A Multihop-Authenticated Proxy Mobile IP Scheme for Asymmetric VANETs

Sandra Céspedes, *Member, IEEE*, Sanaa Taha, *Student Member, IEEE*, and Xuemin (Sherman) Shen, *Fellow, IEEE*

***Abstract*—Vehicular communications networks are envisioned for the access to drive-thru Internet and IP-based infotainment applications. These services are supported by roadside access routers (ARs) that connect vehicular ad hoc networks (VANETs) to external IP networks. However, VANETs suffer from asymmetric links due to variable transmission ranges caused by mobility, obstacles, and dissimilar transmission power, which make it difficult to maintain the bidirectional connections and to provide the IP mobility required by most IP applications. Moreover, vehicular mobility results in short-lived connections to the AR, affecting the availability of IP services in VANETs. In this paper, we study the secure and timely handover of IP services in an asymmetric VANET and propose a multihop-authenticated Proxy Mobile IP (MA-PMIP) scheme. MA-PMIP provides an enhanced IP mobility scheme over infrastructure-to-vehicle-to-vehicle (I2V2V) communications that uses location and road traffic information. The MA-PMIP also reacts, depending on the bidirectionality of links, to improve availability of IP services. Moreover, our scheme ensures that the handover signaling is authenticated when V2V paths are employed to reach the infrastructure so that possible attacks are mitigated without affecting the performance of the ongoing sessions. Both analysis and extensive simulations in OMNeT++ are conducted, and the results demonstrate that the MA-PMIP improves service availability and provides secure seamless access to IP applications in asymmetric VANETs.**

***Index Terms*—Asymmetric links, infrastructure-to-vehicle-to-vehicle (I2V2V), IP mobility, multihop networks, mutual authentication, Proxy Mobile IP (PMIP), vehicular ad hoc network (VANET).**

I. Introduction

VEHICULAR communications networks are envisioned to support a wide variety of infrastructure-based infotainment applications. Considering the race between the always-increasing access demand and the deployment of the supporting infrastructure, application availability has been accordingly extended through multihop communications in vehicular ad hoc networks (VANETs), i.e., through infrastructure-to-vehicle-to-vehicle (I2V2V) communications. Thus, this kind of "cooperation" in VANETs has been proposed at the MAC and network layers [1]–[4], among others.

I2V2V communications come as a convenient solution for the ubiquitous access to IP services in VANETs. On one hand, when a direct connection between vehicles and the infrastructure is not available, the bidirectional links required by IP applications could be established by means of multihop communications. This way, infrastructure networks that are in process to be deployed, e.g., the recently standardized 802.11p/WAVE network, or networks that provide limited coverage, such as 802.11b/g/n hotspots, may benefit from extended coverage due to data forwarding mechanisms through V2V communications [5]. On the other hand, when the coverage is not an issue due to the presence of a well-deployed infrastructure, such as 3G and LTE networks, the multihop communications may decrease the levels of the energy consumption when signals have to cover shorter distances, to improve the spectral efficiency, and to increase network capacity and throughput [6], [7].

Although I2V2V communications are promising, they have been mainly proposed for dissemination of safety and delay-sensitive information but little for infotainment applications. In the case of safety applications, the scope is usually of broadcast nature or delimited to a certain geographic area, resulting in a well-defined strategy to be followed if multihop paths become necessary during data dissemination. However, when I2V2V communications are proposed for infotainment applications, such as IP-based services and drive-thru Internet access, more challenges arise in the provision of seamless communications through multihop VANETs.

First, due to the dynamics of a vehicular network, vehicles may transfer their active connections through different IP access networks. Thus, the on-going IP sessions are affected by the change of IP addresses, which consequently results in broken connections. Second, additional complexity may be added due to links variability during V2V communications and the presence of asymmetric links caused by variable transmission ranges between infrastructure and VANET devices. Moreover, if two vehicles decide to cooperate in the relaying of packets, they are arbitrary mobile hotspots that have not met each other before. As a result, it becomes difficult to generate a security association between them leading to security threats for both infrastructure and vehicles involved in the relayed communications [8].

Manuscript received September 4, 2012; revised January 16, 2013; accepted February 19, 2013. Date of publication March 15, 2013; date of current version September 11, 2013. This work was supported in part by the Ontario Research Fund Research Excellence and in part by Icesi University. The review of this paper was coordinated by Dr. T. Taleb.

S. Céspedes is with the Department of Information and Communications Technology, Icesi University, Cali, Colombia, and also with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: slcesped@bbcr.uwaterloo.ca).

S. Taha is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada, and also with the Faculty of Computers and Information, Cairo University, Cairo, Egypt (e-mail: staha@uwaterloo.ca).

X. Shen is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: xshen@bbcr.uwaterloo.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2013.2252931

0018-9545 © 2013 IEEE

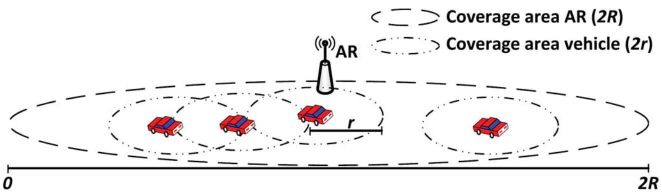


Fig. 1. Asymmetric links in a VANET.

In this paper, we address the aforementioned challenges and propose a multihop-authenticated Proxy Mobile IP (MA-PMIP) scheme. The main contributions of this paper are summarized as follows.

1) We propose an IP mobility scheme for multihop VANETs, which also integrates location and road traffic information to enable timely handovers.
2) We consider the asymmetric links in VANETs, to adapt the geonetworking routing mechanism depending on the availability of bidirectional links.
3) We design an efficient and mutual authentication scheme that thwarts authentication attacks when handovers occur through I2V2V communications, which achieves a reduced overhead.

To the best of our knowledge, MA-PMIP is the first attempt to consider a predictive IP mobility scheme designed for multihop asymmetric VANETs, with the security issues of employing I2V2V communications.

The remainder of this paper is organized as follows. In Section II, we recall the concepts of asymmetric VANETs, symmetric polynomials, and PMIP as the preliminaries. In Section III, we discuss the related work and motivations for proposing MA-PMIP. Next, our reference system model is described in Section IV. The proposed MA-PMIP scheme is introduced in Section V, followed by an analytical evaluation in Section VI. Security analysis and experimental evaluations are presented in Sections VII and VIII, respectively. Finally, concluding remarks are provided in Section IX.

II. Preliminaries

In this section, we define an asymmetric VANET, describe the PMIP protocol [9], and outline the symmetric-polynomial key generation technique [10], which will serve as the basis of the proposed MA-PMIP scheme. Throughout this paper, the terms vehicle, node, and mobile router (MR) are interchangeably used to refer to the vehicle's onboard router communicating with other vehicles and with the infrastructure.

A. Asymmetric VANET

An asymmetric VANET, shown in Fig. 1, suffers from asymmetric transmission ranges due to mobility, path losses in the presence of obstacles, and dissimilar transmission power among VANET devices. Although one-way links may not affect some applications that require only the link from access router (AR) to vehicle (e.g., some safety-related information), this problem severely affects IP-based applications. In particular, TCP requires the packets to be acknowledged, but one-way links make it impossible to confirm reception of packets. In fact, a vehicle will not be able to initiate any client–server application unless it establishes a bidirectional link with the AR. Note that the client–server architecture is the most common architecture deployed for Internet applications.

Therefore, symmetric links have been a frequent assumption for investigating the deployment of IP services, although empirical studies have found up to 15% asymmetric links in ad hoc networks [11]. Nevertheless, when the asymmetric links are discounted by routing protocols in ad hoc networks, it can result in low data transmission rates and low network connectivity. Thus, the presence of asymmetric links has been studied from the point of view of data dissemination in VANETs [12] and its implications in geographic routing [13], but the impact on the provision of IP services in VANETs has yet to be studied. Since previous works have shown that the inclusion of asymmetric links in the routing decisions may result in better network performance [11], we consider the asymmetric VANET as the foundation for our network model introduced in Section IV.

B. PMIP

PMIP is a localized network-based IP mobility protocol (RFC 5213 [9]). It is a localized protocol because it serves within a PMIP domain (e.g., a single administrative domain). In addition, it is a network-based one because the network acts on behalf of the mobile node to provide IP mobility. PMIP defines two entities: the Mobile Access Gateway (MAG) and the local mobility anchor (LMA). The MAG acts as a proxy for all the mobility signaling on behalf of the mobile node. It detects new connections, notifies the LMA about them, and behaves as the AR that advertises the network prefix to the mobile node. The LMA is the anchor point inside a PMIP domain. It stores the binding between the mobile node's unique identifier and its network prefix, and maintains a tunnel to forward the packets toward the MAG that is serving the mobile node.

C. Symmetric Polynomials (for Security)

A symmetric polynomial is defined as any polynomial of two or more variables that achieves the interchangeability property, i.e., $f(x, y) = f(y, x)$ [10]. Such a mathematical function is often used by key establishment schemes to generate a shared secret key between two entities. A polynomial distributor, such as the AR, securely generates a symmetric polynomial and evaluates this polynomial with each of its users' identities. For example, given two users' identities 1 and 2, and symmetric polynomial $f(x, y) = x^2y^2 + xy + 10$, the resultant evaluation functions are $f(1, y) = y^2 + y + 10$ and $f(2, y) = 4y^2 + 2y + 10$, respectively. The polynomial distributor keeps the original polynomial secured, and sends the evaluated polynomials to each user in a secure way. Afterward, the two users can share a secret key between them by calculating the evaluation function for each other. Continuing with the previous example, if user 1 evaluates its function $f(1, y)$ for user 2, it obtains $f(1, 2) = 16$. In the same way, if user 2 evaluates function $f(2, y)$ for user 1, it obtains $f(2, 1) = 16$. Therefore, both users share a secret key, i.e., 16, without transmitting any additional messages to each other.

III. Related Work and Motivations

IP addressing and mobility solutions for vehicular environments have been studied from different perspectives. In the case of multihop VANETs, several approaches have been proposed to enable network mobility (i.e., for providing IP mobility to all the in-vehicle local network users), based on the Network Mobility Basic Support (NEMO BS) protocol (RFC 3963 [9]) or based on the PMIP. The NEMO-based solutions in [4] and [14] employ a geographic routing protocol to obtain IP addresses directly from the infrastructure. Geographic routing has been shown to be effective, to the point that it has been standardized for communications in intelligent transport systems [15]. Nevertheless, although NEMO minimizes the binding update signaling, it also brings a costly tunneling overhead. Thus, there have been proposals to balance the tradeoff between these two factors in one-hop scenarios [16]. However, this is yet to be explored when NEMO BS is extended through multihop communications.

On the other hand, since the standard PMIP only supports mobility for a single node, the solutions in [17]–[19] adapt the protocol to reduce the signaling when a local network is to be served by the in-vehicle Mobile Router (MR). Lee *et al.* [17] propose P-NEMO to maintain the Internet connectivity at the vehicle, and provide a make-before-break mechanism when vehicles switch to a new access network. In [18] and [19], forward solicitations from local users are proposed, so that nodes in the local network may configure addresses directly from the PMIP domain; the first solution proposes to use a proxy router to forward such solicitations, whereas the second extends some functionalities for the MR to serve as a mobile MAG, so that it exchanges mobility signaling with the LMA. However, these works do not address the mobility problem when other vehicles are connected through multihop paths, which is the main concern addressed in this paper.

