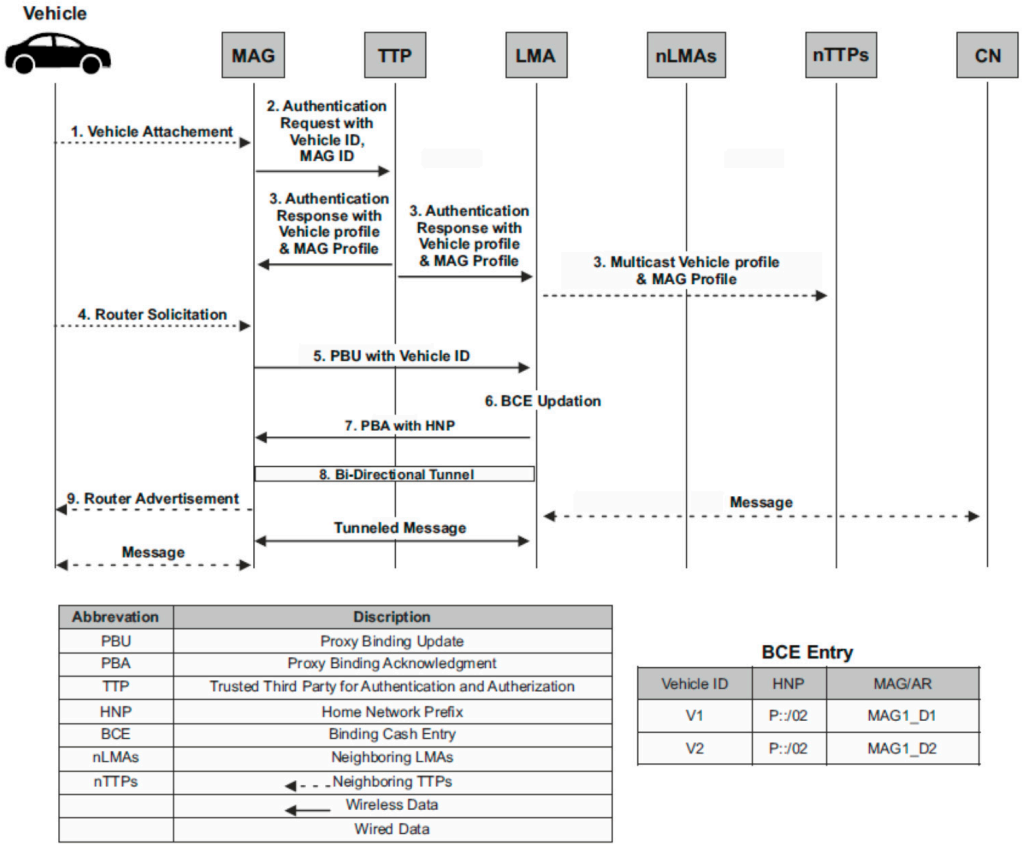


Figure 2. Multicast-enabled architecture for handover for VANET.

3.2. Message Flow Diagram during Intra-Domain Handover in PMIPv6 for VANET

When a vehicle changes its attachment point from one MAG to another MAG in the same PMIPv6 domain, an intra-domain handover is the result. Figure 4 illustrates the sequence of messages that are swapped among various network entities, such as the LMA/MAG [19–21] and TTP, during an intra-domain handover. By sending a PBU signal to the LMA and requesting to be deregistered, the previous MAG starts the disengagement procedure in step 1. The LMA then starts a timer. The vehicle's entry is then deleted from the BCE after waiting for the threshold duration for a binding update request from the new

MAG. After receiving the request from the new MAG, it transmits the PBA message to the previous MAG, calling for the removal of the vehicle binding status in step 2. In step 3, when a vehicle sends a router solicitation message to a new MAG requesting attachment, for authentication, it then sends a request to a TTP already present in the local domain. It includes the vehicle ID and the MAG ID. If the vehicle is already authenticated, then its authentication information would have been communicated earlier, during the initial connection to the PMIPv6 domain. For this local TTP, it then multicasts the authentication request to the neighboring TTPs in step 5. The TTP having the authentication information then unicasts the authentication information back to the local TTP in step 6.



Abbrevation	Discription
PBU	Proxy Binding Update
PBA	Proxy Binding Acknowledgment
TTP	Trusted Third Party for Authentication and Autherization
HNP	Home Network Prefix
BCE	Binding Cash Entry
nLMAs	Neighboring LMAs
nTTPs	Neighboring TTPs
	Wireless Data
	Wired Data

BCE Entry

Vehicle ID	HNP	MAG/AR
V1	P::/02	MAG1_D1
V2	P::/02	MAG1_D2

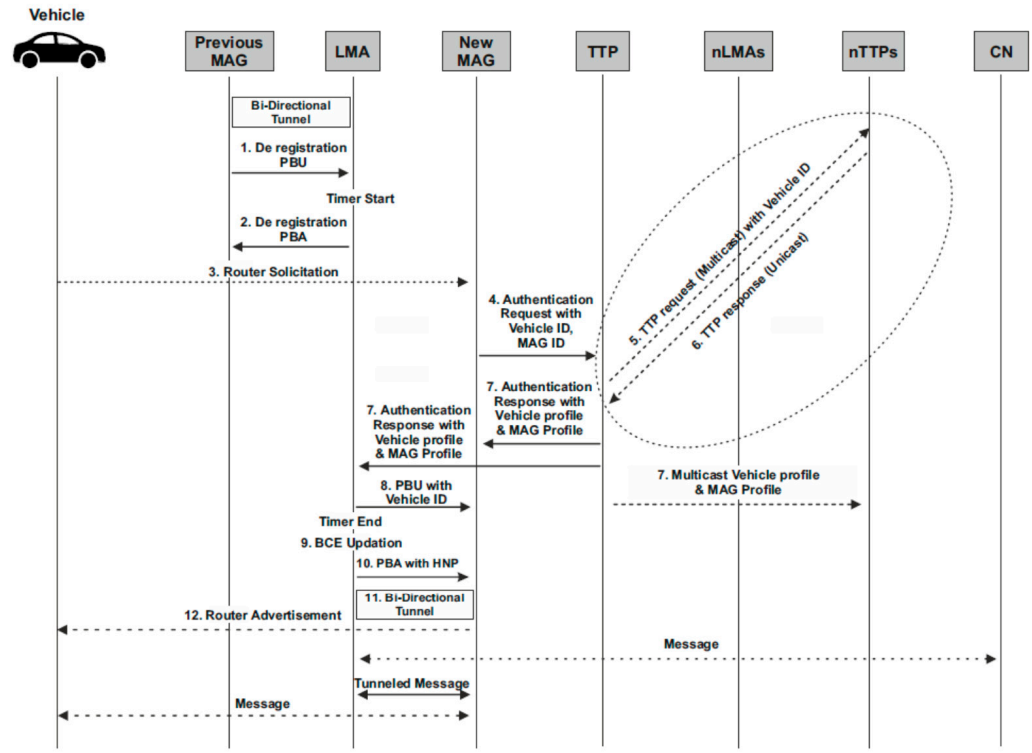
Figure 3. Sequence diagram when a vehicle connects to the PMIPv6 domain.

