

Article

A Comprehensive Cost Analysis of Intra-Domain Handoff with Authentication Cost in PMIPv6 for Vehicular Ad Hoc Networks (VANETs)

Amit Kumar Goyal ¹, Gaurav Agarwal ², Arun Kumar Tripathi ¹, Vikas Goel ³, Girish Sharma ⁴,
Kueh Lee Hui ^{5,*} and Mangal Sain ^{6,*}

¹ Department of Computer Applications, KIET Group of Institutions, Delhi-NCR, Ghaziabad 201206, India; athroam@gmail.com (A.K.G.); mailtoaruntripathi@gmail.com (A.K.T.)

² Department of Computer Science and Engineering, Invertis University Bareilly, Bareilly 243001, India; gaurav.a1@invertis.org

³ Department of Information Technology, KIET Group of Institutions, Delhi-NCR, Ghaziabad 201206, India; vikas.goel@kiet.edu

⁴ DSEU Shakarpur Campus, Government of NCT Delhi, Delhi 110092, India; gkps123@gmail.com

⁵ Department of Electrical Engineering, Dong-A University, Busan 49236, Korea

⁶ Division of Computer Engineering, Dongseo University, 47 Jurye-ro, Sasang-gu, Busan 47011, Korea

* Correspondence: leehkueh@dau.ac.kr (K.L.H.); mangalsain1@gmail.com (M.S.)

Abstract: In metro cities, the effective and efficient management of traffic is one of the most demanding and time taking tasks. Vehicular ad hoc networks (VANET) provide unfailing, low-cost solutions for transportation systems with intelligence. VANET, a subclass of mobile ad hoc networks (MANET), allows exchange of information among vehicles and/or roadside devices. VANET can be implemented in numerous application areas such as effective traffic management, safety, and user comfort for drivers as well as passengers. It provides phenomenal growth to both in industries and research communities. Secure mobility and handoff management are the most promising and challenging research issues in VANET. In this paper, we have introduced the security in intra domain mobility handoff in PMIPv6 for VANET. Existing intra handover schemes does not include the authentication cost while evaluating the total packet delivery cost for intra domain handoff. Our proposed scheme includes the authentication cost of an intra-domain handover for evaluating the total packet delivery cost of handover for next-generation mobility management protocols, which is PMIPv6 for the vehicular network. We have considered the vital parameters such as the number of MAGs, setup cost, binding update cost, unit transmission cost for analyzing the total packet delivery cost. Furthermore, a comparative study with authentication and without authentication cost for the considered parameters shows that our proposed scheme secures the handover process with slight variation in cost.

Keywords: VANET; PMIPv6; mobility management; host mobility; network mobility



Citation: 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. <https://doi.org/10.3390/electronics11101625>

Academic Editor: Alexey Vinel

Received: 30 March 2022

Accepted: 16 May 2022

Published: 19 May 2022

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



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Vehicular ad hoc networks [1], consisting of high-speed vehicles along with stationary objects, are infrastructure-neutral, distributed heterogeneous wireless networks. Communication in VANET may be either vehicle-to-vehicle (V2V) in which two vehicles can communicate directly or using multi-hop communication, whereas in vehicle-to-infrastructure (V2I) [2], vehicles and fixed infrastructure known as roadside unit (RSU) [2], such as base station, mobile router (MR) and access point (AP) communicate with each other. A typical VANET communication scenario is shown in Figure 1. Pure ad hoc communication (V2V), pure cellular/WLAN (V2I) and hybrid communication (V2I) architectures are three possible types of communication architectures in VANET. Pure ad hoc communication permits communication via a single hop or multiple hops and stands to vehicle-to-vehicle

(V2V) communication. In pure cellular/WLAN, communication between vehicles and fixed roadside unit takes place, which is referred as vehicle-to-infrastructure communication (V2I). On the other hand, the hybrid architecture, consisting of a vehicle with moving router (MR), permits the hybrid vehicle (HV) communication mode in which multi-hop routing may be used to connect the vehicles to RSU, with other vehicles acting as gateways.

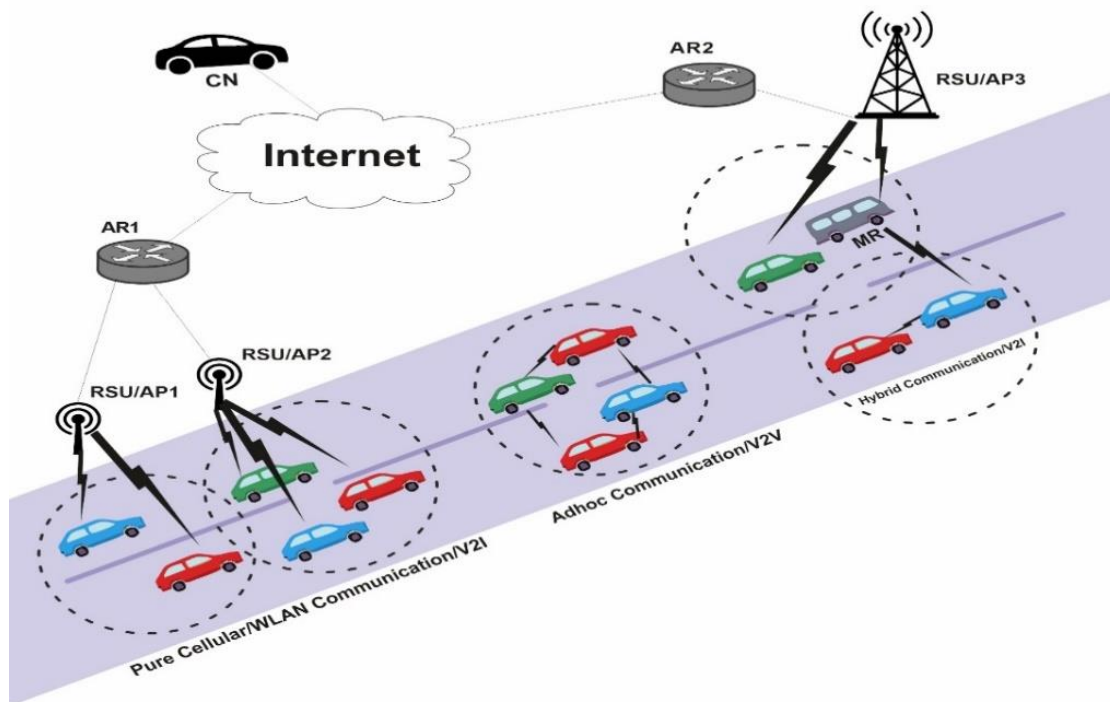


Figure 1. VANET Communication Architecture.

Mobility management [3,4] is one of the most significant and difficult concerns for VANET. Serving networks can use mobility management to detect a vehicle's point of attachment (location management [5]) and maintain a vehicle's connection while it travels around (handover management [6]). Because of the distinctions in the above three communication architectures, the mobility management solutions for each can be developed differently to achieve the better results. The Internet engineering task force (IETF) has specified numerous standards which were used for developing various protocols for mobility management. These protocols are categorized either into host-based mobility management protocol where host is involved in mobility signaling to provide global mobility or into network-based mobility protocols in which network handles the localized mobility, as shown in Figure 2.