Although PMIP has a good acceptance for its applicability in vehicular scenarios, it has an important restriction for its deployment in I2V2V communications. The protocol, by definition, requires the mobile node to have a direct connection to the MAG for two reasons. First, the MAG is expected to detect new connections and disconnections based on one-hop communications. Second, the network-based mobility service should be provided only after authenticating and authorizing the mobile node for that service; however, those tasks are assumed to happen over the link between the MAG and the mobile node but not in the presence of intermediate routers (RFC 5213 [9]). Therefore, it is still necessary to devise a solution in which the multihop links in the VANET are considered.

Moreover, none of the aforementioned studies explores the problem of security. In the case of NEMO-based solutions, they let the routing protocol be responsible for securing the communications, whereas the PMIP-based solutions rely on the assumption that the intermediate node—in this case, the proxy MR—is by some means a secure entity in the PMIP domain.

Continuing with the problem of security, authentication and privacy-preserving schemes for VANETs have been proposed in [20] and [21]. In particular, previous works that propose authentication schemes for multihop wireless networks [22] have been mainly focused on two different approaches: 1) end-to-end authentication, which employs a relay node to only forward the authentication credentials between the mobile node and the infrastructure; and 2) hop-by-hop authentication, which implements authentication algorithms between every two hops. Following the first approach, the mobile node uses its public key certificate to authenticate itself to the foreign gateway in [23]. On the other hand, the scheme in [24] uses both symmetric key, for authenticating a mobile node to its home network, and public key for mutual authentication between a home network and a foreign network. However, the expensive computation involved with public key operations tends to increase the end-to-end delay.

Conversely, a symmetric key-based authentication scheme for multihop Mobile IP is proposed in [25]. In the work, a mobile node authenticates itself to its home authentication server, which derives a group of keys to be used by mobile nodes. Despite the low computation and communication overheads, the symmetric key-based schemes cannot achieve strong levels of authentication such as those achieved by public-key-based schemes. This is because the sharing of the secret key between the two peers increases the chances for adversaries to identify the shared key. Instead, public-key-based schemes create a unique secret key for each user; hence, it is more difficult for adversaries to identify the keys.

Following the second approach, mutual authentication that depends on both secret splitting and self-certified schemes is proposed in [26]. However, both schemes are prone to denial-of-service (DoS) attacks. Another scheme for hop-by-hop authentication, which is called ALPHA, is presented in [27]. In ALPHA, the mobile node signs the messages using a hash chain element as the key for signing, and then delays the key disclosure until receiving an acknowledgement from the intermediate node. Although ALPHA protects the network from insider attacks, it suffers from a high end-to-end delay. A hybrid approach, the adaptive message authentication (AMA) scheme, is proposed in [28]. AMA adapts the strength of the security checks depending on the security conditions of the network at the moment of packet forwarding.

Different from the aforementioned authentication schemes, in this paper, we propose a lightweight mutual authentication scheme to be employed between the MR and the relay, which mitigates the high delay that is introduced by previous hop-by-hop schemes. Therefore, the proposed scheme can be used with seamless handover operations in our multihop VANET during the I2V2V communications.

IV. Reference System

A. Network Model

We consider a vehicular communication network such as the one shown in Fig. 2. Connections to the infrastructure are enabled by means of roadside ARs, where each one is in charge of a different wireless access network. Vehicles are equipped with wireless interfaces and GPS tracking systems that feed a location service from which the location of vehicles can be retrieved. Beacon messages are employed by vehicles to give

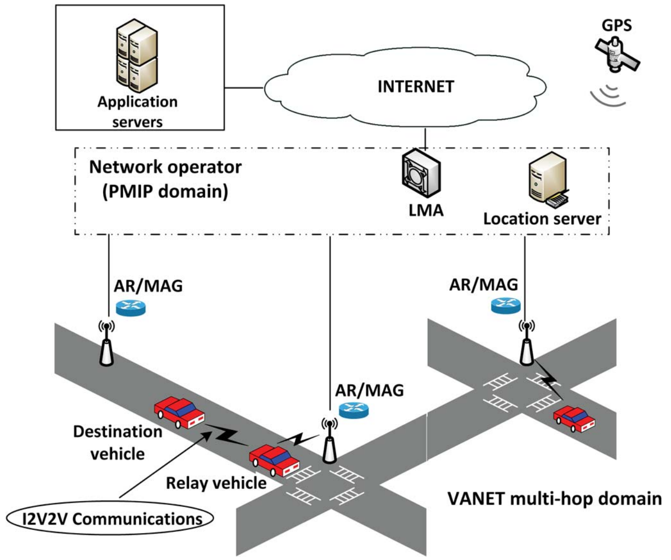


Fig. 2. Network topology.

information about their location, direction, speed, acceleration, and traffic events to their neighbors.

We consider the presence of asymmetric links in the VANET (see Fig. 1). The delivery of packets is assisted by a geographic routing protocol. To serve this protocol, a location server stores the location of vehicles and is available for providing updated responses to queries made by nodes participating in the routing of packets. To forward packets within the multihop VANET, a virtual link between the AR and the vehicle is created [15]. This means that a georouting header is appended to each packet, where the location and the geoidentifier of the recipient are indicated. This way, the georouting layer is in charge of the hop-by-hop forwarding through multihop paths, with no need of processing the IP headers at the intermediate vehicles.

The ARs service areas are well defined by the network operator. A well-defined area means that messages from ARs to the VANET are only forwarded within a certain geographic region [29]. Each AR announces its services in geocast beacon messages with the flag `AccessRouter`. The beacons are forwarded through multihop paths as long as the hops are located inside the coordinates indicated by the geocast packet header. This way, vehicles in the service area can extract information from the geocast header, such as AR's location, AR's geoidentifier, and the service-area limiting coordinates. We assume that the infrastructure is a planned network with non-overlapping and consecutive service areas. Note that, although service areas are consecutive, some locations within them are not reachable through one-hop connections. This may be caused by weak channel conditions and by the asymmetric links between ARs and vehicles.

To ensure the proper operation of the georouting protocol and the MA-PMIP, it is required to maintain state information at the entities exchanging IP packets. The following are the required data structures.

Neighbors table: This table stores information about the neighboring nodes. The table indicates a link type—unidirectional or bidirectional—for each neighbor. A node detects the bidirectional links in the following way: Incoming links are verified when beacon messages are received from neighbors (i.e., this node can hear its neighbors); outward links are verified by checking the neighbors' locations and the node's transmission power to calculate whether such neighbors are inside the radio range (i.e., the neighbors can hear this node). The table is stored by vehicles and ARs.

Default gateway table: This table stores information about the AR in the current service area. It contains the AR's geoidentifier and the service-area coordinates. If the destination of a packet is an external node, the geographic routing forwards the packet toward the default gateway indicated in this table. Then, the AR routes the packet to its final destination. The table is stored by vehicles.

We only consider IP-based applications accessed from the VANET. Such applications are hosted in external networks that may be private (for dedicated content), or public, such as the Internet. Since we have selected PMIP for handling the IP mobility in the network, all the ARs are assumed to belong to a single PMIP domain. The AR and MAG are colocated in our model. Therefore, the terms AR and MAG are used interchangeably in the following sections.

Different from [29], in our scheme, the AR does not send router advertisement messages announcing the IP prefix to vehicles in the service area. Instead, when a vehicle joins the network for the first time, individual IP prefixes are allocated through PMIP. It is required by MA-PMIP to obtain this initial IP configuration, only when a one-hop connection exists between the vehicle and the MAG, so that authentication material is securely exchanged for future handovers of the vehicle over multihop paths.

B. Threat and Trust Models

We consider both internal and external adversaries to be present during I2V2V communications. Internal adversaries are legitimate users who exploit their legitimacy to harm other users. Thus, having the same capabilities as the legitimate users, internal adversaries have authorized credentials that can be used in the PMIP domain. Two types of internal adversaries are defined: impersonation and colluder. The former impersonates another MR's identity and sends neighbor discovery messages, such as router solicitation (RS), through the relay router (RR). The latter colludes with other domain users using their authorized credentials to identify the shared secret key between two legitimate users.

External adversaries are unauthorized users who aim at identifying the secret key and breaking the authentication scheme. Those adversaries have monitoring devices with capabilities to eavesdrop messages transmitted between an MR and a RR. Moreover, they can inject their own messages and also delete other authorized users' transmitted messages. We consider that replay, man-in-the-middle (MITM), and DoS attacks are launched by external adversaries. The goal of replay and MITM attacks is to identify a shared key between two legitimate users, whereas the goal of the DoS attack is to exhaust the system

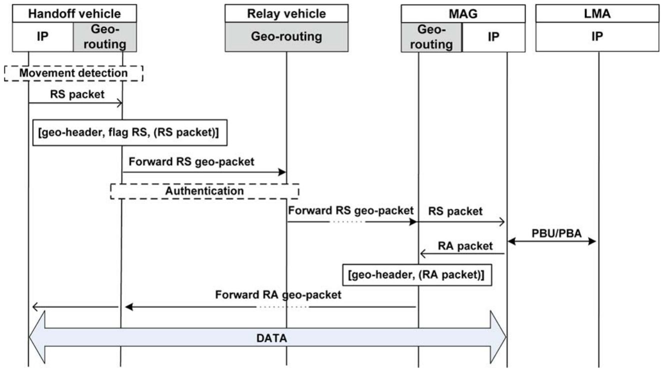


Fig. 3. Handover through I2V2V communications with MA-PMIP (Basic).

resources following a kind of irrational attack. A DoS attacker can also be considered an internal adversary, when the attacker is one of the legitimate nodes.

In our model, we assume the LMA and all MAGs in the domain to be trusted entities. An MR trusts its first attached MAG in such a way that this MAG does not reveal the MR's evaluated domain polynomial, which is used by the MR to create shared keys with RRs. In addition, the MR trusts the LMA that maintains the secret domain polynomial, which can be used to reveal the shared keys for all nodes in the network. The concept of domain polynomial will be explained in detail in Section V-D.

V. Multihop-Authenticated Proxy Mobile IP Scheme

In this section, we introduce the basic and predictive operation of MA-PMIP, the handling of asymmetric links, and the multihop authentication mechanism that allows for secure signaling during handovers.

A. Basic Operation

The signaling of MA-PMIP for initial IP configuration follows the signaling defined by the standard PMIP. Once the vehicle joins the domain for the first time, it sends RS messages employing the multicast ALL_ROUTERS address as destination. Nevertheless, the RS messages are delivered in a unicast form when the geolocation of the AR has been received through geocast beacons. Upon reception, the MAG employs the RS messages as a hint for detecting the new connection. After the PMIP signaling has been completed, the MAG announces the IP prefix in a unicast Router Advertisement (RA) message delivered to the vehicle over the one-hop connection. To enable communications from the in-vehicle local network, the MR may obtain additional prefixes by means of prefix delegation (draft-ietf-netext-pd-pmip-02 [9]) or prefix division (draft-petrescu-netext-pmip-nemo-00 [9]) as it is currently proposed at the Internet Engineering Task Force for network mobility support with PMIP.