Upon successful authentication, the TTP will send the authentication response consisting of the vehicle and MAG profiles to the MAG and LMA in step 7. In addition to this, the TTP also multicasts this profile information to the neighboring TTPs so that, later, during the inter-domain handover, this information can be used. The new MAG then transmits the PBU message to the LMA in step 8 and the vehicle's BCE is then updated by tying the same HNP to the new MAG in step 9. In step 10, the PBA message is delivered by the LMA to the new MAG [22,23]. Considering this, it creates a new, bidirectional tunnel between the LMA and the new MAG during step 11. Following this, the new MAG sends the vehicle a router advisory message that contains the same HNP (step 12). The vehicle will not be aware of the above because the HNP will be preserved throughout the transfer.

3.3. Message Flow Diagram during Inter-Domain Handover in PMIPv6 for VANET

When a vehicle changes its attachment point from one MAG to another MAG in a different PMIPv6 domain, an inter-domain handover is the result. Figure 5 depicts the sequence diagram of messages that are traded among various network entities such as the LMA/MAG and TTP during an inter-domain handover. Upon receiving the attachment request from the vehicle in step 1, the new MAG forwards the authentication request

to the TTP present in the local domain in step 2. The TTP multicasts the authentication request to the neighboring TTPs in step 3, and if the vehicle was already authenticated, then its authentication information would have been communicated earlier, during the initial connection or during some intra-domain handover to the PMIPv6 domain. The TTP having the authentication information then unicasts the authentication information back to the local TTP in step 4. Upon successful authentication, the TTP will send the authentication response consisting of the vehicle and MAG profile to the MAG and LMA in step 5. In addition to this, the TTP also multicasts this profile information to the neighboring TTPs so that, later, during the other inter-domain handover, this information can be used. In step 6, when a new MAG seeks an attachment, the vehicle's router will send a solicitation message; the new MAG then transmits a PBU message to the new LMA in step 7 and the previous LMA receives a PBU message from the new LMA in step 8. In step 9, the new LMA receives the PBA message from the previous LMA. Consequently, this creates a bidirectional tunnel connecting the previous and new LMAs during step 10. Step 11 of the process updates the BCE by coupling the same HNP to the new MAG, and in step 12, the PBA message is sent to the new MAG by the new LMA. In step 13, a new, bidirectional tunnel will be constructed between the new LMA and the new MAG. In step 14, the new MAG sends the vehicle a router advertisement message with the same HNP. The vehicle will not be aware of any of the above because the HNP is preserved throughout the transfer.



BCE Entry during Intra handover

Vehicle ID	HNP	MAG/AR
V1	P::/02	MAG1_D1
V1	P::/02	MAG2_D1

Figure 4. Sequence diagram for intra-domain handover for a vehicle in the PMIPv6 domain.

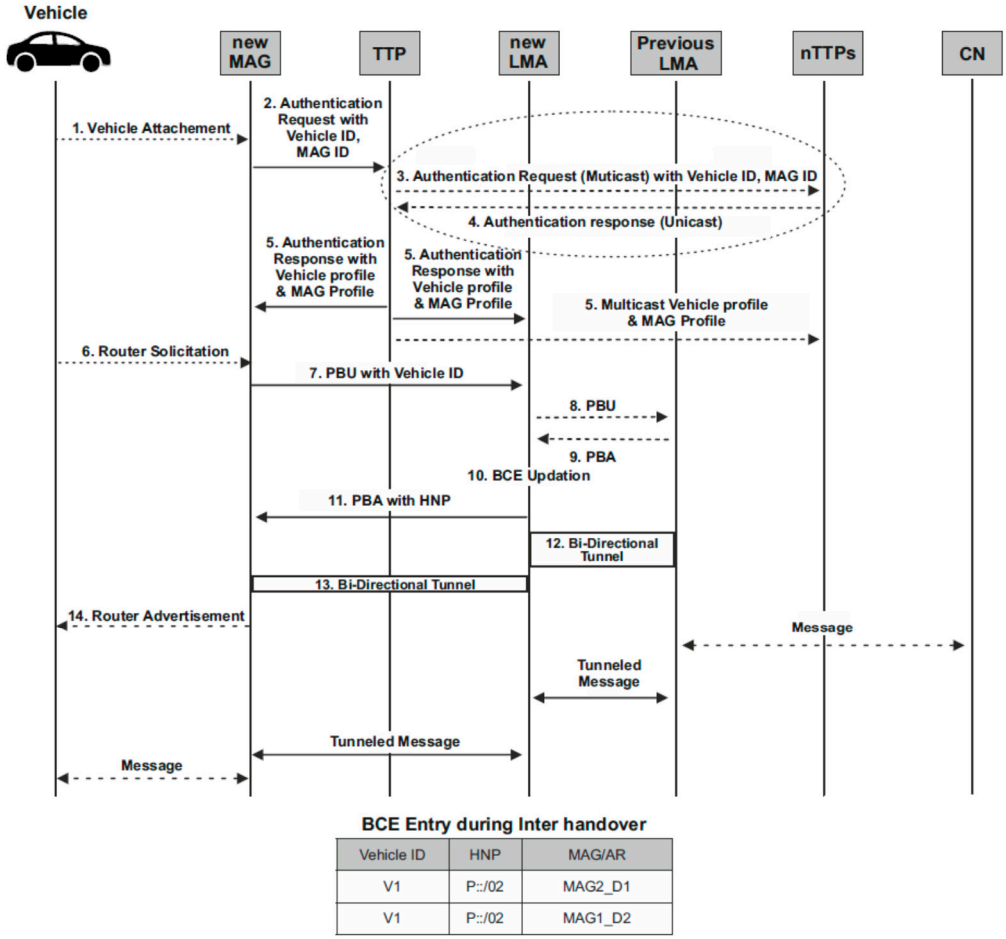


Figure 5. Sequence diagram for inter-domain handover for a vehicle in the PMIPv6 domain.

4. Numerical Analysis

The architecture specified in Figure 3 is used to determine the overall cost of sending a packet, TC_{PMIPv6}^{VANET}, while varying various parameters for analysis purposes. Table 1 [19] provides a collection of the formal notation, abbreviations, and symbols used in analyzing the intra-domain and inter-domain handover costs for vehicles in PMIPv6.

Table 1. List of parameters used to analyze the handover cost of a vehicle.