Mobile IP, which comes in two versions, MIPv4 [7] and MIPv6 [8,9], well-known IP mobility protocol. It's been standardized to allow host-based mobility. These facilitate IP host mobility by letting to use two different IP addresses: a fixed home address known as (HoA), and an address, known as a care-of-address (CoA), which varies as the IP subnet of vehicle changes. Furthermore, in global mobility also known as host-based mobility, the host take part in the mobility related activities. The serving network, on the other hand, is responsible for mobility-related activities in a network-based management strategy. The network manages the entire IP mobility signaling. Several protocols such as MIPv6, Hierarchical Mobile IPv6 (HMIPv6) [9], and Fast mobile IPv6 (FMIPv6) [9] come under the host-based mobility management category. Similarly, for Network-based proxy mobile IPv6 (PMIPv6) [9,10], Fast handover Proxy Mobile IPv6 (FPMIPv6) [11] are the well-known mobility protocols providing localized mobility.

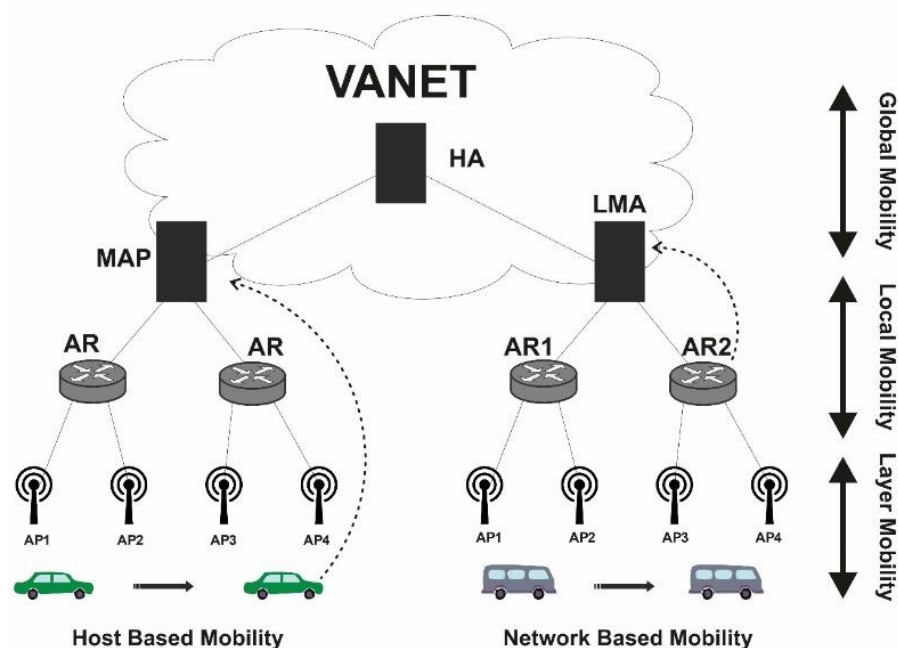


Figure 2. Mobility Classification in Host-based and Network Based.

The remainder of the work is organized in the following manner: Section 2 provides a comprehensive overview of mobility management protocols, and in Section 3 we propose the system model that discusses insight of communication sequence diagram among various network entities for VANET in PMIPv6 domain and the model for evaluating the total cost during intra-domain handover management. Section 4 focuses on the mathematical analysis of cost for intra-domain handover management, whereas Section 5 provides the qualitative result analysis based on various parameters along with comparative study with authentication and without authentication cost has presented and at last, Section 6 summarizes the work with future work in VANET.

2. Related Work

The IETF introduced PMIPv6, the localized network-based mobility management standard, in which the mobile nodes such as vehicles do not participate in mobility-related signaling. PMIPv6 reuses characteristics of MIPv6. In PMIPv6, when a vehicle joins the PMIPv6 mobility domain, the network entity gives the vehicle a unique home network prefix (HNP) [12]. Within the same mobility domain, the vehicle will always be identified by this unique prefix. As a result, the vehicle considers the PMIPv6 domain to be its home network. Figure 3 shows the basic PMIPv6 [12] architecture which encompasses two functional units namely, the mobile access gateway (MAG) [9,13] and an anchor point, known as a local mobility anchor (LMA) [9,13].

The MAG, which work as an access router (AR), has a responsibility to detect the movement of vehicle. On detecting the movement, MAG starts the necessary actions required for handover with the vehicle's LMA. It does so by sending a proxy binding update message (PBU) to LMA, the gateway of the PMIPv6 domain. Furthermore, LMA and MAG are connected by a tunnel to utilize the vehicle's address from its HNP. All traffic meant for a vehicle passes via the LMA, which serves as an anchor point in topology. It is responsible for maintaining the routing and vehicle accessibility within the PMIPv6 domain. LMA additionally maintains the binding state of each registered vehicle via binding cache entry (BCE) [13,14]. The BCE includes the vehicle's identification, its HNP, a proxy registration flag, and also the tunnel's established interface identification. LMA also verifies the authorization status for each MAG. In PMIPv6 domain, when point of attachment of a vehicle changes, the handover may be either a Layer 2 handover, an

Intra-domain handover, or it may be an Inter-domain handover. When a vehicle switches access points within the same MAG, this is known as a Layer 2 handover. The LMA is unaffected by this change because the MAG modifies the vehicle's binding locally. When a vehicle switches its point of attachment between two MAGs attached to the same LMA, an inter-domain handover occurs. By switching PMIPv6's handoff signaling, the MAGs keep the vehicle bound to LMA, whereas in inter-domain handover, the vehicle's attachment points shift between two MAGs connected to distinctive LMAs. Only intra-domain mobility roaming is managed by the PMIPv6 protocol. In PMIPv6, several strategies for handling handover have been presented. In 2012, a Clustered SPMIPv6 [15] was offered as an improved architecture. They used the method of grouping the MAGs into clusters, each with its own cluster Head MAG (HMAG). By executing intra-cluster handoff signaling and providing an efficient path for data connections, the HMAG minimized the strain on LMA. In terms of LMA load, local handoff latency, and transmission cost performance measures, they compared the analytical and numerical results of CSPMIPv6, SPMIPv6, and PMIPv6 protocols. In 2014, for PMIPv6 networks [16], the authors have developed a mobility-aware Dual Pointer Forwarding system. According to them, their mobility-aware binding improvements can reduce packet delivery overhead. They also calculated the cost of binding updates and packet delivery for route optimization and discovered that their system outperformed PMIPv6 and other pointer forwarding techniques in terms of total signaling costs. The effect of optimal pointer chain length and SMR was also looked at. Finally, when compared to PMIPv6 and PF, the proposed PF technique outperformed both in terms of performance and total cost. Another work proposed the constrained application protocol that was based on group mobility [17] and was supposed to support mobility in a web based IoT scenario. One sensor that is responsible for communicating the body sensors' control signals to the web-of-things mobility management system Two sorts of IP addresses, one permanent address used for the sensor IP address, and a temporary address used for the Access Router address. According to the results of their numerical analysis, their proposed protocol outperforms the existing constrained application protocol without group. In 2019, the authors proposed the AE-PMIPv6 scheme [18], which used the BCE at the LMA, as part of the PMIPv6 protocol. They've consolidated the MNs' BCEs, resulted in a reduction in signaling overhead. During the MN's enrolment phase, the planned AE-PMIPv6 system contained the idea of leveraging virtual addressing and addressing pool methods, allowing the MAG to combine the MNs' binding information and issue HNPs ahead of time. Furthermore, the proposed approach allowed the MAG to combine the data of such MNs into a separate BUL, as well as the LMA to combine the required HNPs into a single BCE, resulting in better resource utilization and decreased buffering costs. They devised a mechanism for delivering a seamless changeover for MNs in the urban traffic network. The new approach's potential to reduce network signaling costs and buffering latency has been proved through simulation. Finally, the proposed system was able to obtain HNPs prior to MN handoff/registration by exploiting the addressing pool technique, reducing both signaling costs and handoff latency. The simulation results demonstrated that AE-PMIPv6 outperforms the E-PMIPv6 scheme in respect of buffering cost, signaling cost, and handoff latency. The authors, in 2019, proposed a mobile node group-based handoff technique [19] that minimized handover during travelling. Enhanced Cluster Sensor Proxy Mobile IPv6 combined two strategies to provide a quick handover solution. The first strategy, cluster mobile nodes moving in a group will be allowed in advance before their actual handoff and second method allowed to modify the mobile node's mobility-related signaling during their handover signaling. In comparison to current mobility management processes, they claim that the efficiency of their scheme has been verified by comprehensive simulation tests and numerical analyses.