Fig. 3 shows the handover signaling when MA-PMIP in basic mode is operating. The movement detection can be triggered by any of the following events: 1) The vehicle has started receiving AR geocast messages with a geoidentifier that is different from the one registered in the *default gateway table*, or 2) the vehicle has detected that its current location falls outside the service area of the registered AR. If the vehicle loses one-hop connection toward the MAG but is still inside the registered service area, then no IP mobility signaling is required, and packets are forwarded by means of the georouting protocol.

After movement detection, the RS message is an indicator for others (i.e., relay vehicle and MAG) of the vehicle's intention to reestablish a connection in the PMIP domain. Thus, an authentication is required to ensure that both the MR and the relay are legitimate and are not performing any of the attacks described in Section IV-B. Once the nodes are authenticated, the RS packet is forwarded until it reaches the MAG, and the PMIP signaling is completed afterward.

B. Predictive Handovers

To take advantage of the location information in the VANET, we propose a prediction mechanism that enables a timely handover procedure. It consists of an estimation of the time at which the vehicle will move to a new service area and is coupled with the recently standardized Fast handovers for PMIP (FPMIP) (RFC 5949 [9]). The FPMIP in predictive mode defines the signaling between the previous MAG (PMAG) and the new MAG (NMAG) to pre-establish a tunnel and forward the data packets to the new access network. This aims at minimizing packet losses when the mobile node loses connectivity in both previous and new access networks. Once the node is detected in the new access network, the NMAG forwards the buffered packets to the node and signals the LMA so that the MAG-to-MAG tunnel can be deactivated.

We do not introduce any changes to the standard FPMIP. Instead, the extensions necessary at the PMAG for estimating the time at which the handover will occur are introduced. This way, the MAG-to-MAG tunnel can be timely established. Furthermore, the proposed predictive mechanism works for both one-hop and multihop connected vehicles in the VANET. The prediction is enabled only for those vehicles that have active communications since the mechanism is triggered only when the PMAG has packets to forward to the roaming vehicle. For inactive vehicles that hand over across the PMIP domain, they may follow the basic MA-PMIP signaling described in Section V-A.

The prediction process is shown in Fig. 4. The PMAG queries the location of a vehicle for which a packet has to be delivered. This information is retrieved from the location server, together with the destination vehicle's velocity and traffic density (i.e., vehicles per meter). The traffic density is calculated by the location server based on the information received about the vehicles in that particular service area. To estimate the time at which the handover will occur, we construct a weighted average that considers two aspects: the current driving characteristics at the destination vehicle (i.e., current or last reported velocity v_r) and the average flow velocity v_{avg} determined from traffic conditions. According to the Greenshield's model, the average flow velocity v_{avg} can be related to traffic conditions as follows [30]:

$$v_{\text{avg}} = \left(1 - \frac{k}{k_{\text{jam}}}\right) v_f \qquad (1)$$

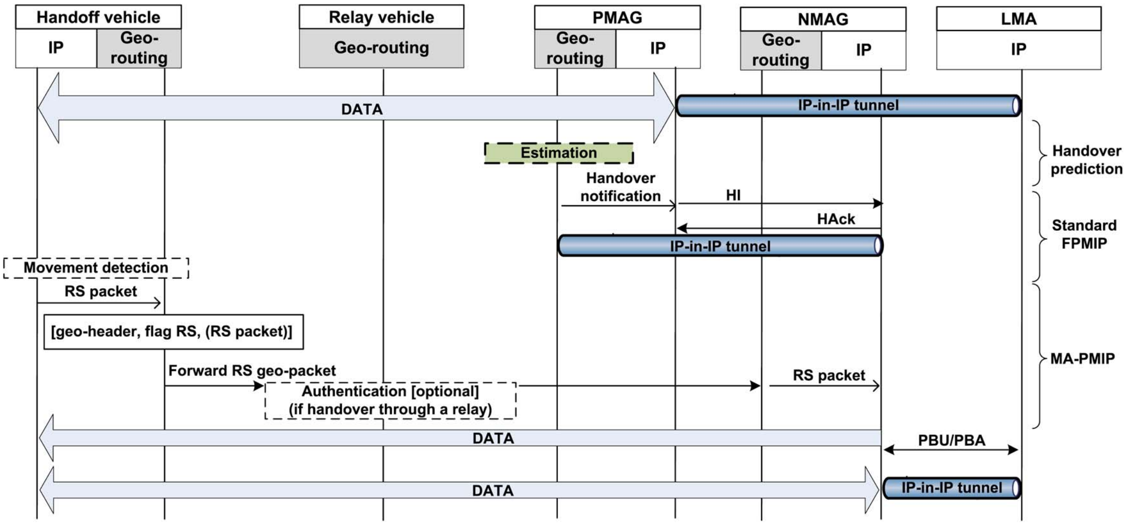


Fig. 4. Prediction mechanism for fast handovers in MA-PMIP.

where k is the traffic density, k_{jam} is the density associated with a completely stopped traffic flow, and v_f corresponds to the free-flow speed, i.e., the road speed limit. Therefore, we calculate the estimated vehicle's velocity as

$$v_{\mathrm{est}} = (1 - \kappa) \times v_r + \kappa \times v_{\mathrm{avg}}. \tag{2}$$

The PMAG may retrieve the current velocity v_r from the local *neighbors table*, or it may use the last reported velocity that is retrieved from the location server. The value for κ could be adjusted at the service-area level, according to different priorities. For example, a value of $\kappa = 0.875$ could be employed for a service area in which drive-thru traffic is dominant (i.e., not an area where vehicles typically park) so that velocity is mostly determined by the road density. It is important to note that, since v_r is close to a "real-time" report of the current velocity, it encloses not only the velocity due to past traffic conditions but the isolated driver's behavior as well.

Once v_{est} is estimated, the time to reach the edge of the service-area level is easily calculated as $t_{\mathrm{est}} = d_{\mathrm{est}}/v_{\mathrm{est}}$, where d_{est} corresponds to the Euclidean distance from the current location of the vehicle to the edge of the service area. We then form a heuristic to make the following decision: If the time to reach the edge is less than the one determined by a threshold value, the PMAG initiates the signaling for the FPMIP shown in Fig. 4. After the vehicle moves to the new service area, it sends the RS message as a result of the movement detection, and the tunnel between the LMA and the NMAG is set for the normal routing of traffic to the vehicle's new location.

C. Handling of Asymmetric Links

The asymmetric links in MA-PMIP are detected and handled in two different layers: 1) at the network layer, by means of the Neighbor Discovery Protocol and the Neighbor Unreachability Detection mechanism (RFC 4861 [9]); and 2) at the geonetworking layer, which follows the procedure described in Section IV-A for the link-type identification. The only requirement from the MAC layer is to expose the asymmetric links to the upper layers.

MA-PMIP employs the two mechanisms to react to the directionality of links during the delivery of IP packets. For instance, consider an IP application that requires a bidirectional link for its proper operation. We then assume that IP packets are marked by the application server to indicate the required application's directionality. Such a marking could be set in the flow label field of the IPv6 header. In the case that the server does not employ/support flow labeling, the LMA may still set the mark by checking the transport protocol in the IP packet header. In either case, the LMA codes the directionality in the flow label field of the outer header of packets sent in the tunnel LMA → MAG. This way, the MAG has the necessary information for routing the packets accordingly in the VANET.

Before packets are forwarded, the MAG checks the directionality requirement for each packet and proceeds as follows:

Bidirectional flow

- If neighbor discovery detects that the destination vehicle is disconnected from the MAG, the packet is discarded, unless the prediction mechanism has been activated.
- Else, if the vehicle is still connected, the packet is delivered to the geonetworking layer to continue with routing.

Unidirectional flow

- If the prediction mechanism has been activated, then forward the packet accordingly.
- Else, the packet is delivered to the geonetworking layer to continue with routing.

Once the geonetworking layer receives a packet, it employs the information in the *neighbors table* to select relays that are close to the destination. If the flow of packets requires bidirectionality, the selected relays are additionally filtered, depending whether or not they are set as bidirectional in the *neighbor table*. This combined routing metric distance/type of link is employed in both directions: from the MAG to the destination vehicle and from the destination vehicle to the MAG.

D. Authentication

As shown in Figs. 3 and 4, an efficient authentication scheme should be employed to mutually authenticate a roaming vehicle (i.e., an MR) and an RR. The keys generated at the MR and the RR for authentication are based on the concept of symmetric polynomials.

Decentralized key generation schemes that use symmetric polynomials are proposed in [31] and [32]. Such schemes generate a shared secret key between two arbitrary mobile nodes located in two heterogeneous networks, and they achieve a t-secrecy level, where t represents the degree of the generated polynomial. A scheme with a t-secrecy can be broken if $t+1$ users collude to reveal the secret polynomial. Moreover, for only one mobile node revocation, the decentralized schemes require to change the entire system's keys, which leads to a high communication overhead. Therefore, our design premises for the proposed authentication scheme are to reduce the revocation overhead and to increase the secrecy level achieved by the previous schemes.

Our authentication scheme consists of three main phases: the key establishment phase, for establishing and distributing keys; the registration phase, for receiving the secure material from the PMIP domain; and the authentication phase, for mutually authenticating an MR and an RR [33].

1) Key Establishment Phase: Considering a unique identity for each MAG, the LMA maintains a list of those identities and distributes them to all legitimate users in the PMIP domain. The MAGs list's size depends on the number of MAGs in the domain. For n MAGs, each legitimate MR requires $(n \times \log n)$ bits to store this list. We argue that such storage space can be adequately found in vehicular networks. The LMA is also authorized to replace the identity of any MAG with a new identity.

Each MAG in the domain generates a four-variable symmetric polynomial $f(w,x,y,z)$, which we call the network polynomial, and then sends this polynomial to the LMA. After collecting network polynomials $f_i(w,x,y,z)$ from each MAG$_i$, the LMA computes the domain polynomial $F(w,x,y,z)$ as follows:

$$F(w,x,y,z) = \sum_{i \in_R n}^{l} f_i(w,x,y,z), \qquad 2 \leq l \leq n \tag{3}$$

where n is the number of MAGs in the domain. The LMA randomly chooses and sums l network polynomials from the received n polynomials to construct the domain polynomial. The reason for not summing all the network polynomials is twofold: increasing the secrecy of the scheme from t-secrecy to $t \times 2^n$-secrecy (this is later proven in Section VII-A) and decreasing the revocation overhead at the time of MR's revocation. After constructing the domain polynomial $F(w,x,y,z)$, the LMA evaluates it for each MAG's identity $\mathrm{ID}_{\mathrm{MAG}_i}$. The LMA then securely sends to each MAG its corresponding evaluated polynomial. Later on, the evaluated polynomials $F(\mathrm{ID}_{\mathrm{MAG}_i}, x, y, z)$, with $i = 1, 2, \ldots, n$, are used to generate shared secret keys among arbitrary nodes in the domain.