Parameter	Description
$T_{\text{veh1}-\text{veh2}}/\text{H}_{\text{veh1}-\text{veh2}}$	Transmission cost or hop count of transmitting a packet from one vehicle to another vehicle
$T_{\text{TTP1}-\text{TTP2}}/\text{H}_{\text{TTP1-TTP2}}$	Cost of sending a packet from TTP1 to TTP2 and calculated as $\sqrt{1 + N_{\text{Veh/LMA}}}$
TP	Binding update/lookup cost at LMA/MAG
T_{setup}	Setup cost of a vehicle and MAG to obtain initial connection in PMIPv6 domain
$N_{\text{Veh}/MAG}$	Number of vehicles attached per MAG
$N_{\text{MAG/LMA}}$	Number of MAGs connected to LMA
$S_{control}$	Size of control packet transmitted (bytes)
S_{Data}	Data packet's size (bytes) during transmission
$T_{\text{LMA}-\text{LMA}}$	Cost of sending a packet from LMA1 to LMA2
β	At LMA/MAG, the unit cost for a vehicle lookup
τ	Cost per hop/unit transmission cost for a packet to travel across a wired link
μ	Cost per hop/unit transmission cost for a packet to travel on a wireless link
S_{TTP}	Size (bytes) of the authentication-related control packet

4.1. Intra-Domain Handoff for Vehicles in PMIPv6 with Authentication

The total cost of packet delivery (TC^{VANET}_{PMIPv6}) in VANET in particular has three components, namely the authentication cost ($T^{VANET}_{Authentication}$) with a trusted third party (TTP), the binding update cost (BUC^{VANET}_{PMIPv6}), and the packet delivery cost (PDC^{VANET}_{PMIPv6}). Therefore, Equation (1) represents the total packet delivery cost (TC^{VANET}_{PMIPv6}) as the sum of these three component costs.

$$TC^{VANET}_{PMIPv6} = T^{VANET}_{Authentication} + BUC^{VANET}_{PMIPv6} + PDC^{VANET}_{PMIPv6} \quad (1)$$

The authentication of each vehicle along with the network entities is crucial in ensuring secure communication. As a result, the authentication procedure includes both the authentication of vehicles and network entities such as the MAG and LMA. Additionally, it was presumed that each PMIPv6 domain would have a trusted third-party (TTP) server in place, making the TTP responsible for authenticating each entity. Furthermore, it is believed that all TTPs are linked and situated one hop apart. Thus, the authentication cost, $T^{VANET}_{Authentication}$, is expressed as in Equation (2) as the sum of the cost of the authentication of network entities and the cost of the authentication of mobile entities such as vehicles.

$$T^{VANET}_{Authentication} = T^{VANET}_{Network-Entities} + T^{VANET}_{Mobile-Entities} \quad (2)$$

Network entities and the TTP server will exchange authentication control messages, S_{TTP}, throughout the course of the authentication procedure. The PMIPv6 domain contains several MAGs; each MAG will send a control message to the TTP server for authentication, and the TTP server will respond by sending the control message back to the MAG. In the same way, the LMA sends the control message to the TTP, and, in response, the TTP will send a control message back to the LMA. Hence, the cost of the authentication of network entities $T^{VANET}_{Network-Entities}$ can be as stated in Equation (3).

$$T^{VANET}_{Network-Entities} = N_{MAG} \times (S_{TTP} \times 2T_{MAG-TTP}) + S_{TTP} \times 2T_{LMA-TTP} \quad (3)$$

Secure communication requires the validation of every vehicle. A link between the vehicle and the MAG must be created to authenticate a vehicle, and this requires the setup cost, T_{Setup}. The control message, S_{TTP}, is sent by the MAG with the authentication request to the TTP server. As a result, each vehicle in the PMIPv6 domain will send this control message to the TTP server through the MAG, and once the authentication is complete, the TTP server will send the authentication control message back to the MAG. Hence, the authentication cost of mobile entities ($T^{VANET}_{Mobile-Entities}$) is as represented in Equation (4).

$$T^{VANET}_{Mobile-Entities} = N_{Veh} \times \left(T_{Setup} + Max(S_{TTP} \times 2T_{MAG-TTP}, S_{TTP} \times T_{TTP-LMA})\right) \quad (4)$$

Therefore, from Equations (3) and (4), the authentication cost $T^{VANET}_{Authentication}$ expressed in Equation (2) can be characterized as in Equation (5).

$$\begin{aligned} T^{VANET}_{Authentication} = \quad & N_{MAG} \times (S_{TTP} \times 2T_{MAG-TTP}) + S_{TTP} \times 2T_{LMA-TTP} + N_{Veh} \\ & \times \left(T_{Setup} + Max(S_{TTP} \times 2T_{MAG-TTP}, S_{TTP} \times T_{TTP-LMA})\right) \end{aligned} \quad (5)$$

Once authentication is complete, the TTP server multicasts the authentication response to the corresponding LMA, as well as the TTPs of neighboring PMIPv6 domains, for inter-domain handover. The binding update cost (BUC^{VANET}_{PMIPv6}) concerns the cost of constructing a special, two-way tunnel connecting the MAG and LMA, $T_{Tunnel-Establishment}$, as stated in Equation (6). This tunnel is then used to exchange the data packets destined for the vehicle from a correspondent node (CN) or vice versa. If the given vehicle's entry cannot be in the BCE, it then performs the registration of a new MAG; otherwise, a BCE lookup for the vehicle is performed. Each connected vehicle has an entry stored in the BCE that contains information on the vehicle's ID, its home network prefix (HNP), a proxy care-of-address

(p-CoA), and the IP address of the associated MAG. The BUC_{PMIPv6}^{VANET} in VANET is expressed as follows in Equation (6).

$$BUC_{PMIPv6}^{VANET} = T_{Tunnel-Establishment} \quad (6)$$

Building a bidirectional tunnel between the MAG and LMA requires the transmission of two control messages. One of these messages is a PBU from the MAG to LMA, and the other is a PBA from the LMA to MAG. As a result, it costs twice as much for network entities to exchange a control packet $(T_{MAG-LMA})$. The control packet's size, $S_{Control}$, depends on the mobility option, mobility header, and IPv6 header size. Therefore, the tunnel establishment cost, $T_{Tunnel-Establishment}$, is expressed as follows in Equation (7).

$$T_{Tunnel-Establishment} = S_{Control} \times 2T_{MAG-LMA} \quad (7)$$

After the CN and vehicle have established a secure connection, packet exchange can begin. A packet produced by the CN is transferred to the LMA in the first phase. The LMA looks for a BCE entry for the intended vehicle and any associated MAGs. When it locates them, the LMA sends the packet across a secure bidirectional tunnel to the related MAG, and, finally, the MAG transmits the packet to the designated vehicle. Data packets, S_{Data}, are sent across wired and wireless networks. For ease of use, wireless connections are taken for the CN to the MAG and the MAG to the vehicle. Wired links between the MAG and LMA are taken into consideration in the same reference. Given that wireless networks are unstable and have a major impact on the cost of packet delivery, here, μ is used to represent the unit cost of packet transmission over a wired link, and τ is taken to represent the unit cost of packet transmission over a wireless link. A packet's transmitting cost could be specified as in Equation (8).

$$PDC_{PMIPv6}^{VANET} = S_{Data} \times \left(\mu \times T_{CN-MAG} + \tau \times 2T_{LMA-MAG} + \mu \times T_{MAG-Veh}\right) + T_P \quad (8)$$

where the processing cost, Tp, as expressed in Equation (9), comprises the lookup cost in the BCE; in Equation (9), β represents the unit cost of lookup at the LMA.

$$T_P = \beta \times \log(N_{MAG} \times N_{Veh/MAG}) \quad (9)$$

Thus, Equations (8) and (9), when combined, give the cost of sending a packet PDC_{PMIPv6}^{VANET} as expressed in Equation (10).

$$\begin{aligned} PDC_{PMIPv6}^{VANET} = \quad & S_{Data} \times \left(\mu \times T_{CN-MAG} + \tau \times 2T_{LMA-MAG} + \mu \times T_{MAG-Veh}\right) \\ & + \beta \times \log(N_{MAG} \times N_{Veh/MAG}) \end{aligned} \quad (10)$$