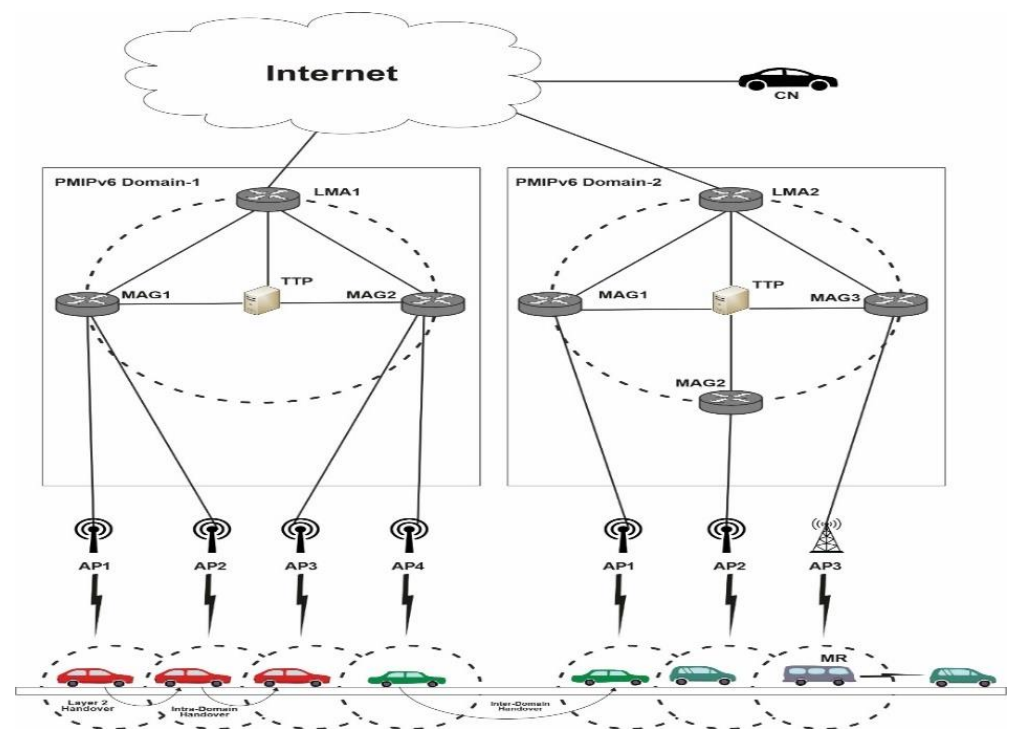


Figure 3. PMIPv6 Architecture in VANET.

However, none of the aforementioned solutions consider authentication costs when calculating total packet delivery costs in PMIPv6 for VANET intra domain handoff. Thus, ignoring this scenario leads to insecure handover, insufficient signaling. To address these problems, we propose a scheme that include the authentication cost in intra-domain handover for evaluating the total cost of packet delivery in next-generation mobility management protocols, PMIPv6 for Vehicular network.

3. Proposed Work

The proposed scheme introduces the security in mobility during hands over. Existing intra handover schemes does not include the authentication cost while evaluating the total packet delivery cost for intra domain handoff in PMIPv6 for VANET. Our proposed scheme includes the authentication cost in intra-domain handover for evaluating the total cost of packet delivery for next-generation mobility management protocols, PMIPv6 for vehicular network.

3.1. Communication Sequence Diagram among PMIPv6 Entities for VANET

Figure 4 depicts the sequence of messages that are exchanged when a vehicle attaches itself to PMIPv6 domain. In steps 1 and 2, when a vehicle connects to an access point connected to one of the MAGs for the first time, a trusted third-party server performs access authentication [20] using the vehicle's identity (TTP) [21]. TTP is responsible for authentication and authorization of network entities such as vehicles, MAGs and LMAs. Upon successful authentication in step 3, the MAG will have Vehicle ID, and the LMA address that will be used in step 4 to send a PBU message. On behalf of the vehicle, the MAG then sends the PBU message along with the Vehicle ID to LMA. The authentication and authorization of MAG is then checked by LMA by sending authentication request to TTP in step 5. After step 6, the MAG is declared as the authorized to send PBU message. In step 7, LMA then sends a proxy binding acknowledgment (PBA) message with vehicle's HNP. It also facilitates access for the vehicle by constructing a bi-directional tunnel to the MAG. After that LMA then creates the binding cache entry (BCE) in step 8. Unlike MIPv6, instead of a tunnel between the LMA and the vehicle, the PMIPv6 generates a

tunnel between the LMA and the MAG. The PBA message received from the LMA allows MAG to replicate the vehicle's home network on the entire access network, and then MAG send a router advertisement (RA) to the vehicle. Following receipt of the RA notification, the vehicle builds its home address by merging the RA message's HNP with its interface address. In PMIPv6, which has the per-vehicle prefix approach only, each vehicle is issued a unique home network prefix. Unlike MIPv6, when travelling within a PMIPv6 domain, the vehicle is issued a unique home address. The bidirectional tunnel [22] allows all messages sent from the vehicle becomes routed through the tunnel to LMA. Any communication intended for the vehicle is received by the LMA, the domain's topological anchor points. The received message is then forwarded to the MAG via the tunnel by the LMA. After eliminating the outer header, the message is passed to the vehicle by the MAG present on the opposite end of the tunnel. The following section looks at how the PMIPv6 protocol handles handovers of vehicles in VANET.