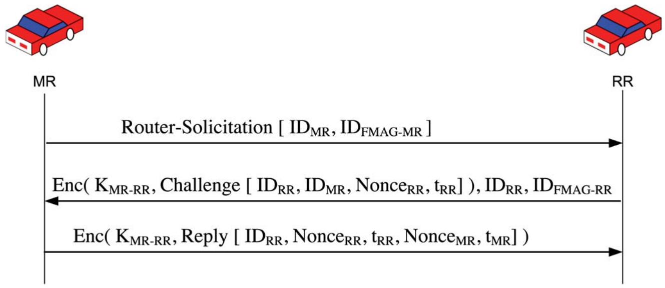

MR
RR
Router-Solicitation [$\mathrm{ID_{MR}}$, $\mathrm{ID_{FMAG\text{-}MR}}$]
Enc($\mathrm{K_{MR\text{-}RR}}$, Challenge [$\mathrm{ID_{RR}}$, $\mathrm{ID_{MR}}$, $\mathrm{Nonce_{RR}}$, $\mathrm{t_{RR}}$]), $\mathrm{ID_{RR}}$, $\mathrm{ID_{FMAG\text{-}RR}}$
Enc($\mathrm{K_{MR\text{-}RR}}$, Reply [$\mathrm{ID_{RR}}$, $\mathrm{Nonce_{RR}}$, $\mathrm{t_{RR}}$, $\mathrm{Nonce_{MR}}$, $\mathrm{t_{MR}}$])

Fig. 5. Authentication phase.

2) MR Registration Phase: When an MR first joins the PMIP domain, it authenticates itself to the MAG to which it is directly connected. This initial authentication may be done by any existing authentication schemes, such as the RSA. After guaranteeing the MR's credentials, the first-attached MAG securely replies by evaluating its domain polynomial $F(\mathrm{ID}_{\mathrm{FMAG}}, x, y, z)$ using the MR's identity, to obtain $F(\mathrm{ID}_{\mathrm{FMAG}}, \mathrm{ID}_{\mathrm{MR}}, y, z)$. Afterward, the LMA also sends the list of current MAGs' identities to the MR. The MR stores this list along with the identity of its first-attached MAG $(\mathrm{ID}_{\mathrm{FMAG}})$. As a result, MR a can establish a shared secret key with another MR b in the same PMIP domain, by evaluating its received polynomial $F(\mathrm{ID}_{\mathrm{FMAG}-a}, \mathrm{ID}_a, y, z)$ to obtain $F(\mathrm{ID}_{\mathrm{FMAG}-a}, \mathrm{ID}_a, \mathrm{ID}_{\mathrm{FMAG}-b}, \mathrm{ID}_b)$. Similarly, b evaluates its received polynomial $F(\mathrm{ID}_{\mathrm{FMAG}-b}, \mathrm{ID}_b, y, z)$ to obtain $F(\mathrm{ID}_{\mathrm{FMAG}-b}, \mathrm{ID}_b, \mathrm{ID}_{\mathrm{FMAG}-a}, \mathrm{ID}_a)$. Since the domain polynomial F is a symmetric polynomial, the two evaluated polynomials result in the same value, and this value represents the shared secret key between MRs a and b, i.e., K_{a-b}.

3) Authentication Phase: Fig. 5 shows the MR–RR authentication phase. When an MR roams to a relayed connection, the neighbor discovery messages for movement detection in MA-PMIP go through an RR. Thus, the goal of this phase is to support mutual authentication between the roaming vehicle and the RR. It is composed of the three stages described as follows.

MR initialization: The MR sends an RS message that includes its identity and its first attached MAG's identity $\mathrm{ID}_{\mathrm{FMAG\text{-}MR}}$. Therefore, the intended RR checks its stored MAG list to see if $\mathrm{ID}_{\mathrm{FMAG\text{-}MR}}$ is currently a valid identity. If there is no identity that is equal to $\mathrm{ID}_{\mathrm{FMAG\text{-}MR}}$, the RR rejects the MR and assumes that it is a revoked or malicious node. Otherwise, if $\mathrm{ID}_{\mathrm{FMAG\text{-}MR}}$ is a valid identity, the RR continues with the next step to check the MR's authenticity.

Challenge generation: By using the MR's identity and $\mathrm{ID}_{\mathrm{FMAG\text{-}MR}}$, the RR generates the shared key $K_{\mathrm{MR-RR}}$, as described in the registration phase. The RR then constructs a challenge message, which includes its own identity $\mathrm{ID}_{\mathrm{RR}}$, the MR's identity, a random number $\mathrm{Nonce}_{\mathrm{RR}}$, and timestamp t_{RR}. Finally, the RR encrypts the challenge message using the shared key $K_{\mathrm{MR-RR}}$, and sends it, along with $\mathrm{ID}_{\mathrm{RR}}$ and its first attached MAG's identity $\mathrm{ID}_{\mathrm{FMAG-RR}}$, to the MR.

Response generation: After receiving the challenge message, the MR checks $\mathrm{ID}_{\mathrm{FMAG-RR}}$ using its stored MAGs' identity list. When guaranteeing that $\mathrm{ID}_{\mathrm{FMAG-RR}}$ is a valid identity, the MR reconstructs the shared key, by using the RR's identity and $\mathrm{ID}_{\mathrm{FMAG-RR}}$, and then decrypts the received challenge message. The MR accepts the RR as a legitimate relay if the RR's decrypted identity is the same as the identity received with the challenge message, i.e., $\mathrm{ID}_{\mathrm{RR}}$. The MR then constructs a reply message, which includes RR's identity, $\mathrm{Nonce}_{\mathrm{RR}}$, t_{RR}, a new random number $\mathrm{Nonce}_{\mathrm{MR}}$, and a timestamp t_{MR}. The MR encrypts the reply message using the shared key and sends it to the RR. The latter decrypts the message and accepts the MR as a legitimate user if the decrypted $\mathrm{Nonce}_{\mathrm{RR}}$ is equal to the original random number that the RR sent in the challenge message.

Once the authentication phase is completed, the RS message is properly forwarded toward the MAG, which allows for MA-PMIP to continue its operation and maintain seamless communications. In Fig. 5, $\mathrm{Enc}(K, M)$ represents an encryption operation of message M using key K.

4) MR Revocation: To achieve backward secrecy, the authentication in the MA-PMIP scheme should guarantee that a revocated MR does not use any of its previous shared keys to deceive an RR. When an MR is revoked, the LMA replaces the MR's first-attached MAG's identity $\mathrm{ID}_{\mathrm{FMAG\text{-}MR}}$ with another unique identity $\mathrm{ID}_{\mathrm{NFMAG}}$ and broadcasts the new identity in a message to all legitimate nodes in the domain. Subsequently, each legitimate node updates its stored MAG list by replacing the old identity with the new one. The LMA also sends a message to each MAG in the domain, which includes a list of the MRs that have $\mathrm{ID}_{\mathrm{NFMAG}}$ as their first-attached MAG's identity, along with an evaluated polynomial $F(\mathrm{ID}_{\mathrm{NFMAG}}, x, y, z)$ for the FMAG's new identity. Afterward, the MAGs send the evaluated polynomial for those MRs that are in the received list and under MAGs' coverage areas. Eventually, each MR in the MR list receives a new evaluated polynomial $F(\mathrm{ID}_{\mathrm{NMAG}}, \mathrm{ID}_{\mathrm{MR}}, y, z)$ for both its identity and the new first-attached MAG's identity. Therefore, instead of changing the entire domain keys, only those MRs that share the same $\mathrm{ID}_{\mathrm{FMAG\text{-}MR}}$ need to change their evaluated polynomials and keys.

VI. Analytical Evaluation of MA-PMIP

A. Signaling Cost and Handover Latency

We evaluate the performance of the MA-PMIP with respect to the following metrics: 1) location update signaling cost C_{BU} (e.g., exchange of proxy binding update/acknowledgment (PBU/PBA) messages); 2) packet delivery overhead cost C_{PD} (e.g., additional IP tunnel headers); and 3) handover delay T_{HD} (i.e., the time the vehicle experiences packet losses due to movement and configuration at the new service area). To calculate these metrics, we follow a methodology similar to [17] to calculate the probability that a vehicle moves across i service areas. We have chosen the MANET centric NEMO (MANEMO) scheme [4] for comparison purposes. Both MANEMO and MA-PMIP enable IP mobility in multihop VANET scenarios and consider communications from the in-vehicle local network. MA-PMIP by default employs authentication and predictive handovers. However, we also analyze the MA-PMIP basic operation.

Assume that the infrastructure is composed of N service areas and that each area is served by one AR. Each well-defined area is square, with perimeter D and area A. The service-area residence time (i.e., the time a vehicle spends inside a service area) is assumed to have a general distribution $f_{\mathrm{SA}}(t)$ with mean $1/\mu$. According to the fluid flow model, the service-area crossing rate μ can be calculated as $\mu = vD/(\pi A)$, where v indicates the average velocity, and π indicates the vehicle's direction.

Since we consider that the IP services consist in the downloading of information from servers at the infrastructure side, only incoming data sessions are studied for simplicity of the analysis. Sessions have an average length of L (packets), with exponentially distributed intersession arrival times and arriving at an average rate λ_I. Each vehicle has independent and identically distributed session arrival rates.

The intersession arrival time is defined as the elapsed time between the arrival of the first data packet of a session and the arrival of the next session's first data packet. During an intersession arrival time, the probability of crossing i service areas, i.e., $\alpha(i)$, is expressed by

$$\alpha(i) = \begin{cases} 1 - \frac{1}{\rho_s}\left[1 - f_{\mathrm{SA}}^{*}(\lambda_I)\right], & \text{if } i = 0 \\ \frac{1}{\rho_s}\left[1 - f_{\mathrm{SA}}^{*}(\lambda_I)\right]^2 \left[f_{\mathrm{SA}}^{*}(\lambda_I)\right]^{i-1}, & \text{if } i > 0 \end{cases} \tag{4}$$

where $\rho_s = \lambda_I/\mu$ indicates the session-to-mobility ratio, and $f_{\mathrm{SA}}^{*}(\lambda_I)$ is the Laplace transform of the service-area residence time distribution [16]. Further derivation details of (4) can be found in [17] and references therein.

The location update signaling cost per handover BU is obtained according to the number of hops the signaling messages have to cross to reach the anchor point (i.e., the LMA in the MA-PMIP and the home agent in MANEMO). It is calculated as follows:

$$\mathrm{BU}^{\text{MA-PMIP}} = d_{\mathrm{MAGs}} \times P + d_{\mathrm{LMA}} \times U^{\text{MA-PMIP}} \tag{5}$$

$$\mathrm{BU}^{\text{MA-PMIP(Basic)}} = d_{\mathrm{LMA}} \times U^{\text{MA-PMIP}} \tag{6}$$

$$\mathrm{BU}^{\mathrm{MANEMO}} = (n \times \omega + d_{\mathrm{HA}})U^{\mathrm{MANEMO}} \tag{7}$$

where d_{MAGs} is the number of hops between the previous and next MAGs, P is the size (in bytes) of the Handover Indicator and Handover Acknowledgment messages in the MA-PMIP with predictive handover, U is the size (in bytes) of BU/BA and PBU/PBA messages, d_{HA} and d_{LMA} are the number of hops for the AR to reach the anchor point, n is the number of links traversed in the multihop path, and ω is the relative weight of transmitting packets over a wireless link compared with a wired link. Note that the PBU/PBA messages in (5) and (6) are only transmitted at the infrastructure side, as defined by the PMIP standard. On the contrary, MANEMO's signaling is transmitted also in the wireless domain.