Therefore, Equations (5), (7) and (10), give rise to Equation (11) as the total cost (TC_{PMIPv6}^{VANET}) of packet delivery in PMIPv6 for VANET [23].

$$\begin{aligned} TC_{PMIPv6}^{VANET} = \quad & N_{MAG} \times (S_{TTP} \times 2T_{MAG-TTP}) + S_{TTP} \times 2T_{LMA-TTP} + N_{Veh} \\ & \times \left(T_{Setup} + Max(S_{TTP} \times 2T_{MAG-TTP}, \right. \\ & \left. S_{TTP} \times T_{TTP-LMA})\right) + S_{Control} \times 2T_{MAG-LMA} + S_{Data} \\ & \times \left(\mu \times T_{CN-MAG} + \tau \times 2T_{LMA-MAG} \right. \\ & \left. + \mu \times T_{MAG-Veh}\right) + \beta \times \log(N_{MAG} \times N_{Veh/MAG}) \end{aligned} \quad (11)$$

4.2. Intra-Domain Handover for VANET in PMIPv6 with Multicasting

The intra-domain handover for VANET in PMIPv6 for the proposed architecture is represented by Equation (12).

$$TC_{Intra-PMIPv6}^{VANET} = T_{Intra-Authentication}^{VANET} + BUC_{Intra-PMIPv6}^{VANET} + PDC_{Intra-PMIPv6}^{VANET} \quad (12)$$

The authentication cost, $T^{VANET}_{Intra-Authentication}$, will have the component $T^{VANET}_{Intra-Network-Entities}$, which is the same as $T^{VANET}_{Network-Entities}$ in Equation (3). During intra-domain handoff, if the TTP of the local PMIPv6 domain has information about the vehicle, then it is authenticated; otherwise, the authentication request from the TTP present in the local PMIPv6 domain is multicasted to neighboring TTPs, and the TTP that has the authentication information will unicast the authentication response back to the requested TTP. The cost of authentication for vehicles includes the minimum cost required to multicast to neighboring TTPs. Thus, the authentication cost for vehicle, $T^{VANET}_{Intra-Mobile-Entities}$ is expressed as in Equation (13).

$$\begin{aligned} T^{VANET}_{Intra-Mobile-Entities} = \; & N_{Veh} \times \left(T_{Setup} + Max(S_{TTP} \times 2T_{MAG-TTP}, S_{TTP} \right. \\ & \left. \times T_{TTP-LMA})\right) + (S_{TTP} \\ & \times Min(2T_{TTP1-TTP2}, 2T_{TTP1-TTP3,}, \ldots\ldots 2T_{TTP1-TTPn})) \end{aligned} \tag{13}$$

The binding update cost for intra-domain handoff, $BUC^{VANET}_{Intra_{-PMIPv6}}$, for VANET in PMIPv6 is same as BUC^{VANET}_{PMIPv6} in Equation (7), and the packet delivery cost for intra $-$ domain handoff, $PDC^{VANET}_{Intra-PMIPv6}$, is also same as PDC^{VANET}_{PMIPv6} in Equation (10). Therefore, referring to Equations (3), (7), (10) and (13), they give rise to Equation (14) as the total cost, $TC^{VANET}_{Intra-PMIPv6}$, for intra-domain handover for the proposed model [23].

$$\begin{aligned} TC^{VANET}_{Intra-PMIPv6} = \; & N_{MAG} \times (S_{TTP} \times 2T_{MAG-TTP}) + S_{TTP} \times 2T_{LMA-TTP} + N_{Veh} \\ & \times \left(T_{Setup} + Max(S_{TTP} \times 2T_{MAG-TTP}, S_{TTP} \times T_{TTP-LMA})\right) \\ & + (S_{TTP} \times Min(2T_{TTP1-TTP2}, 2T_{TTP1-TTP3,}, \ldots\ldots 2T_{TTP1-TTPn})) \\ & + S_{Control} \times 2T_{MAG-LMA} + S_{Data} \\ & \times \left(\mu \times T_{CN-MAG} + \tau \times 2T_{LMA-MAG} + \mu \times T_{MAG-Veh}\right) + \beta \\ & \times \log(N_{MAG} \times N_{Veh/MAG}) \end{aligned} \tag{14}$$

4.3. Cost of Inter-Domain Handover in PMIPv6 for VANET

Originally, inter-domain handover was not supported by PMIPv6. For inter-domain handover, the IETF takes into consideration the usage of the previously suggested technique, Mobile IPv6 (MIPv6). The problems in MIPv6, such as duplicate address detection (DAD), Home Agent Binding Update (HA-BU), and Correspond Node-Binding Update (CN-BU), which are transmitted in MIPv6, increase the latency. Our proposed architecture suggests a new approach to facilitating inter-domain handover by using the method of multicasting the authentication information with PMIPv6. By adding the multicast facility to TTPs, the Layer 4 connection is maintained in both the intra-domain and inter-domain handover of vehicles, which was not formerly supported in PMIPv6 mobility management protocols. The cost of inter-domain handoff for VANET for the proposed architecture is expressed by Equation (15).

$$TC^{VANET}_{Inter-PMIPv6} = T^{VANET}_{Inter-Authentication} + BUC^{VANET}_{Inter-PMIPv6} + PDC^{VANET}_{Inter-PMIPv6} \tag{15}$$

The authentication cost required in authenticating the network entities such as the LMA and MAG is represented as $\left(T^{VANET}_{Inter-Network-Entities}\right)$, whereas the cost of mobile entities' authentication is represented by $\left(T^{VANET}_{Inter-Mobile-Entities}\right)$. Therefore, the authentication cost for inter-domain handover for VANET in PMIPv6 is expressed as in Equation (16).

$$T^{VANET}_{Inter-Authentication} = T^{VANET}_{Inter-Network-Entities} + T^{VANET}_{Inter-Mobile-Entities} \tag{16}$$

Network entities and the TTP server will exchange authentication control messages, S_{TTP}, throughout the course of the authentication procedure. The PMIPv6 domain contains several MAGs, and each MAG will send a control message to the TTP server for authentication, and the TTP server will respond by sending a control message back to the MAG. In the same way, the LMA sends the control message to the TTP, and, in response, the TTP

will send the control message back to the LMA. Hence, the authentication cost of network entities $T^{VANET}_{Inter-Network-Entities}$ can be expressed as in Equation (17).

$$T^{VANET}_{Inter-Network-Entities} = N_{MAG} \times (S_{TTP} \times 2T_{MAG-TTP}) + S_{TTP} \times 2T_{LMA-TTP} \quad (17)$$

A connection between a vehicle and MAG requires the setup cost, T_{Setup}, for the authentication of every vehicle. The MAG is responsible for generating and forwarding the authentication request to the TTP server utilizing an authentication control message, S_{TTP}, on the vehicle's behalf. Consequently, an authentication control message, S_{TTP}, will be delivered for each vehicle present in the PMIPv6 domain, to the TTP server, via the MAG. After authentication is complete, the TTP will send the authentication control message back to the MAG. During inter-domain handoff, if the TTP of the local PMIPv6 domain has information about the vehicle, then it is authenticated; otherwise, the authentication request from the TTP present in the local PMIPv6 domain is multi-casted to neighboring TTPs and the TTP that has the authentication information will unicast the authentication response back to the requested TTP. The cost of authentication for vehicles includes the minimum cost required to multicast to neighboring TTPs. Hence, the cost of mobile entities' authentication for inter-domain handoff, $\left(T^{VANET}_{Inter-Mobile-Entities}\right)$, can be expressed as in Equation (18).