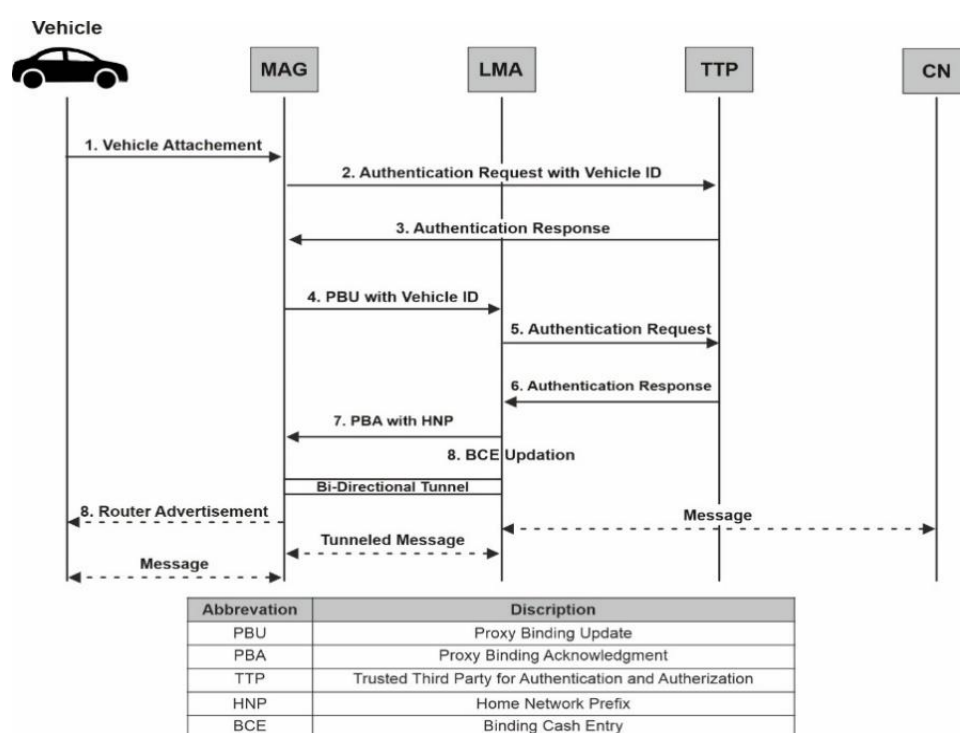


Figure 4. Communication Sequence Diagram in PMIPv6 for VANET.

3.2. Intra-Domain Handover Management in PMIPv6 for VANET

In Figure 5, the sequence diagram of message exchanged among various entities, when in intra-domain handover a vehicle changes its attachment point. In step 1, The preceding MAG initiates the disengagement process by sending a deregistration request to LMA via a PBU signal. The LMA then set a timer to complete the handover process in step 2. It then waits for the threshold period for a binding update request from the new MAG before removing the vehicle's entry from BCE. Upon receiving the request from new MAG, it then sends the PBA message to previous MAG requesting the vehicle binding status to be removed in step 3. In step 4, once new MAG seeks attachment via router solicitation message from vehicle, it sends the authentication request to TTP for the authentication of the vehicle (steps 5–6). The PBU message is then sent to LMA by the new MAG (steps 7–8) and vehicle's BCE is then updated by tying the same HNP to the new MAG. In step 9, LMA delivers the PBA message to the new MAG. Thus, constructing a new bidirectional tunnel between the LMA and the new MAG. After then, the new MAG then sends the vehicle a router advisement message consisting with the same HNP (step 11). Because the

HNP remains intact throughout transfer, the vehicle will be completely oblivious of the entire operation.

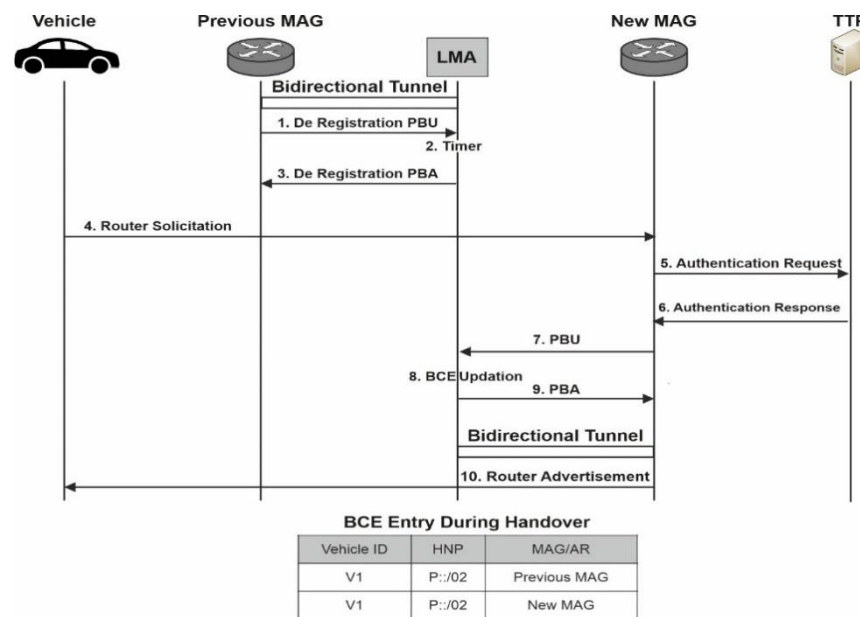


Figure 5. Handover of Vehicle in PMIPv6.

4. Mathematical Analysis

The communication model described above is used to calculate the total packet delivery cost with certain modifications for the analysis purposes. These changes took into account the authentication cost along with binding cost and packet delivery cost. The total packet delivery cost is represented as TC_{PMIPv6}^{VANET} . The formal notation, abbreviations, and symbols used in mathematical analysis are listed in Table 1 [23–25].

Table 1. Parameter description used for cost analysis of VANET in PMIPv6.

Parameters Used	Description
T_{a-b}/H_{a-b}	The cost of sending a packet from vehicle a to vehicle b/Hop Count between vehicle a and b in the network
T_p	Vehicle processing costs for binding updates or lookups at LMA/MAG
T_{setup}	Setup time taken by a vehicle and MAG to obtain PMIPv6 connection
$N_{Veh/MAG}$	Per MAG, the number of working vehicles
N_{MAG}	number of MAGs present in the domain
$S_{control}$	Control packet size (in bytes) transmitted
S_{Data}	data packet's size (in bytes) in transmission
α	Unit cost of binding update occurred with LMA
β	Unit cost for looking up a vehicle at LMA/MAG
τ	packet's unit transmission cost over a wired link (hop)
μ	packet's unit transmission cost on a wireless link (hop)
S_{TTP}	Control packet size for authentication (in bytes)

4.1. Cost Analysis for Intra-Domain Handover Management in PMIPv6 for VANET

Figure 6 shows the Intra-domain PMIPv6 architecture for VANET.