The total location update signaling cost C_{BU} (bytes × hops), incurred by a vehicle moving across several service areas is calculated as follows:

$$C_{\mathrm{BU}} = \sum_{i=0}^{\infty} i \times \mathrm{BU} \times \alpha(i) \tag{8}$$

where BU is replaced by (5)–(7), accordingly.

The delivery overhead cost per packet PD accounts for extra information and extra links traversed when delivering a data packet from a server to the vehicle. It is computed as follows:

$$\begin{aligned} \mathrm{PD}^{\text{MA-PMIP}} &= d_{\text{server}} + \beta\left(H(d_{\text{LMA}} + d_{\text{MAGs}}) + (n \times \omega)\right) \\ &\quad + (1-\beta)\left(H \times d_{\text{LMA}} + (n \times \omega)\right) \qquad (9) \\ \mathrm{PD}^{\text{MA–PMIP(Basic)}} &= d_{\text{server}} + H \times d_{\text{LMA}} + (n \times \omega) \qquad (10) \\ \mathrm{PD}^{\text{MANEMO}} &= d_{\text{server}} + H(d_{\text{HA}} + n \times \omega) \qquad (11) \end{aligned}$$

where d_{server} is the distance from the application server to the anchor point, and H is the size of the tunneling IP header.

In (9), β represents the portion of packets that traverse the extra PMAG-to-NMAG tunnel before the vehicle is fully detected at the new location during predictive handovers (see Fig. 4). Although MANEMO and MA-PMIP (Basic) require data packets to traverse the same number of hops (i.e., if the LMA and the home agent are equally distanced from the AR), the packets in MANEMO are encapsulated up to the destination vehicle. Instead, MA-PMIP (Basic) employs the tunnel only between the LMA and the serving MAG.

The total packet delivery cost C_{PD} (bytes × hops) considers the number of active hosts m in the in-vehicle network and the average session length L (packets). L depends on downloading data rate γ, packet size S, and intersession arrival rate λ_I. Thus, C_{PD} is calculated as follows:

$$C_{\text{PD}} = m \times \mathrm{PD} \times L \tag{12}$$

where PD is replaced by (9)–(11), accordingly.

Total cost C_T is obtained by adding the total location update and total packet delivery cost of each scheme. Therefore, $C_T = C_{\text{BU}} + C_{\text{PD}}$.

Furthermore, we quantify the delay D_{HD} incurred during a handover event as $D_{\text{HD}} = t_{L2} + t_{\text{MD}} + t_{\text{BU}} + a$. The layer 2 connection delay is represented by t_{L2}, t_{MD} is the movement detection delay, t_{BU} is the location update delay, and a is the anchor point's processing time. Suppose that t_{L2} and a are equivalent in MANEMO and MA-PMIP; therefore, they can be neglected for the comparison. The movement detection is completed when an RS message is received by the AR at the new location. Thus, when employing MANEMO, a vehicle first exchanges RS/RA messages, and then sends the location update signaling to the home agent. We calculate t_{MD} and t_{BU} of MANEMO as follows:

$$\begin{aligned} t_{\text{MD}}^{\text{MANEMO}} &= 2n\tau \qquad (13) \\ t_{\text{BU}}^{\text{MANEMO}} &= 2n\tau + \mathrm{RTT}_{\text{AR-HA}} \qquad (14) \end{aligned}$$

where τ corresponds to the delay between transmission and reception of a data packet in the wireless domain. τ depends on propagation delay δ, link speed C, and access delay due to contention T_w. The round-trip time (RTT) between the AR and the home agent, i.e., $\mathrm{RTT}_{\text{AR-HA}}$, considers the time it takes to exchange BU/BA messages.

TABLE I
COST AND HANDOVER DELAY PARAMETERS

Parameter	Value	Parameter	Value
D	700m	A	490Km^2
ω	2	n	2
$1/\lambda_I$	10s–800s	N	50
d_{HA}	3hops	d_{LMA}	3hops
d_{server}	8hops	d_{MAGs}	1hop
U^{MANEMO}	124bytes	$U^{\text{MA-PMIP}}$	124bytes
P	124bytes	v	30Km/h–110Km/h
H	40bytes	β	5%
m	5hosts	γ	150Kbps–1Mpbs
S	1024bytes	$\delta + S/C$	2.5ms
T_w	0ms–5ms	$RTT_{\text{AR-HA}}$	10ms
$RTT_{\text{MAG-LMA}}$	10ms	$RTT_{\text{PMAG-NMAG}}$	10ms
T_k	3μs	T_e	2μs

Conversely, when MA-PMIP (Basic) is employed, the MAG triggers a location update as soon as the RS is received. Nonetheless, we have to consider the extra delay imposed by the authentication mechanism between source and relay vehicles. Thus, the delays are expressed by

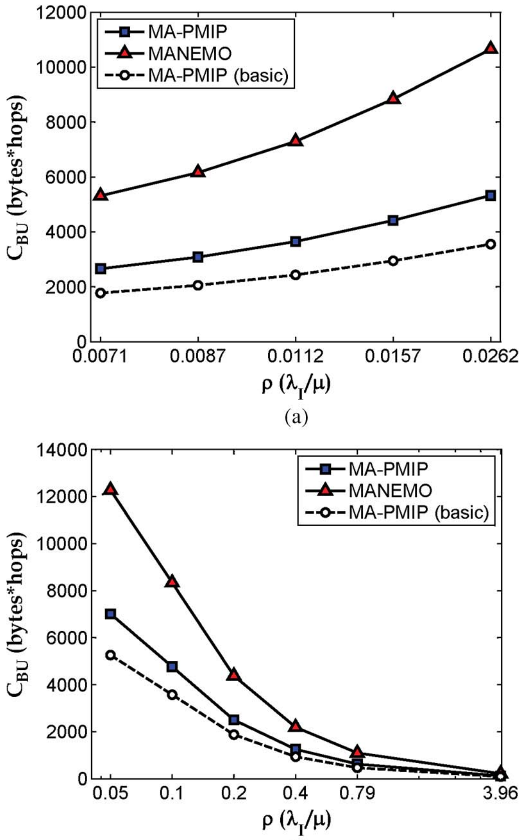
$$\begin{aligned} t_{\text{MD}}^{\text{MA–PMIP(Basic)}} &= n\tau + \mathrm{AUTH} \qquad (15) \\ t_{\text{BU}}^{\text{MA–PMIP(Basic)}} &= \mathrm{RTT}_{\text{MAG–LMA}} + n\tau \qquad (16) \end{aligned}$$

where $\mathrm{AUTH} = 2\tau + 2(T_k + T_e)$. AUTH considers the delays for key generation T_k and for encryption/decryption T_e. Moreover, when MA-PMIP with predictive handovers is employed, packets have been redirected to the new location during the handover. Hence, the reception of packets is immediately resumed after the movement detection is completed. Consequently, the delay calculations are derived as follows:

$$\begin{aligned} t_{\text{MD}}^{\text{MA-PMIP}} &= n\tau + \mathrm{AUTH} \qquad (17) \\ t_{\text{BU}}^{\text{MA-PMIP}} &= 0. \qquad (18) \end{aligned}$$

Numerical results are obtained in MATLAB based on the values presented in Table I. The service-area residence times are assumed to follow an exponential distribution [17]. Fig. 6 shows that MA-PMIP and MA-PMIP (Basic) achieve less location update cost compared with MANEMO. In particular, Fig. 6(a) shows that the difference among the schemes becomes larger for increasing values of ρ, i.e., for longer residence times compared with the session length. However, a different behavior is observed when ρ becomes extremely large. In such a case, the longer session lengths dominate compared with mobility [see Fig. 6(b)], and the three schemes tend to reduce the location update cost. It is also observed that the reduced packet losses in the predictive MA-PMIP come at the cost of a nearly 30% increase of location signaling cost when compared with MA-PMIP (Basic).

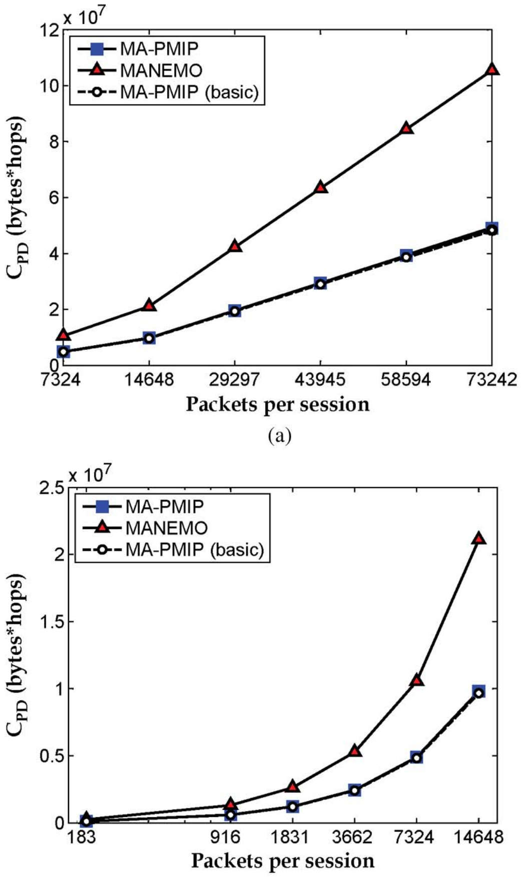
We study the impact of different session lengths (packets) in the packet delivery cost. Different downloading data rates and session arrival rates are studied. Fig. 7 shows how the packet delivery cost naturally increases for longer data sessions. However, MA-PMIP still outperforms MANEMO with a reduced cost. Based on the same figure, it is observed that the packet overhead introduced by the prediction mechanism is almost equivalent to the basic MA-PMIP. This is because only a



(a)

(b)

Fig. 6. Location update comparison. (a) Different velocities $(1/\lambda_I) = 600$ s, and $v = 110$ Km/h $-$ 30 Km/h. (b) Different session lengths $v = 50$ Km/h, and $(1/\lambda_I) = 800$ s $-$ 10 s.



(a)

(b)

Fig. 7. Packet delivery comparison. (a) Different rates $\gamma = 200$ Kb/s $-$ 4Mb/s, $S = 300$ B, and $(1/\lambda_I) = 600$ s. (b) Different session lengths $v =$ 150 Kb/s $(1/\lambda_I) = 800$ s $-$ 10 s, and $S = 300$ B.

percentage of packets are affected by the double encapsulation when the MAG-to-MAG tunnel is employed.