$$\begin{aligned} T^{VANET}_{Mobile-Entities} = \; & N_{Veh} \times \left(T_{Setup} + Max(S_{TTP} \times 2T_{MAG-TTP}, \right. \\ & S_{TTP} \times T_{TTP-LMA})) + (S_{TTP} \\ & \left. \times Min(2T_{TTP1-TTP2}, 2T_{TTP1-TTP3,}, \ldots\ldots 2T_{TTP1-TTPn})\right) \end{aligned} \quad (18)$$

Therefore, from Equations (17) and (18), the authentication cost for inter-domain handover in VANET [24–27] in PMIPv6, $T^{VANET}_{Inter-Authentication}$, expressed in Equation (16), can be represented by Equation (19).

$$\begin{aligned} T^{VANET}_{Inter-Authentication} = \; & N_{MAG} \times (S_{TTP} \times 2T_{MAG-TTP}) + S_{TTP} \times 2T_{LMA-TTP} + N_{Veh} \times \\ & (T_{Setup} + Max(S_{TTP} \times 2T_{MAG-TTP}, S_{TTP} \times T_{TTP-LMA})) + \\ & (S_{TTP} \times Min(2T_{TTP1-TTP2}, 2T_{TTP1-TTP3,}, \ldots\ldots 2T_{TTP1-TTPn})) \end{aligned} \quad (19)$$

The binding update cost, $BUC^{VANET}_{Inter-PMIPv6}$, for inter-domain handoff for VANET in the proposed model is expressed in Equation (20). It includes the costs for both the construction of a tunnel between the new MAG and the new LMA and a tunnel connecting the previous LMA and the new LMA. During tunnel establishment, the control message, $S_{Control}$, will be exchanged twice by the LMA and MAG.

$$BUC^{VANET}_{Inter-PMIPv6} = S_{Control} \times \left(2T_{MAG-LMA} + 2T_{LMA-LMA}\right) \quad (20)$$

Meanwhile, the packet delivery cost for inter − domain handoff, $PDC^{VANET}_{Inter-PMIPv6}$, is the same as PDC^{VANET}_{PMIPv6} in Equation (10).

Therefore, from Equations (10), (19) and (20), the total cost for inter-domain handover, $TC^{VANET}_{Inter-PMIPv6}$, represented in Equation (15) can be represented by Equation (21).

$$\begin{aligned} TC^{VANET}_{Inter-PMIPv6} = \; & N_{MAG} \times (S_{TTP} \times 2T_{MAG-TTP}) + S_{TTP} \times 2T_{LMA-TTP} + N_{Veh} \\ & \times \left(T_{Setup} + Max(S_{TTP} \times 2T_{MAG-TTP}, S_{TTP} \times T_{TTP-LMA})\right) \\ & + (S_{TTP} \times Min(2T_{TTP1-TTP2}, 2T_{TTP1-TTP3,}, \ldots\ldots 2T_{TTP1-TTPn}) \\ & + S_{Control} \times (2T_{MAG-LMA} + 2T_{LMA-LMA}) + S_{Data} \\ & \times \left(\mu \times T_{CN-MAG} + \tau \times 2T_{LMA-MAG} + \mu \times T_{MAG-Veh}\right) + \beta \\ & \times \log(N_{MAG} \times N_{Veh/MAG}) \end{aligned} \quad (21)$$

5. Result Analysis

In this section, the suggested scheme's performance is explained. The total packet delivery cost for intra-domain and inter-domain handover for VANET in PMIPv6 with the IP multicasting approach and without multicasting is analyzed. The total cost relies on several components, including the binding update, the authentication of network entities such as the LMA/MGA along with vehicles, and the packet delivery costs, as described in the previous section. By assessing the impact on the total cost of packet delivery by varying the number of parameters, such as the MAGs present in the PMIPv6 domain, and the unit transmission cost for wired and wireless links, the setup time cost is observed. This part also includes a comparison study of the factors under consideration with and without the use of IP multicasting of authentication information in intra-domain handover, as well analyzing the total cost in the inter-domain handover for VANET in the proposed architecture. The different parameter values [19] used in analyzing the cost are listed in Table 2.

Table 2. Parameter values utilized in analyzing the handover cost of vehicle for VANET using PMIPV6.

Variable Used	Default Value	Minimum	Maximum
T_{setup}(ms)	200	100	500
$N_{Veh/MAG}$	200	100	1000
$N_{MAG/LMA1}$	20	10	200
$N_{MAG/LMA2}$	30	10	300
$N_{MAG/LMA3}$	50	10	500
$T_{MAG\text{-}LMA}/H_{MAG\text{-}LMA}$	20	10	100
$T_{Veh\text{-}MAG}/H_{Veh\text{-}MAG}$	1	1	1
$T_{CN\text{-}MAG}/H_{CN\text{-}MAG}$	1	1	1
$T_{MAG\text{-}TTP}/H_{LMA\text{-}TTP}$	1	1	1
$S_{control}$ (*bytes*)	50	50	50
S_{data} (*bytes*)	1024	1024	1024
$T_{LMA1-LMA2}$	20	1	100
β	1	1	10
τ	1	1	10
μ	4	1	10
S_{TTP} (bytes)	100	100	100

To establish a communication link, we require a wired and wireless connection that involves a fixed setup cost associated with it. Due to the unreliability of wireless connectivity, the setup time for the communication channel is longer in wireless connection. The setup cost has a significant impact on the total packet delivery cost. The effect of varying the setup cost on the overall costs of the suggested architecture, i.e., IP multicasting, and without multicasting, is shown in Figure 6. We estimated the total cost for both the suggested architecture that makes use of IP multicasting and PMIPv6 without multicasting, by varying the setup cost ranging from 100 to 500. When the setup costs vary at 100, 200, and 500, and with the increase in the number of vehicles from 100 to 1000, the total cost marginally increases for the proposed scheme as compared to the PMIPv6 approach of intra-domain handoff. The setup cost and the number of vehicles have no bearing on the final cost when the multicasting of authentication information is taken into account. Due to the proposed architecture, the security is enhanced as authentication is used during intra-domain handoff, and the proposed architecture is able to provide inter-domain handoff by using the IP multicasting scheme.

Figure 7 shows the impact of changes in traffic density and unit transmission cost on the wired link. The total cost for the intra-domain handoff of a vehicle in PMIPv6 increases proportionally to an increase in the wired link's packet's unit transmission cost, τ, from 1 to 10, with IP multicasting and without multicasting. As the unit transmission cost, τ, i.e., the number of hops, increases from 1 to 10, the total cost increases linearly in proportion. Regarding the impact on the total cost calculated with the proposed architecture, and when it is compared with the total cost without multicasting in PMIPv6, we observed very slight

variation, which can be considered negligible on account of the authentication achieved during the intra-domain handover of the vehicle.