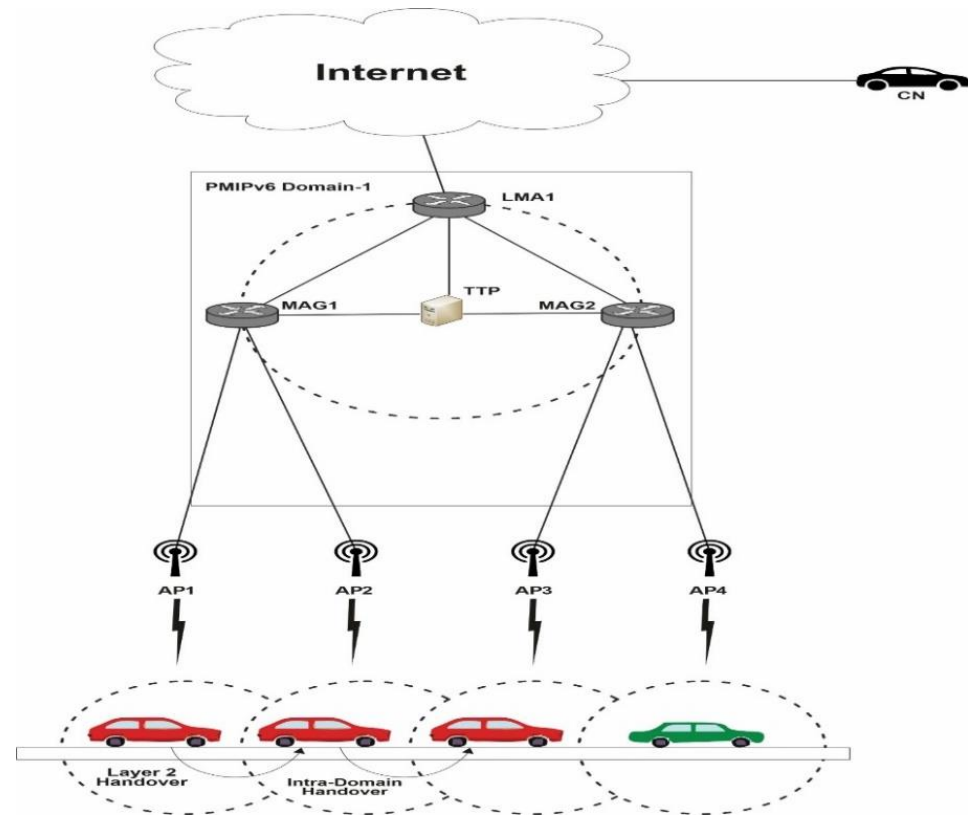


Figure 6. Intra-Domain Handover of Vehicle in PMIPv6 for Cost Analysis.

The total packet delivery cost (TC_{PMIPv6}^{VANET}) [23–25] in VANET depends namely in three verticals, Binding Update Cost (BUC_{PMIPv6}^{VANET}) [26], Authentication cost/delay ($T_{Authentication}^{VANET}$) [9,26] with Trusted Third Party (TTP) and Packet Delivery Cost (PDC_{PMIPv6}^{VANET}) [9,26]. Thus, the total packet delivery cost (TC_{PMIPv6}^{VANET}) is the summation of these three costs and can be expressed by Equation (1).

$$TC_{PMIPv6}^{VANET} = BUC_{PMIPv6}^{VANET} + T_{Authentication}^{VANET} + PDC_{PMIPv6}^{VANET} \quad (1)$$

These components cost of total cost are described as follows:

4.1.1. Binding Update Cost

Similar to PMIPv6, the binding update cost (BUC_{PMIPv6}^{VANET}) in VANET is expressed by Equation (2) and it depends on the summation of connection setup cost between vehicle and MAG, i.e., T_{Setup} , cost of establishing a dedicated bi-directional tunnel between MAG and LMA for exchanging the data packets between these network entities, i.e., $T_{Tunnel-Establishment}$ and at the last registration cost, i.e., T_P , of new MAG and associated vehicle. It includes BCE lookup or registration of new MAG for the specified vehicle, if its entry is not found in BCE. Once completed, The BCE holds an entry for each connected vehicle. The BCE contains the Vehicle's ID, vehicle's home network prefix (HNP), and proxy care-of-address (p-CoA), i.e., IP address of connected MAG. The BUC_{PMIPv6}^{VANET} in VANET is expressed as follows:

$$BUC_{PMIPv6}^{VANET} = T_{Setup} + T_{Tunnel-Establishment} + T_P \quad (2)$$

Setup cost, T_{Setup} , plays an important role in association of vehicle in PMIPv6 domain. In our proposed model it is considered as fixed as in [9,26]. Another critical factor is the cost incurred in establishment of a bidirectional tunnel between MAG and LMA. It includes exchange of two control messages, i.e., one for PBU another one for PBA between LMA and MAG. Therefore, it doubles the cost of exchanging the control packet ($T_{MAG-LMA}$) between network entities. The size of control packet, $S_{Control}$, depends on length of IPv6 header, mobility header, mobility option(s). The IPv6 header usually consists of 40 bytes, mobility header is of 6 bytes and the mobility option varies according to the protocol used. For our analysis, we have considered 50 bytes $S_{Control}$. Therefore, the tunnel establishment cost, $T_{Tunnel-Establishment}$ will be expressed in Equation (3)

$$T_{Tunnel-Establishment} = S_{Control} \times 2T_{MAG-LMA} \quad (3)$$

When a vehicle attaches to PMIPv6 domain, it must be registered with LMA. The processing cost of same is represented by T_p . It includes lookup cost of BCE table if an entry already exists in BCE table or generation of new BCE entry if the no record exists for the MAG/vehicle association. Here, α is unit binding update cost with LMA, N_{MAG} specifies the number of MAGs connected with LMA in PMIPv6 domain and $N_{Veh/MAG}$ specifies the number of active vehicles per MAG. Hence, the processing costs for binding updates or lookups at LMA/MAG, T_p , is expressed in Equation (4).

$$T_p = \alpha \times \log(N_{MAG} \times N_{Veh/MAG}) \quad (4)$$

Therefore, from Equations (2)–(4), the Binding Update Cost, BUC_{PMIPv6}^{VANET} , expressed in (2) can be represented as in (5)

$$BUC_{PMIPv6}^{VANET} = T_{Setup} + S_{Control} \times 2T_{MAG-LMA} + \alpha \times \log(N_{MAG} \times N_{Veh/MAG}) \quad (5)$$

4.1.2. Authentication Cost

For secure communication among vehicles connected to a network, the authentication of every vehicle and network entities plays an important role. For simplicity, we have considered intra-domain VANET handover, and the CN is residing in the same PMIPv6 domain. It also assumed that a Trusted Third Party (TTP) server is implemented at each PMIPv6 domain. TTP is responsible for authentication of each network entity such as vehicle, MAG and LMA. TTP verifies the MAG and LMA only once but verifies the vehicles each time when it becomes connected to *new* MAG. Hence, the authentication cost will be the summation of authentication cost of network entities ($T_{Network-Entities}^{VANET}$) and authentication cost of mobile entities such as vehicle ($T_{Mobile-Entities}^{VANET}$). The $T_{Authentication}^{VANET}$ in VANET is expressed as follows in Equation (6):

$$T_{Authentication}^{VANET} = T_{Network-Entities}^{VANET} + T_{Mobile-Entities}^{VANET} \quad (6)$$

For authentication process, the authentication control messages, S_{TTP} , will be exchanged between network entities MAGs/LMA and TTP server. Since there exists number of MAGs in PMIPv6 domain. Hence, for every MAG, an authentication control message will be sent to TTP server by MAG and in response to the same again the control message will be sent by TTP to MAG back after authentication. Hence, authentication cost of network entities $T_{Network-Entities}^{VANET}$ can be expressed in Equation (7)

$$T_{Network-Entities}^{VANET} = N_{MAG}(S_{TTP} \times 2T_{MAG-TTP}) + S_{TTP} \times 2T_{LMA-TTP} \quad (7)$$

For secure communication every vehicle must be authenticated. For the same, a connection between vehicle and MAG must be established involving the set-up cost, T_{Setup} . The MAG is responsible for sending the authentication request to TTP server on behalf of

the vehicle using authentication control message, S_{TTP} . Hence, for every vehicle (N_{Veh}) in PMIPv6 domain, an authentication control message will be sent to TTP server via MAG and in response to the same again the authentication control message will be sent by TTP to MAG back after authentication is completed. Hence, the authentication cost of mobile entities such as vehicle ($T_{Mobile-Entities}^{VANET}$) can be expressed in Equation (8).

$$T_{Mobile-Entities}^{VANET} = N_{Veh} (T_{Setup} + S_{TTP} \times 2T_{MAG-TTP}) \quad (8)$$