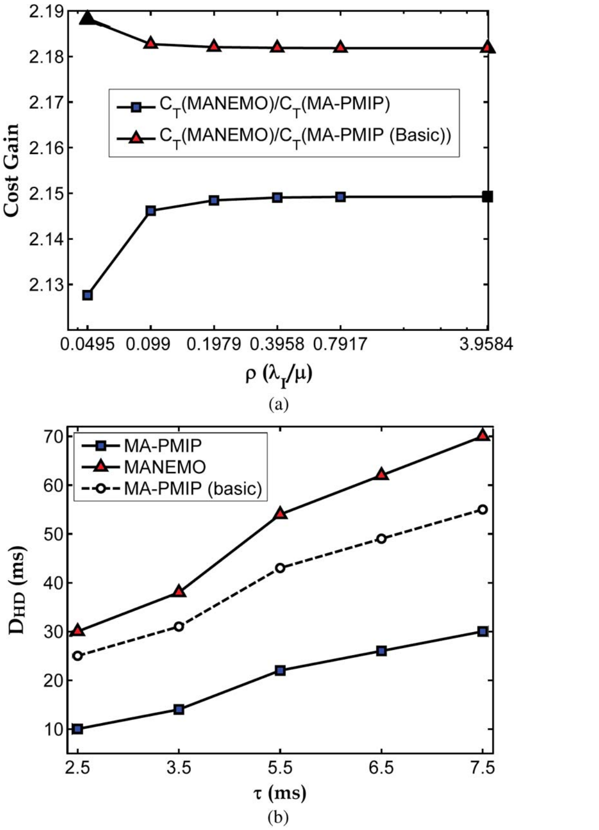
Furthermore, we calculate the total cost gain as $C_T(\text{MANEMO})/C_T(\text{MA-PMIP})$. Since the results in Fig. 6(b) show a decreasing difference among the different location update costs, we employ the cost gain to demonstrate that, even when the three schemes behave similar for large values of ρ, the total reduction in cost is still dominated by the reduced packet delivery overhead. Fig. 8(a) shows that the gain becomes stable when ρ becomes large. Both MA-PMIP and MA-PMIP (Basic) achieve less than half of the total cost of MANEMO.

Although we introduce additional signaling for authenticating the handovers through I2V2V communications, the MA-PMIP handover delay remains lower than the one in MANEMO, albeit the latter does not consider any authentication mechanism. This behavior is shown in Fig. 8(b). It is observed that the additional signaling employed by MA-PMIP with predictive handovers (see Fig. 6) significantly reduces the handover delay [see Fig. 8(b)]. Thus, the reception of data packets is resumed near two times faster than in MA-PMIP (Basic), and 2.3–3 times faster than in MANEMO.

B. Authentication Computation and Communication Overheads

Here, we evaluate the performance of MA-PMIP with respect to the computation and communication overheads required by the authentication mechanism proposed in Section V-D. Table II shows a comparison between MA-PMIP and previous multihop authentication schemes. T represents the required time for an operation, and B represents the transmitted bytes. Our scheme has the smallest computation overhead among the reported schemes because the authentication requires only two symmetric key encryption operations $(2 \times T_c)$. AMA [28] and the GMSP [24] require time for signing and verifying signatures (T_s, T_v); hence, their computation overheads are higher than that in MA-PMIP. Similarly, the multihop MIP scheme [25] consumes a time T_{EAP} in achieving the Extensible Authentication Protocol, which includes at least one signature and one verification.

Considering the communication overhead perspective, we observe that AMA, GMSP, and multihop MIP require to transmit a sender certificate in each transmitted message. Instead, MA-PMIP exchanges the list of MAGs only once at the key establishment phase and the challenge/response messages $B_{\text{CHL/RESP}}$ during handovers. The average length of the sender certificate is 3500 bytes, whereas the list of MAGs has a length of $n \log_2 n$ bits, where n is the number of MAGs in the PMIP domain. Therefore, MA-PMIP would require to satisfy the condition $n \log_2 n \geq 28\,000$ bits $\times\, m$, where m is the number of transmitted messages in the certificate-based



(a)

(b)

Fig. 8. Cost gain and Handover delay. (a) Cost gain comparison $(1/\lambda_I) = 800$ s $- 10$ s, $v = 50$ Km/h, $S = 300$ B, and $\gamma =$ 150 Kb/s. (b) Handover delay $T_w = 0$ ms $- 5$ ms, and $\delta + S/C = 2.5$ ms.

TABLE II
COMPUTATION AND COMMUNICATION OVERHEADS

Scheme	Computation overhead	Communication overhead
AMA [28]	$T_s + T_v \times Pr_{check}$	B_{cert}
GMSP [24]	$T_s + T_v + T_c$	B_{cert}
Multi-hop MIP [25]	$T_c + T_{EAP}$	$B_{EAP} + B_{key-exchange}$
ALPHA [27]	$T_c + T_{disclose}$	$B_{ACK} + B_{disclose}$
MA-PMIP	$2 \times T_c$	$B_{FMAGs-list} + B_{CHL/RESP}$

schemes, in order for MA-PMIP to have a higher communication overhead than the other schemes. Consequently, n should be at least $236.64\sqrt{m}$ to satisfy such a condition. However, since n is a fixed value, and m increases over time with the length of active sessions, n becomes much smaller than m with time. Therefore, the condition cannot be satisfied, and MA-PMIP's communication overhead is lower compared with the certificate-based schemes. Note that ALPHA [27] results in the smallest communication overhead; however, it suffers from a T_{disclose} delay in the computation overhead, which is required before disclosing the secret key.

In Fig. 9, we employ Crypto++ benchmark[1] to compare the authentication operation cost of each scheme. We use AES and RSA 1024 (for symmetric and public key operations, respectively) to calculate the computation time required by the different schemes. The RTT between vehicle and relay node is 5 ms.

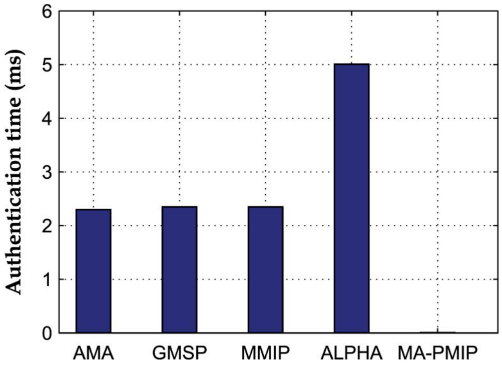


Fig. 9. Comparison of computation time for authentication in MA-PMIP and existing schemes based on Crypto++ benchmark.

VII. SECURITY ANALYSIS OF MA-PMIP

The security of MA-PMIP is based on the secrecy level of the key establishment phase in the proposed authentication scheme. Therefore, in the following, we compute the security level of MA-PMIP and show that it thwarts both the internal and external adversaries defined in Section IV-B.

A. Internal Adversaries

MA-PMIP thwarts the impersonation attacks by using a shared secret key, which is only known by the two communicating entities. To illustrate this, consider adversary A, which aims to impersonate an MR to join an NMAG through an RR and to benefit illegally from the domain services. First, A sends an RS message and attaches the MR's identity ID_{MR}. The RR replies with a challenge message, which is encrypted by the shared key $K_{\text{MR-RR}}$. To pass the authentication check, A needs to decrypt the challenge message and identify the RR's random number Nonce_{RR}, which is included in the encrypted challenge message. However, A cannot reconstruct the shared key by using only the identities of the MR and RR. In addition to the identities, the adversary needs to know one of the evaluated polynomials $F(\text{FMAG}_{\text{MR}}, \text{ID}_{\text{MR}}, y, z)$ or $F(\text{FMAG}_{\text{RR}}, \text{ID}_{\text{RR}}, y, z)$. Since the evaluated polynomials are secret, it is impossible for an impersonation adversary to break the authentication in MA-PMIP.

Moreover, MA-PMIP mitigates the collusion attacking effect by increasing its secrecy level. Generally, a t-degree symmetric polynomial allows for a t-secrecy scheme, which means that $t + 1$ colluders are needed to identify the secret polynomial and reconstruct the whole system's keys. However, in our scheme, the domain polynomial is constructed as in (3), where the LMA randomly selects a group of the network polynomials to calculate the domain polynomial. In the following theorem, we show that at least $t \times 2^n + 1$ colluders are needed to break our authentication scheme's secrecy.

Theorem 1: The proposed MA-PMIP achieves $t \times 2^n$-secrecy level.

Proof: If we consider the secrecy of each network polynomial as t, then the secrecy s of the domain polynomial can be

[1] http://www.cryptopp.com/benchmarks.html

computed as follows:

$$\begin{aligned} s &= \sum_{k=2}^{n} \binom{n}{k} \times t \\ s &= t \times \sum_{k=0}^{n} \binom{n}{k} - \left[\binom{n}{0} + \binom{n}{1} \right] \\ s &= t \times \left[2^n - (1+n) \right] \\ s &\simeq t \times 2^n \end{aligned} \tag{19}$$

where n is the number of MAGs in the domain, and t is the degree of network polynomials. Since the secrecy increases from t to $t \times 2^n$, the number of colluders that can break the scheme also increases from $t+1$ to $(t \times 2^n)+1$. ■

Consequently, as a way to mitigate the colluder attacks in our scheme, t is chosen to be a large number, and n should be preferably large.

B. External Adversaries

Similar to impersonation attacks, DoS attackers may trigger forged RS messages to exhaust the RR and MAG resources. Without authentication in MA-PMIP, the RR forwards all RS messages to the MAG and facilitates the DoS attack. However, using the authentication, a DoS adversary A should know a valid shared key $K_{\mathrm{MR}_i-\mathrm{RR}}$ in order for the RR to forward the RS message. Since A is an external adversary, it cannot construct any key, even if it knows the identity of a legitimate MR.

On the other hand, A may repeat one of the RS messages that have been previously transmitted by a valid user, to trigger a replay attack. However, MA-PMIP thwarts this attack by adding both timestamp and random nonce for each transmitted message between the MR and the RR. Finally, A may trigger an MITM attack to impersonate an MR or an RR. However, given that both the challenge and replay messages are encrypted, A cannot replace the MR or RR identities. Once more, A would need to know the shared key first to perform such an attack.

VIII. Experimental Evaluation

We have performed OMNeT++ simulations to corroborate the analytical evaluation and security analysis presented in Sections IV and VII, respectively. The MiXiM and INET packages are used for simulating wireless communications and the TCP/IP stack, respectively. We have implemented the MA-PMIP and MA-PMIP (Basic) schemes, which are compared with the implementations of MANEMO [4] and the standard PMIP [9] in terms of IP mobility support. Our schemes are also compared with the implementation of AMA [28], in terms of the impact of the security mechanisms on the ongoing communications.

A. Proof of Concept

A simulation scenario similar to the one presented in [4] is considered for our proof of concept, where the ARs are evenly deployed over a road segment, and the vehicle of interest moves at a constant average speed v_r. The vehicle connects through one-hop and two-hop paths with the infrastructure, to download IP packets from an external application server. In each handover, we consider the worst case scenario in which, every time the vehicle joins a new AR, it first connects through a relay. Hence, the MA-PMIP's authentication is performed before the forwarding of the RS is completed.