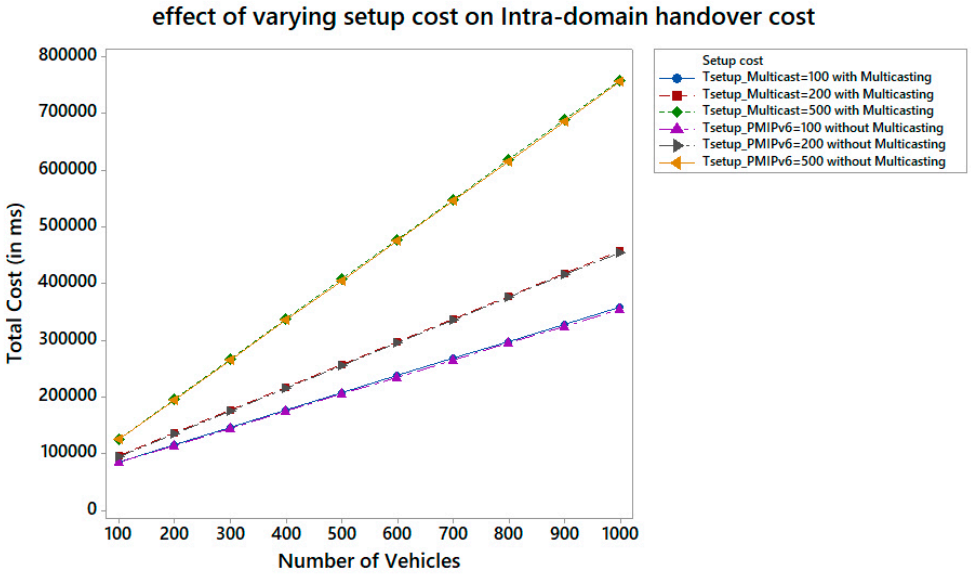


Figure 6. Effect of varying setup cost on intra-domain handoff.

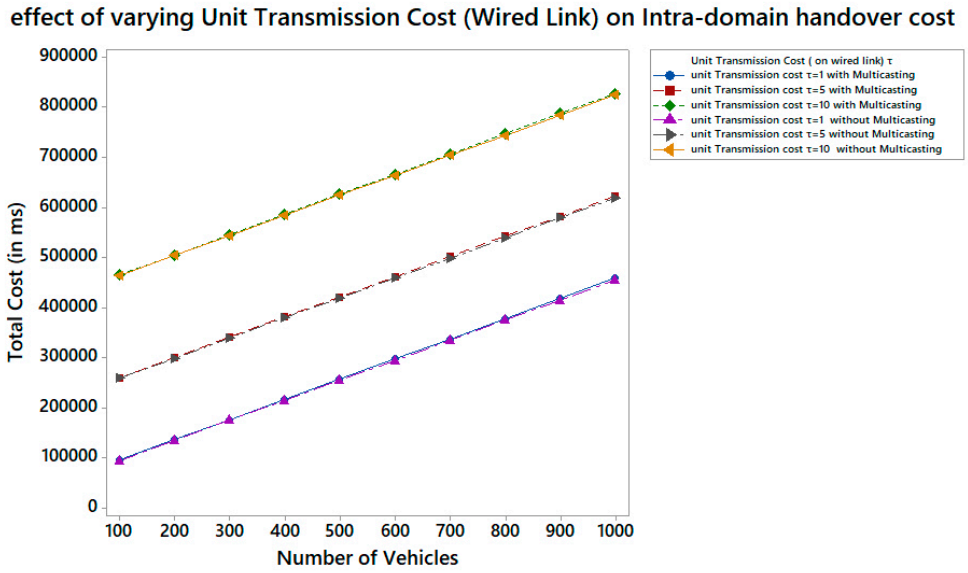


Figure 7. Effect of varying unit transmission cost (wired link) on intra-domain handoff.

Figure 8 illustrates the effect of changing the unit transmission cost on the wireless link in the intra-domain handoff of a vehicle on PMIPv6 with the proposed scheme, as compared to intra-domain handoff in the traditional PMIPv6. We know that as the wireless link delay increases, there is more interference in the wireless channel, and the performance quality of PMIPv6 degrades. The increased latency in the wireless area has little impact on the suggested architecture because PMIPv6 is used. We have varied the unit transmission cost on the wireless link, μ, from 1 to 10 and compared the total cost for the proposed architecture with IP multicasting and the typical PMIPv6 scheme. Because only the PMIPv6 is adjusted to permit inter-domain handover and the intra-domain handover has no impact on the latency, the basic PMIPv6 and the proposed technique share the same intra-domain handover latency.

Originally, inter-domain handover was not supported by PMIPv6. For inter-domain handover, the IETF takes into consideration the usage of the previously suggested technique,

Mobile IPv6 (MIPv6). The problems in MIPv6 include DAD that uses 1000 s latency, which causes a higher delay during inter-domain handover. Our proposed architecture suggests a new approach to facilitating inter-domain handover by using the method of multicasting the authentication information with PMIPv6, in which no problem of duplicate addresses is present. In the proposed architecture, when the TTP authenticates a vehicle, it sends the authentication response to the MAG, and the TTP also multicasts this profile information to the neighboring TTPs so that, later, during the other inter-domain handover, this information can be used. Figure 9 shows the effect of the varying setup cost on inter-domain handoff when setup cost, T_{setup}, is varied from 100 to 500. Figure 10 depicts the effect of the varying unit transmission cost on the wired link, τ, from 1 to 100, and shows that the total cost increases proportionately with an increase in transmission cost, whereas the effect of the varying unit transmission cost on the wireless link, μ, is represented by Figure 11. If we compare the cost of the intra-domain handoff and inter-domain handoff of a vehicle in PMIPv6 with IP multicasting, we observe a slight variation in inter-domain handoff, which may be reduced later.

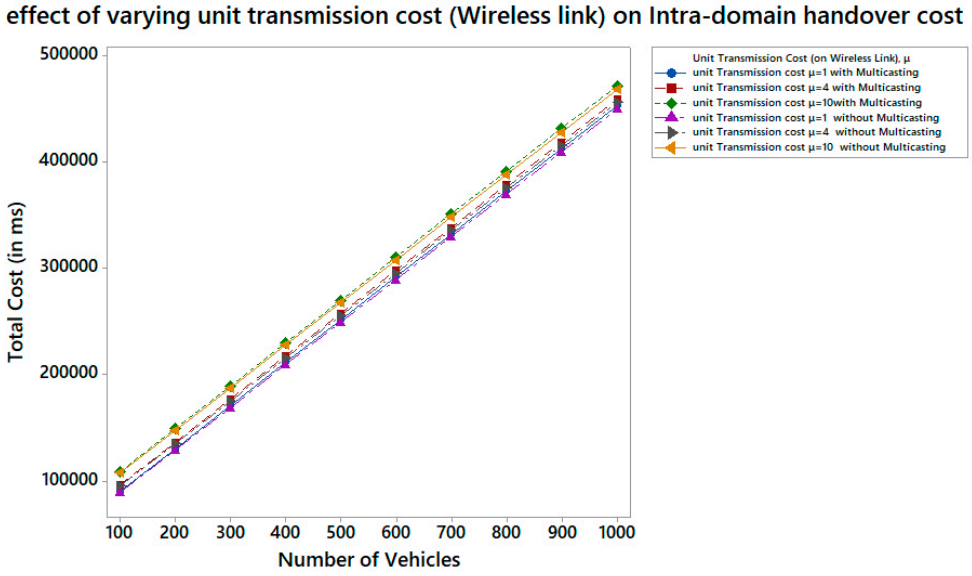


Figure 8. Effect of varying unit transmission cost (wireless link) on intra-domain handoff.