Therefore, from Equations (6)–(8), the authentication cost $T_{Authentication}^{VANET}$ expressed in (6) can be represented as in Equation (9).

$$T_{Authentication}^{VANET} = N_{MAG} (S_{TTP} \times 2T_{MAG-TTP}) + S_{TTP} \times 2T_{LMA-TTP} + N_{Veh} (T_{Setup} + S_{TTP} \times 2T_{MAG-TTP}) \quad (9)$$

4.1.3. Packet Delivery Cost

The exchange of packets can start after establishment of secure connection between CN and vehicle. In the first step a packet created by CN transfers to LMA. The LMA search for an entry in BCE corresponding to destined vehicle and associated MAG. Once it finds, LMA forwards the packet to the associated MAG through secure bidirectional tunnel and at the last MAG forwards the packet to specified vehicle. The cost associated in packet delivery can be expressed as in Equation (10)

$$PDC_{PMIPv6}^{VANET} = S_{Data} (\mu T_{CN-MAG} + \tau 2T_{LMA-MAG} + \mu T_{MAG-Veh}) + T_P \quad (10)$$

The size of data packet is considered as S_{Data} and transmitted over wired and wireless links. For simplicity, wireless links are assumed between CN to MAG and MAG to vehicle. In the same reference wired links are considered between MAG and LMA. Since wireless links are unreliable and significantly affects the packet delivery cost. Here, μ is considered as unit transmission cost of packet over the wireless link and τ is considered as unit transmission cost of packet over a wired link.

The processing cost, T_P , involves the look up cost in the BCE and expressed in (11) where unit cost of look up at LMA is represented by β .

$$T_P = \beta \times \log(N_{MAG} \times N_{Veh/MAG}) \quad (11)$$

Thus, from Equations (10) and (11), the cost of delivering a packet PDC_{PMIPv6}^{VANET} is expressed as follows in (12):

$$PDC_{PMIPv6}^{VANET} = S_{Data} (\mu T_{CN-MAG} + \tau 2T_{LMA-MAG} + \mu T_{MAG-Veh}) + \beta \times \log(N_{MAG} \times N_{Veh/MAG}) \quad (12)$$

Therefore, from Equations (5), (9) and (12), the total cost (TC_{PMIPv6}^{VANET}) of the packet delivery in of Intra-domain handoff with authentication in PMIPv6 for vehicular ad hoc networks (VANETs) of Equation (1) can be expressed as in Equation (13).

$$\begin{aligned} TC_{PMIPv6}^{VANET} = & T_{Setup} + S_{Control} \times 2T_{MAG-LMA} \\ & + \alpha \\ & \times \log(N_{MAG} \times N_{Veh/MAG}) + N_{MAG} (S_{Control} \times 2T_{MAG-TTP}) \\ & + S_{Control} \times 2T_{LMA-TTP} \\ & + N_{Veh} (T_{Setup} + S_{Control} \times 2T_{MAG-TTP}) \\ & + S_{Data} (\mu T_{CN-MAG} + \tau 2T_{LMA-MAG} + \mu T_{MAG-Veh}) \\ & + \beta \times \log(N_{MAG} \times N_{Veh/MAG}) \end{aligned} \quad (13)$$

5. Result Analysis

The performance description of the proposed scheme is explained in this section. The total cost in PMIPv6 domain for VANET depends on various components such as binding update cost, authentication cost and, packet delivery cost. By altering the various parameters such as number of MAGs, the unit transmission cost, the setup time cost, and binding update cost, we are able to evaluate the influence on total cost and can see how scalable our solution is. Furthermore, a comparative study with authentication and without authentication cost for the considered parameters is also presented in this section. The values of the parameters utilized in the cost analysis are listed in Table 2.

Table 2. Values of parameters used in cost analysis of VANET in PMIPv6.

Variable Name	Default	Minimum	Maximum
T_{setup} (ms)	200	100	500
N_{MAG}	20	10	200
$N_{Veh/MAG}$	200	100	1000
$T_{MAG-LMA}/H_{MAG-LMA}$	20	10	100
$T_{Veh-MAG}/H_{Veh-MAG}$	1	1	1
T_{CN-MAG}/H_{CN-MAG}	1	1	1
$T_{MAG-TTP}/T_{LMA-TTP}$	1	1	1
$S_{control}$ (bytes)	50	50	50
S_{data} (bytes)	1024	1024	1024
α	3	1	10
β	1	1	10
τ	1	1	10
μ	4	1	10
S_{TTP} (bytes)	100	100	100

The most appropriate parameter to assess the effectiveness of mobility management techniques is signaling cost. The quantity of control messages sent between network elements such as MAG/LMA and vehicles determines this. A PMIPv6 domain contains a LMA as mobility anchor point for the vehicle and various MAGs which servers as access router for vehicles. As vehicle enters PMIPv6 domain, it sends the registration request to MAG via authentication from TTP, and MAG forward the authenticated request to LMA. The total cost in PMIPv6 domain for VANET is the summation of the costs of binding update, authentication, and packet delivery represented by Equation (13). During the movement, a mobile vehicle performs intra domain handover while changing its attachment point from one MAG to another. Hence, number of MAGs in PMIPv6 domain plays an important role for analysis. Figure 7 shows the impact on total cost with authentication cost and without authentication cost by increasing the number of MAGs and number of vehicles in PMIPv6 domain. The diagram depicts that as the number of MAGs and vehicles grow the total cost also increases proportionately when authentication cost is considered. This is due to authentication process of MAGs as well as vehicles. However, when authentication cost is not included, the number of MAGs and number of vehicles do not have an impact on total cost. Wired links are more reliable as compared to wireless link. Here, the transmission cost on wired link is represented by, τ , and we have varied its value from 1 to 10 in terms of hop counts.

Figure 8 depicts the consequence of variations in unit transmission cost and vehicle count on total cost when authentication cost is included as well as when it is not included. When authentication cost is not considered for calculating the total cost, number of vehicles does not have impact on total cost. On the other hand, when authentication cost is involved both the unit transmission cost and number of vehicles have significant impact on total cost. The increase in unit transmission cost of a packet on a wired link (hop), τ , from 1 to 10 increases the total cost in the same proportion.