TABLE III
Simulation Parameters

PHY Layer	Frequency 2.4GHz, Link rate 5.5Mbps, Tx power 2.3mW/25mW (vehicles/AR), Antennas' height 1.5m/3m (vehicles/AR), Sensitivity -80dBm
MAC Layer	802.11 ad hoc mode, RTS/CTS disabled, SNR threshold 2.6dB
Geo-routing Layer	Beacon rate 1pkt/s, Geo-header size 12B
Network Layer	Router Adv rate uniform(0.5s,1.5s),
Application Layer	Bidirectional CBR (best-effort) γ=150Kbps, Bidirectional VBR (video-conferencing) γ=384Kbps, Unidirectional VBR (streaming) γ=512Kbps, VBR σ_γ=0.010s, Packet sizes 300B/1024B (CBR/VBR), Session length 600s
Prediction mode	κ=0.875, threshold=4s, bufferSize=30KB$\sim$1MB
Infrastructure connections	$\mathrm{RTT}_{\text{MAG-LMA}}$=10ms, $\mathrm{RTT}_{\text{PMAG-NMAG}}$=10ms, $\mathrm{RTT}_{\text{AR-HA}}$=10ms, $\mathrm{RTT}_{\text{LMA(HA)-IP Server}}$=20ms

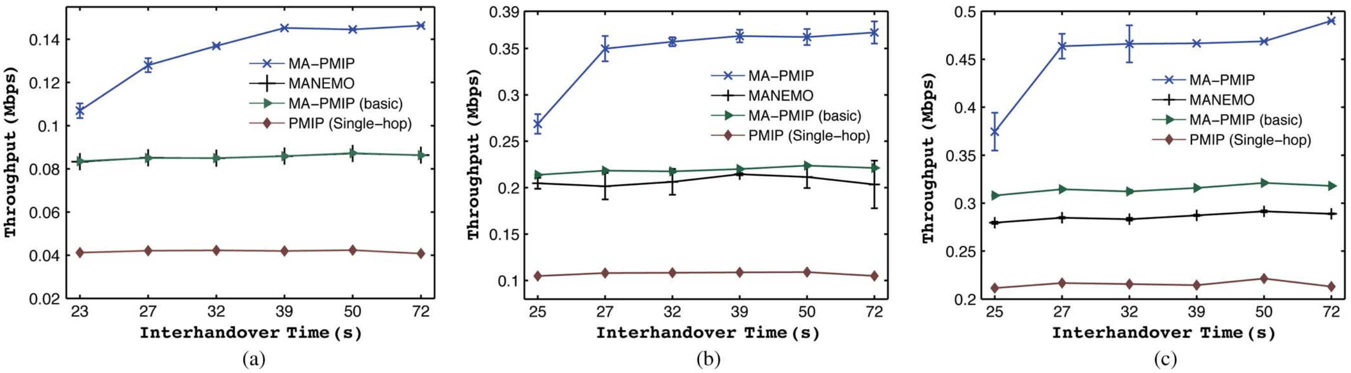
TABLE IV
Road Traffic Parameters

Density	k=30v/Km/lane, k_j=120v/Km/lane;
Velocity	v_r=35$\sim$65Km/h (urban), v_r=80$\sim$110Km/h (highway)
Free-flow speed	v_f=50Km/h (urban), v_f=100Km/h (highway)
Road type	Straight road – two lanes
AR inter-distance	1000m

Nodes in the VANET consume transmission power near 1/10 smaller than the one by ARs, which conveys the asymmetric links between vehicles and ARs (i.e., all the links between ARs and vehicles become asymmetric as soon as a vehicle moves away from the AR, and the AR falls outside the vehicle's transmission range). In a free-space path-loss environment, the values employed for transmission power lead to radio ranges near 150 and 500 m, for vehicles and ARs, respectively. Furthermore, we apply the two-ray interference model—a measurement-based enhanced version of the two-ray ground propagation model for VANETs [34]—for the simulation of radiowave propagation.

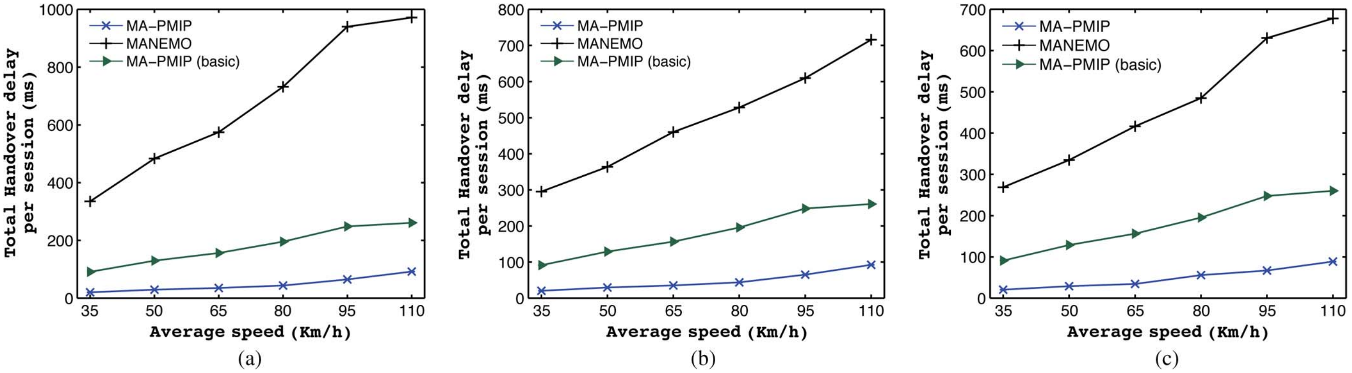
The simulation and road traffic parameters are provided in Tables III and IV, respectively. Although we employ a generic 802.11 wireless technology in our simulations, MA-PMIP is agnostic to the wireless local area network technology employed at the MAC/physical layer. The downstream throughput and handover delay are evaluated considering three types of traffic: constant bit rate (CBR) bidirectional, variable bit rate (VBR) bidirectional, and VBR unidirectional. The first two types account for applications that require a bidirectional link; CBR represents best effort traffic (low-to-medium data rate), such as Internet browsing or e-mail fetching, and VBR represents more demanding applications with medium-to-high data rates. Unidirectional VBR traffic requires only a one-way connection for the delivery of UDP packets after the session has been established, such as in video streaming. All simulation results are plotted with a 95% confidence interval.

The throughput comparisons are shown in Fig. 10. The performance observed in Fig. 10(a) shows that MA-PMIP (Basic) and MANEMO are almost equivalent in the case of CBR traffic.



(a) (b) (c)

Fig. 10. Throughput for different types of traffic versus interhandover time. (a) Bidirectional CBR traffic $\gamma = 150$ Kb/s. (b) Bidirectional VBR traffic $\gamma = 384$ Kb/s. (c) Unidirectional VBR traffic $\gamma = 512$ Kb/s.



(a) (b) (c)

Fig. 11. Total handover delay (I2V2V) for different types of traffic versus average speed. (a) Bidirectional CBR traffic $\gamma = 150$ Kb/s. (b) Bidirectional VBR traffic $\gamma = 384$ Kb/s. (c) Unidirectional VBR traffic $\gamma = 512$ Kb/s.

This is because, with low data rates (one packet per 16 ms), the handover delay in the two schemes becomes almost transparent to the flow of packets. However, the extended coverage of the link vehicle → AR, which is provided by the geonetworking layer, allows for a longer reception of packets and a reduction of 27% of packet losses compared with the standard PMIP. Nevertheless, both MANEMO and MA-PMIP (Basic) suffer from packet losses as soon as the bidirectional link is lost, when the vehicle is unable to connect to a relay that may establish a link toward the infrastructure. Such a problem is alleviated by the prediction feature in MA-PMIP. Since packets are buffered at the new location, MA-PMIP allows for a near lossless reception of packets. Similar results are obtained with VBR traffic. In Fig. 10(b) and (c), it is interesting to see that, for increasing data rates, the performance of MA-PMIP (Basic) outperforms that of MANEMO. This is mainly due to an increase in γ, which is more sensitive to the handover delay.

Fig. 11 shows the average total delay accumulated from all the handovers during the simulation runs. As expected, the total delay of all schemes increases with the increase in velocity. This is due to the vehicle traversing the service areas at a higher rate (i.e., there are reduced residence times); hence, the signaling for handover is exchanged more often. Nevertheless, it can be observed that MA-PMIP and MA-PMIP (Basic) result in a reduced delay. MA-PMIP achieves the lowest delay due to the proactive signaling, which allows for the resumption of the flow of packets as soon as the RS message is forwarded to the MAG in the new service area.

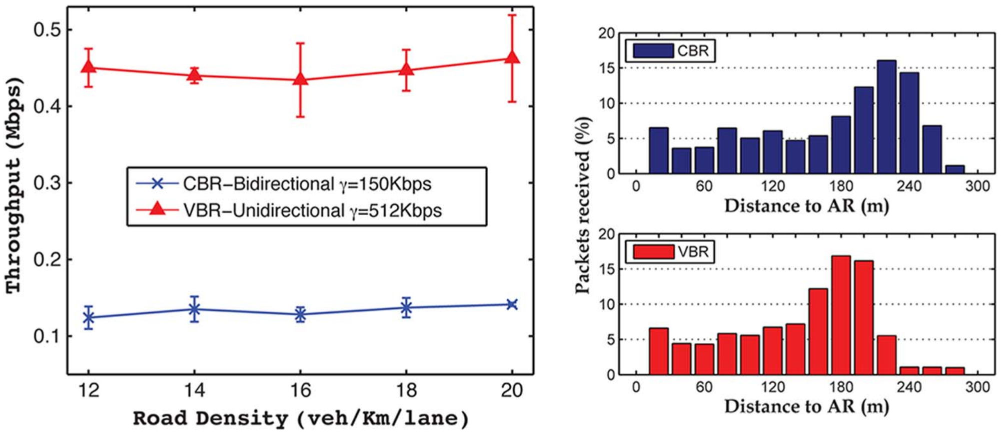
TABLE V
NEW ROAD TRAFFIC PARAMETERS

Density	k=12∼20v/Km/lane, k_j=120v/Km/lane;
Velocity	v_{initial}=80Km/h
Free-flow speed	v_f=100Km/h
Acceleration	$10\% * v_f$
Change of lane	disabled
Road type	Straight road – two lanes
AR inter-distance	1000m

B. More Realistic Simulation Scenario

After our proof of concept of a vehicle moving at a constant average speed, we now employ a more realistic scenario in which all nodes, i.e., vehicles and relays, are traveling at variable speeds on a two-lane highway. The velocity is controlled every Δt according to the formula $v(t+\Delta t) = \min[\max(v(t)+\Delta v, 0), v_f]$, where $\Delta v = \texttt{uniform}(-a * \Delta t, a * \Delta t)$. The change of speed is given by acceleration a, but the resulting speed is always bounded by the maximum speed of the highway v_f [35]. The details of the road traffic parameters employed in this scenario are presented in Table V. We maintain the constraint of a maximum of two hops for the georouting layer to forward a packet in the wireless domain.

The throughput is evaluated for IP applications with CBR bidirectional and VBR unidirectional traffic. By employing different road densities and a variable velocity, we check the effectiveness of delivering packets when the relay selected for



(a) (b)

Fig. 12. MA-PMIP in a realistic highway scenario. (a) Throughput versus road density. (b) Packets received at different distances density $= 20$ v/Km/lane.

forwarding varies from one packet to the succeeding packet. The road densities employed during simulations are all classified as noncongested flow conditions, ranging from reasonable free flow to stable traffic in a highway scenario. Fig. 12(a) shows that MA-PMIP still achieves a throughput close to the original downloading data rate γ. We can observe that, even when the density plays an important role in finding available relays to reach the infrastructure, our scheme is able to adapt to the road traffic conditions, particularly because the geographical protocol takes the forwarding decision on a per-packet basis. The throughputs shown in Fig. 12(a), which are obtained from fully mobile and variable traffic conditions, are consistent with the results obtained in the simulated proof of concept (see Fig. 10).