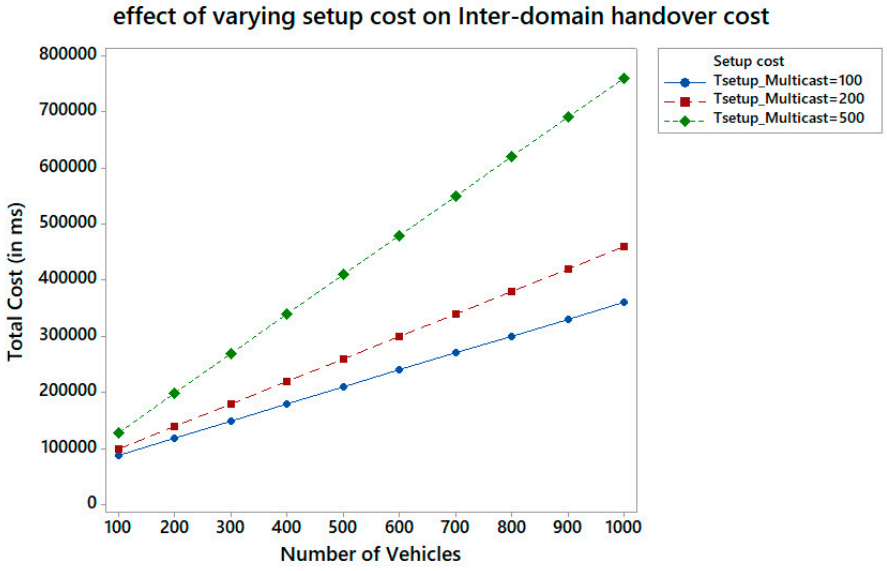


Figure 9. Effect of varying setup cost on inter-domain handoff.

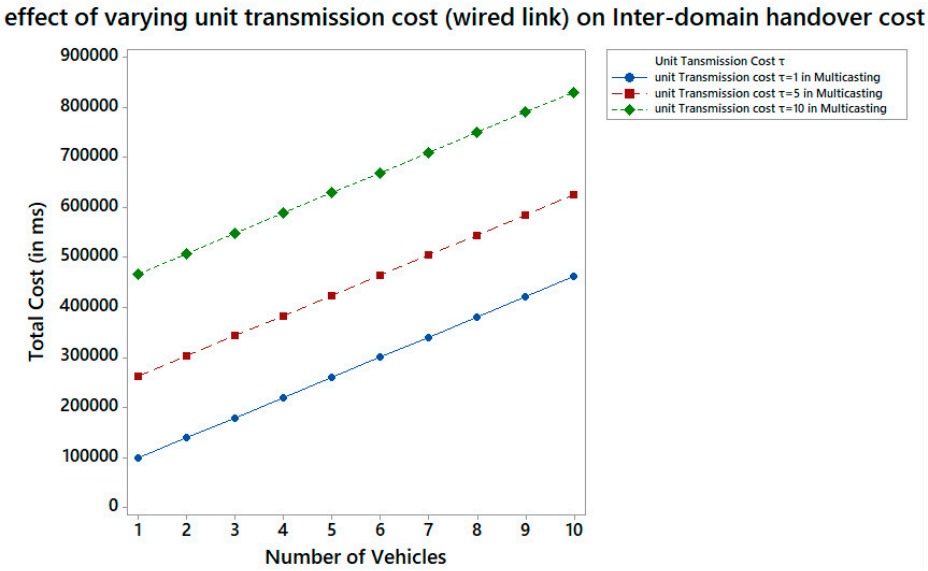


Figure 10. Effect of varying unit transmission cost (wired link) on inter-domain handoff.

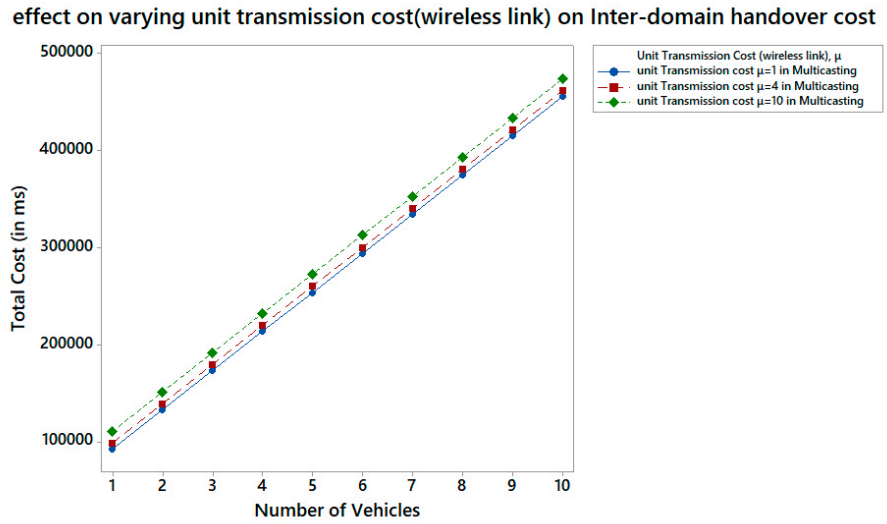


Figure 11. Effect of varying unit transmission cost (wireless link) on intra-domain handoff.

6. Conclusions and Future Work

VANET enables a next-generation communication network that provides vehicle-to-vehicle communication as well as communication between the vehicle and fixed infrastructure. One of the most important responsibilities of VANET is to provide seamless mobility to vehicles. Host-based mobility management protocols and network-based mobility management protocols for ubiquitous services are two categories of IP-based mobility protocols. According to researchers, host-based management protocols are less effective and efficient than network-based management protocols.

The PMIPv6 protocol, which is utilized as a localized mobility management protocol for VANET deployment, is the IP mobility management solution that is more compatible and interoperable. However, PMIPv6 does not support inter-domain handover at all; it is primarily intended for quick intra-domain handover. This article proposed an intra-domain and inter-domain handoff for VANET in PMIPv6 with a multicasting approach and analyzed the total cost of inter-domain and intra-domain handover. Various existing mobility management protocols have shortcomings; for example, MIPv6 supports both intra- and inter-domain handoff but suffers from high handover latency, and it does not support Layer 4 handover. Meanwhile, the PMIPv6 protocol minimizes the problem of high latency but does not support inter-domain handoff. In our proposed architecture, we

have incorporated an authentication procedure to ensure secure handoff communication, and we have used the concept of multicasting authentication information to various trusted servers responsible for authentication, which permits inter-domain handover for VANET in PMIPv6. A cost comparison between the multicasting approach and the case with no multicasting was performed for parameters such as a different number of MAGs, setup costs required in setting up the initial connection, and unit transmission costs for wired and wireless links. Although the proposed approach is more secure than the ones currently in use, the authentication process may include a slight communication overhead, but it is very negligible. In the future, the formation of multicast groups and/or the placement of network components such as the LMA and MAG in the domain could further lower the signaling cost overhead.