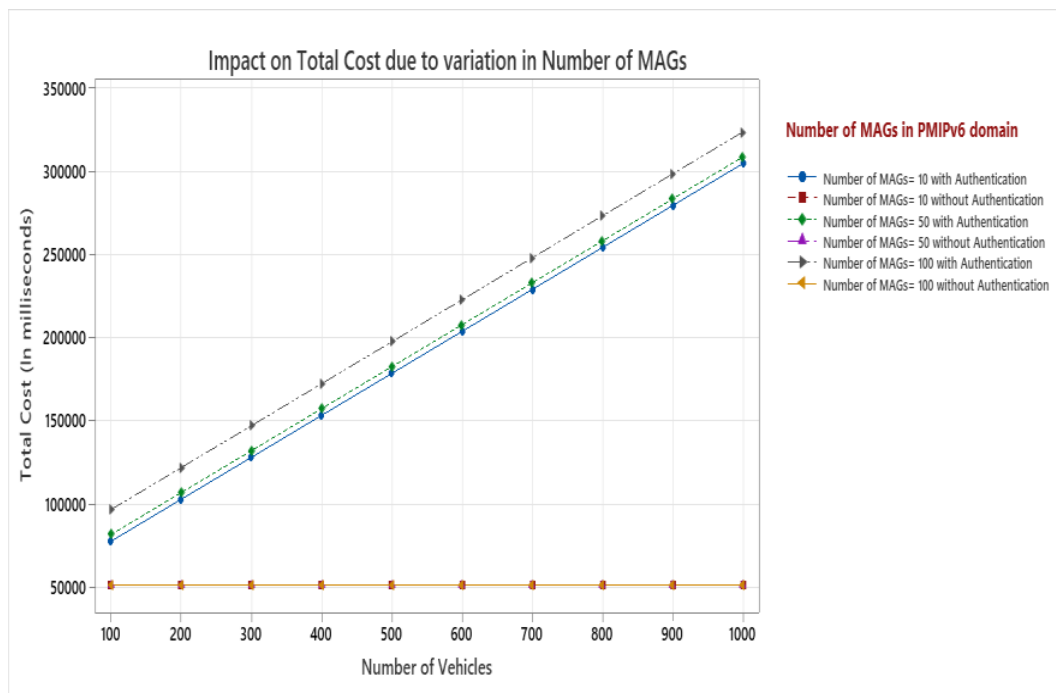


Figure 7. Impact on total cost with variation in number of MAGs.

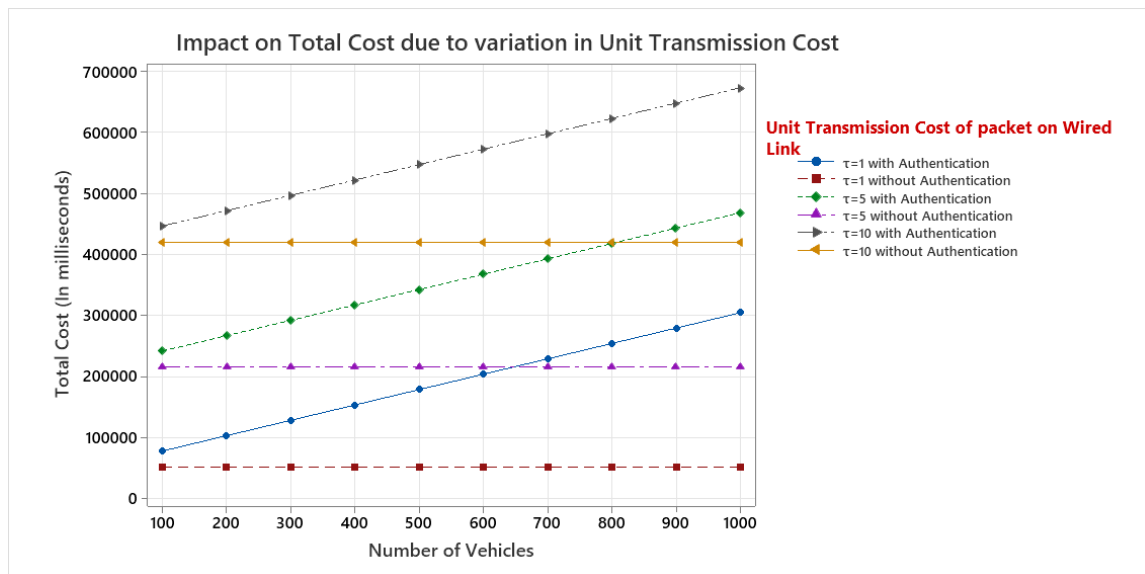


Figure 8. Impact on total cost due to variation in unit transmission cost.

To establish a communication link, a set cost is necessary. It includes wired and wireless links both. Wireless links are unreliable that is why requires more time to establish the communication channel, i.e., setup. Figure 9 depicts the impact of the setup cost on the total costs with authentication and without authentication cost. In our analysis, we have varied setup cost from 100 to 500. when authentication cost is considered, the total cost increases significantly when setup cost increase from 100 to 500 along with increase in number of vehicles from 100 to 1000. LMA is network entity having high end processing capabilities. While calculating the total cost, the setup cost and number of vehicles have no impact on total cost when authentication cost is not involved.

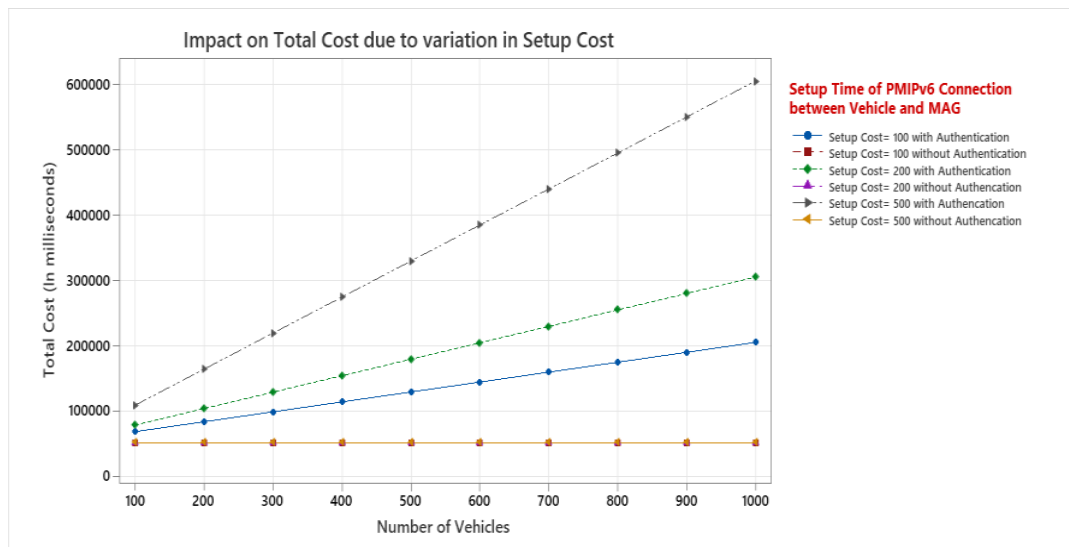


Figure 9. Impact on Total Cost due to variation in Setup Cost.

The impact of the unit cost of binding update with LMA, i.e., α , on total cost with and without considering the authentication cost is shown in Figure 10. It is evident from Figure 10 that the total cost has very negligible impact of unit cost of binding update, α , and approximately coinciding when the value of α varies 1 to 10 in both the authentication cost and without authentication cost, while considering all other parameters as default.

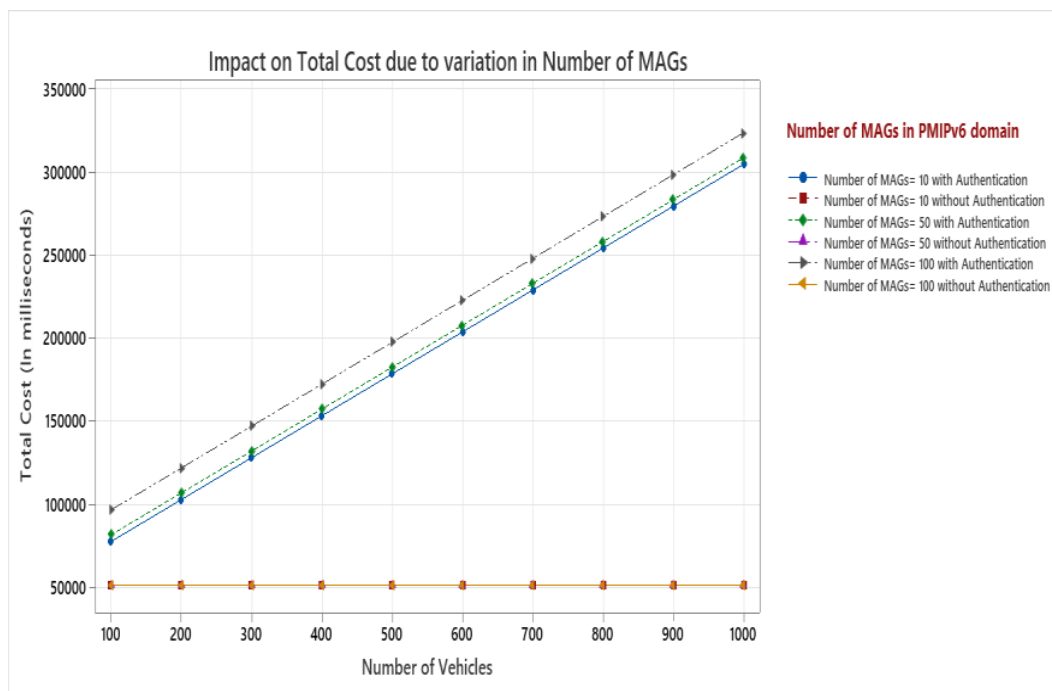


Figure 10. Impact on total cost due to variation in binding update cost.

6. Conclusions and Future Work

In VANET, vehicular communication allows a next-generation communication network to deliver seamless mobility and communication between vehicles. For ubiquitous services, IP-based mobility protocols can be characterized as host-based mobility management protocols and network-based mobility management protocols. As per the researchers, network-based mobility management are more effective and efficient protocol in comparison to host-based

management protocol. Hence, The PMIPv6 protocol is the more compatible and interoperable IP mobility management solution for VANET deployment which is used as a localized mobility management protocol. In this article, we have proposed, examined, and analyzed the total cost of VANET in PMIPv6 mobility management solutions. Various mobility management protocols proposed till yet have not included the authentication cost while calculating the total cost for VANET in PMIPv6 domain. Authentication plays an important role in secure communication. It is pointless to have fast communication if it is not secure. Hence, in the proposed work we have included the authentication process for secure communication and a comparative study with authentication and without authentication cost for the considered parameters such as number of MAGs, setup cost, binding update cost, unit transmission cost is carried out. The proposed model is more secure than the existing models, but it may include the more signaling overhead during the authentication process. In future, we can reduce this signaling cost overhead by adopting one of the authentication schemes such as group and/or ID based authentication.

Author Contributions: A.K.G. and A.K.T. contributed to the main idea of qualitative analysis for the research and wrote the original manuscript. G.A., M.S. and V.G. contributed significantly to improving the technical and grammatical contents of the manuscript. K.L.H., M.S. and G.S., reviewed the manuscript and provided valuable suggestions to further refine the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This This work was supported by Dongseo University, “Dongseo Cluster Project” Research Fund of 2022 (DSU-20220006).

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 Domains and Research Methodologies in VANET: A Survey. *Int. J. Comput. Netw. Inf. Secur. MECS Press* **2019**, *11*, 37–44. [\[CrossRef\]](#)
2. Goyal, A.K.; Agarwal, G.; Tripathi, A.K.; Sharma, G. Systematic Study of VANET Applications, Challenges, Threats, Attacks, Schemes and Issues in Research. In *Green Computing in Network Security*; CRC Press: Boca Raton, FL, USA, 2022; pp. 33–52.
3. Hoh, W.S.; Muthut, S.; Ong, B.-L.; Elshaikh, M.; Warip, M.N.M.; Badlishah, A.R. A Survey of Mobility Management Protocols. *ARPN J. 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 Proceedings of the National Conference on Information Technology and Computer, Haifa, Israel, 3–5 July 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. 2002. Available online: https://www.researchgate.net/publication/242503821_IP_mobility_support_for_IPv4 (accessed on 30 March 2022).
8. Johnson, B.; Arkko, J.; Perkins, C.E. Mobility Support in IPv6. 2011. Available online: https://www.researchgate.net/publication/2407161_Mobility_Support_in_IPv6 (accessed on 30 March 2022).
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.; Moravejsharieh, A.; Lloret, J.; Salleh, R.B. A survey on proxy mobile IPv6 handover. *IEEE Syst. J.* **2014**, *10*, 2018–2217. [\[CrossRef\]](#)
11. Mohammed, B.; Mahamod, I.; Rosdiadee, N.; Alrazak, R.A.; Zain, B. Fast handover solution for network-based distributed mobility management in intelligent transportation systems. *Telecommun. Syst.* **2016**, *64*, 325–346.
12. Moravejsharieh, A.; Modares, H. A proxy MIPv6 handover scheme for vehicular ad-hoc networks. *Wirel. Pers. Commun. Int. J.* **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. MECS Press* **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. Comput. Appl.* **2015**, *58*, 180–191. [\[CrossRef\]](#)

15. Jabir, A.J.; Subramaniam, S.K.; Ahmad, Z.Z.; Hamid, N.A.W.A. Cluster-based proxy mobile IPv6 for IP-WSNs. *EURASIP J. Wirel. Commun. Netw.* **2012**, *173*, 1–7. [[CrossRef](#)]
16. Son, S.; Jeong, J. Cost-effective handoff scheme based on mobility-aware dual pointer forwarding in proxy mobile IPv6 networks. *SpringerPlus* **2014**, *3*, 1–19. [[CrossRef](#)] [[PubMed](#)]
17. Din, S.; Paul, A.; Hong, W.H.; Seo, H. Constrained application for mobility management using embedded devices in the Internet of Things based urban planning in smart cities. *Sustain. Cities Soc.* **2019**, *44*, 144–151. [[CrossRef](#)]
18. Ghaleb, S.M.; Subramaniam, S.; Zukarnain, Z.A.; Muhammed, A.; Ghaleb, M. An efficient resource utilization scheme within PMIPv6 protocol for urban vehicular networks. *PLoS ONE* **2019**, *14*, e0212490. [[CrossRef](#)] [[PubMed](#)]
19. Ghaleb, S.M.; Subramaniam, S.; Ghaleb, M.; Ejmaa, M.E. An Efficient Group-Based Control Signalling within Proxy Mobile IPv6 Protocol. *Computers* **2019**, *8*, 75. [[CrossRef](#)]
20. 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](#)]
21. Sheikh, M.S.; Liang, J.; Wang, W. Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 1–25. [[CrossRef](#)]
22. Tripathi, A.K.; Tripathi, S.K. A Qualitative Analysis of Secured Handover Management Schemes for Mobile IPv6 enabled Networks. In Proceedings of the International Conference on Innovative Applications of Computational Intelligence on Power, Energy and Controls with Their Impact on Humanity (CIPECH), Ghaziabad, India, 1–2 November 2018; pp. 1–8.
23. 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](#)]
24. 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*, 100277. [[CrossRef](#)]
25. Hossain, M.S.; Atiquzzaman, M. Analysis of proxy mobile IPv6: A network-based mobility solution. In Proceedings of the International Conference on Computer and Information Technology (ICCIT), Vienna, Austria, 12–14 May 2012; pp. 338–344.
26. Tripathi, A.K.; Radhakrishnan, R.L.; Lather, J.S. Impact of wireless link delay on handover latency in Mobile IPv6 environment. In Proceedings of the International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT-14), Ghaziabad, India, 7–8 February 2014; pp. 424–428.