Author Contributions: Conceptualization, A.K.G. and G.A.; methodology, A.K.G.; software, G.A.; validation, A.K.T.; formal analysis, A.K.T.; investigation, M.S.; resources, M.S.; data curation, A.K.G.; writing—review and editing, A.K.G.; visualization, A.K.G.; supervision, G.A.; project administration, M.S.; funding acquisition, M.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by Dongseo University, via the "Dongseo Cluster Project" Research Fund of 2023 (DSU-20230006).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Goyal, A.K.; Agarwal, G.; Tripathi, A.K. Network Architectures Challenges Security Attacks Research Domainsand Research-Methodologies in VANET: A Survey. *J. Comput. Netw. Inf. Secur.* **2019**, *11*, 37–44.
2. Goyal, A.K.; Agarwal, G.; Tripathi, A.K.; Sharma, G. *Systematic Study of VANET Applications, Challenges, Threats, Attacks, Schemes and Issues in Research. Green Computing in Network Security*; CRC Press: London, UK, 2022; pp. 33–52.
3. Siang Hoh, W.; Ong, B.L.; Yoon, S.K.; Ahmad, R.B. A Survey of Mobility Management Protocols. ARPN Eng. *Appl. Sci.* **2015**, *10*, 9015–9019.
4. Zhu, K.; Niyato, D.; Wang, P.; Hossain, E.; Kim, D. Mobility and handoff management in vehicular networks: A survey. *Wirel. Commun. Mob. Comput.* **2011**, *11*, 459–476. [CrossRef]
5. Li, C.; Wang, Z. Location-based Security Authentication Mechanism for Ad hoc Network. In Proceeding of the National Conference on Information Technology and Computer, Haifa, Israel, 1 November 2012.
6. Tuysuz, M.F.; Trestian, R. Energy-efficient vertical handover parameters, classification and solutions over wireless heterogeneous networks: A comprehensive survey. *Wirel. Pers. Commun. Int. J.* **2017**, *97*, 1155–1184. [CrossRef]
7. Perkins, C.E. Mobility Support in IPv4. *RFC 3220*. 2002.
8. Johnson, B.; Arkko, J.; Perkins, C.E. Mobility Support in IPv6. *RFC 6275*. 2011.
9. Kong, K.S.; Lee, W.; Han, Y.H.; Shin, M.K.; You, H. Mobility management for all-IP mobile networks: Mobile IPv6 vs. proxy mobile IPv6. *IEEE Wirel. Commun.* **2008**, *15*, 36–45. [CrossRef]
10. Modares, H.; Moravejosharieh, A.; Lloret, J.; Salleh, R.B. A Survey on Proxy Mobile IPv6 Handover. *IEEE Syst. J.* **2016**, *10*, 208–217. [CrossRef]
11. Balfaqih, M.; Ismail, M.; Nordin, R.; Rahem, A.A.; Balfaqih, Z. Fast handover solution for network-based distributed mobility management in intelligent transportation systems. *Telecommu. Syst.* **2017**, *64*, 325–346. [CrossRef]
12. Moravejosharieh, A.; Modares, H. A Proxy MIPv6 Handover Scheme for Vehicular Ad-hoc Networks. *Wirel. Pers Commun.* **2014**, *75*, 609–626. [CrossRef]
13. Tripathi, A.K.; Radhakrishnan, R.; Lather, J.S. Secure and Optimized Authentication Scheme in Proxy Mobile IPv6 (SOASPMIPv6) to reduce Handover Latency. *Int. J. Comput. Netw. Inf. Secur.* **2017**, *9*, 1–12.
14. Leu, F.-Y.; Liu, C.-Y.; Liu, J.-C.; Jiang, F.-C.; Susanto, H. S-PMIPv6: An intra-LMA model for IPv6 mobility. *J. Netw. Comp. Appl.* **2015**, *58*, 180–191. [CrossRef]
15. Li, J.; Lu, H.; Guizani, M. ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs. *IEEE Trans. Parallel Distrib. Syst.* **2015**, *26*, 938–948. [CrossRef]
16. Sheikh, M.S.; Liang, J.; Wang, W. Security. Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 1–25. [CrossRef]

17. Tripathi, A.K.; Kumar Tripathi, S. A Qualitative Analysis of Secured Handover Management Schemes for Mobile IPv6 Enabled Networks. In Proceedings of the 2018 3rd International Innovative Applications of Computational Intelligence on Power, Energy and Controls with their Impact on Humanity, Ghaziabad, India, 1–2 November 2018; Volume 2018, pp. 1–8.
18. Jung, H.; Gohar, M.; Kim, J.I.; Koh, S.J. Distributed Mobility Control in Proxy Mobile IPv6 Networks. *IEICE Trans. Commun.* **2011**, *94*, 2216–2224. [CrossRef]
19. Tuyisenge, L.; Ayaida, M.; Tohme, S.; Afilal, L.E. A mobile internal vertical handover mechanism for distributed mobility management in VANETs. *Veh. Commun.* **2020**, *26*, 455. [CrossRef]
20. Hossain, M.S.; Atiquzzaman, M. Analysis of Proxy Mobile IPv6: A network-based mobility solution. In Proceedings of the 2012 15th International Conference on Computer and Information Technology (ICCIT), Chittagong, Bangladesh, 22–24 December 2012; Volume 795, pp. 338–344.
21. Tripathi, A.K.; Radhakrishanan, R.; Lather, J.S. Impact of wireless link delay on handover latency in Mobile IPv6 environment. *Int. Conf. Issues Chall. Intell. Comput. Tech. (ICICT)* **2014**, *2014*, 424–428.
22. Lee, J.H.; Ernst, T.; Chung, T.M. Cost analysis of IP mobility management protocols for consumer mobile devices. *IEEE Tran. Cons. Electron.* **2010**, *56*, 1010–1017. [CrossRef]
23. Goyal, A.K.; Agarwal, G.; Tripathi, A.K.; Goel, V.; Sharma, G.; Hui, K.L.; Sain, M. A Comprehensive Cost Analysis of Intra-Domain Handoff with Authentication Cost in PMIPv6 for Vehicular Ad Hoc Networks (VANETs). *Electronics* **2022**, *11*, 1625. [CrossRef]
24. Chaehwan, K.; Hyunwoo, H.; Baik, J.-W.; Lee, K.-G. Multicast based Proxy Mobile IPv6 for inter-domain handover. *Math. Comput. Model.* **2013**, *57*, 2863–2872.
25. Jabir, A.J.; Subramaniam, S.K.; Ahmad, Z.Z.; Hamid, N.A. A cluster-based proxy mobile IPv6 for IP-WSNs. *J. Wireless Com. Network* **2012**, *173*, 1–17. [CrossRef]
26. Cho, C.; Choi, J.Y.; Jeong, J.; Chung, T.M. Performance Analysis of Inter-Domain Handoff Scheme Based on Virtual Layer in PMIPv6 Networks for IP-Based Internet of Things. *PLoS ONE* **2017**, *12*, e0170566. [CrossRef] [PubMed]
27. Song, M.; Cho, J.D.; Jeong, J. Analytical Approach of New Random-Walk Based Mobility Management Scheme in IP-Based Mobile Networks. *Inter. J. Adv. Cult. Tech.* **2014**, *2*, 1–13. [CrossRef]