Furthermore, Fig. 12(b) shows the average percentage of delivered packets for different distances between the vehicle and the AR. It is observed that the majority of packets are delivered when the node is more than one-hop away from the AR (distance $> r$). This is due to the predictive mechanism, in which the buffered packets are delivered as soon as the vehicle hands over through a two-hop connection in the new service area. Since we have limited the multihop paths to two hops, there are no packets received for distances larger than 300 m.

C. Buffering During Predictive Handovers

One of the salient features of MA-PMIP is the ability to forward packets in advance to the new service area where the vehicle is roaming. However, this mechanism requires having storage space for the buffering of packets at the NMAG. Thus, we evaluate the packet losses due to different buffer sizes in the NMAG so that we have insight into the space required for an application to perceive a lossless flow of packets. In our test scenario, the vehicle is moving at an average speed $v_r = 50$ Km/h, downloading CBR best effort traffic at a rate of $\gamma = 150$ Kb/s.

Fig. 13 shows the percentage of packet losses when we limit the NMAG's buffer size from 100 to 5000 packets. In our example application, a buffer of approximately 1500 packets (i.e., 450 kB for packet sizes of 300 B) would be enough to maintain seamless communications. The buffer size employed in real deployments should consider scalability issues when the density is high, and several vehicles at a time trigger the predictive handover. Nonetheless, for real-time applications that are sensitive to delay, the predictive handover only helps to reduce the signaling after the vehicle roams to the new service area, because the buffering of real-time traffic is not suitable for such applications.

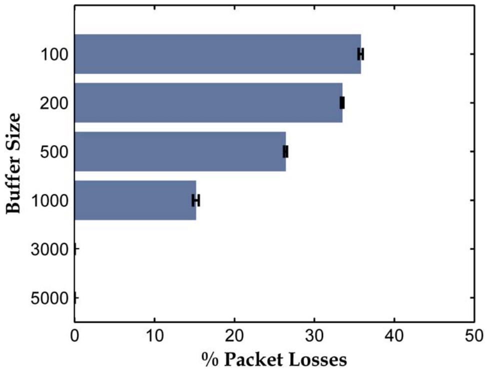
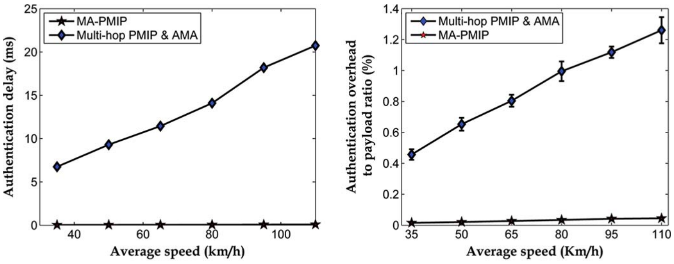


Fig. 13. MA-PMIP packet losses due to buffer overflow.



(a) (b)

Fig. 14. Evaluation of authentication mechanism in MA-PMIP. (a) Authentication delay. (b) Communication overhead.

D. Authentication Performance During Handovers

To measure and compare the impact of the MA-PMIP authentication mechanism, we have integrated an implementation of AMA [28], with a simplified version of a multihop PMIP scheme (i.e., MA-PMIP with our proposed authentication mechanism disabled). Fig. 14(a) shows the authentication delay when the vehicle moves at different average velocities.

Fig. 14(b) shows the comparison in terms of the authentication-overhead-to-payload ratio. As shown in both figures, MA-PMIP not only requires smaller delay and communication overhead than multihop PMIP and AMA but also has almost fixed impact for different velocities. On the other hand, multihop PMIP and AMA have authentication delay and communication overheads that increase almost linearly with velocity.

Compared with multihop PMIP and AMA, MA-PMIP achieves reductions of 99.6% and 96.8% in authentication delay and communication overhead, respectively. The reason for these reductions is the high computation and communication efficiency achieved by our proposed authentication scheme. Therefore, unlike multihop PMIP and AMA, MA-PMIP can be used with seamless mobile applications, such as voice over IP and video streaming.

IX. Conclusion

In this paper, we have proposed a Multihop-Authenticated Proxy Mobile IP scheme, which is designed to enable secure roaming of IP applications in multihop vehicular environments. We have employed the information available in VANETs, such as geographical location and road density, to enhance the performance of PMIP, coupled with a geonetworking layer. MA-PMIP considers the presence of asymmetric links in VANETs and takes the advantage of multihop communications to achieve extended bidirectional links between vehicles and the infrastructure. In addition, aiming to authenticate mutually a vehicle and its relay node, MA-PMIP incorporates an authentication scheme so that the IP communications can be securely handed over across different IP networks. We have provided both numerical and experimental simulations of realistic highway scenarios, which have shown the effectiveness of MA-PMIP to maintain near lossless flows of packets for vehicles with ongoing IP sessions.

For our future work, we will improve the performance of the predictive mechanism of MA-PMIP in two different ways. First, we will investigate an optimal threshold value for the predictive mechanism of MA-PMIP. The threshold determines the moment at which packets are forwarded to the next service area; hence, it has an important impact on the reduction of packet losses during handovers. Parameters such as traffic conditions and storage capacity at the NMAG will be considered. Second, we will study the impact of employing different weights in the calculation of the estimated velocity, which can be customized according to traffic conditions in each service area. Finally, the performance of the MA-PMIP scheme will be investigated using real-world mobility traces that account for variable traffic conditions in highway scenarios.

References

[1] H. Liang and W. Zhuang, "Double-loop receiver-initiated mac for cooperative data dissemination via roadside WLANs," *IEEE Trans. Commun.*, vol. 60, no. 9, pp. 2644–2656, Sep. 2012.

[2] H. Shan, W. Zhuang, and Z. Wang, "Distributed cooperative MAC for multihop wireless networks," *IEEE Commun. Mag.*, vol. 47, no. 2, pp. 126–133, Feb. 2009.

[3] M. Asefi, S. Céspedes, X. Shen, and J. W. Mark, "A seamless quality-driven multi-hop data delivery scheme for video streaming in urban VANET scenarios," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2011, pp. 1–5.

[4] R. Baldessari, W. Zhang, A. Festag, and L. Le, "A MANET-centric solution for the application of NEMO in VANET using geographic routing," in *Proc. TridentCom*, Mar. 2008, p. 12.

[5] J. Yoo, B. S. C. Choi, and M. Gerl, "An opportunistic relay protocol for vehicular road-side access with fading channels," in *Proc. IEEE Int. Conf. Comput., Netw. Commun.*, Oct. 2010, pp. 233–242.

[6] M. E. Mahmoud and X. Shen, "PIS: A practical incentive system for multihop wireless networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 4012–4025, Oct. 2010.

[7] N. Lu, T. H. Luan, M. Wang, X. Shen, and F. Bai, "Capacity and delay analysis for social-proximity urban vehicular networks," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 1476–1484.

[8] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 127–139, Mar. 2012.

[9] IETF, IETF Datatracker: Internet Drafts and RFC's, Dec. 2012. [Online]. Available: https://datatracker.ietf.org/

[10] R. Blom, "An optimal class of symmetric key generation systems," in *Proc. EUROCRYPT' 84*, 1985, pp. 335–338.

[11] P. Mitra and C. Poellabauer, "Asymmetric geographic forwarding," *Int. J. Embedded and Real-Time Commun. Syst.*, vol. 2, no. 4, pp. 46–70, Oct. 2011.

[12] A. Amoroso, G. Marfia, M. Roccetti, and C. E. Palazzi, "A simulative evaluation of V2V algorithms for road safety and in-car entertainment," in *Proc. Int. Conf. Comput. Commun. Netw.*, Jul. 2011, pp. 1–6.

[13] Y.-J. Kim, R. Govindan, B. Karp, and S. Shenker, "Geographic routing made practical," in *Proc. USENIX Symp. Netw. Syst. Des. Implement.*, 2005, pp. 217–230.

[14] I. Ben Jemaa, M. Tsukada, H. Menouar, and T. Ernst, "Validation and evaluation of NEMO in VANET using geographic routing," in *Proc. Int. Conf. ITS Telecommun.*, Nov. 2010, p. 6.

[15] *Intelligent Transport Systems (ITS); Vehicular Communications; Geonetworking; Part 6: Internet Integration; Sub-Part 1: Transmission of IPv6 Packets Over Geonetworking Protocols*, Eur. Telecommun. Stand. Inst., France, Tech. Spec., Nov. 2011.

[16] S. Pack, T. Kwon, Y. Choi, and E. K. Paik, "An adaptive network Mobility support protocol in hierarchical mobile IPv6 networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 7, pp. 3627–3639, Sep. 2009.

[17] J.-H. Lee, T. Ernst, and N. Chilamkurti, "Performance analysis of PMIPv6-based network mobility for intelligent transportation systems," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 74–85, Jan. 2012.

[18] S. Jeon and Y. Kim, "Cost-efficient network mobility scheme over proxy mobile IPv6 network," *IET Commun.*, vol. 5, no. 18, pp. 2656–2661, Dec. 2011.

[19] I. Soto, C. J. Bernardos, M. Calderon, A. Banchs, and A. Azcorra, "Nemo-enabled localized mobility support for Internet access in automotive scenarios," *IEEE Commun. Mag.*, vol. 47, no. 5, pp. 152–159, May 2009.

[20] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3589–3603, Sep. 2010.

[21] R. Lu, X. Li, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86–96, Jan. 2012.

[22] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "SLAB: A secure localized authentication and billing scheme for wireless mesh networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 10, pp. 3858–3868, Oct. 2008.

[23] C. Tang and D. O. Wu, "An efficient mobile authentication scheme for wireless networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1408–1416, Apr. 2008.

[24] B. Xie, A. Kumar, S. Srinivasan, and D. P. Agrawal, "GMSP: A generalized multi-hop security protocol for heterogeneous multi-hop wireless network," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2006, vol. 2, pp. 634–639.

[25] A. Al Shidhani and V. C. M. Leung, "Secure and efficient multi-hop mobile IP Registration scheme for MANET-Internet integrated architecture," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2010, pp. 1–6.

[26] Y. Jiang, C. Lin, X. Shen, and M. Shi, "Mutual authentication and key exchange protocols for roaming services in wireless mobile networks," *IEEE Trans. Wireless Commun.*, vol. 5, no. 9, pp. 2569–2577, Sep. 2006.

[27] T. Heer, S. Götz, O. G. Morchon, and K. Wehrle, "ALPHA: An adaptive and lightweight protocol for hop-by-hop authentication," in *Proc. ACM CoNEXT*, Dec. 2008, pp. 23:1–23:12.

[28] N. Ristanovic, P. Papadimitratos, G. Theodorakopoulos, J.-P. Hubaux, and J.-Y. Le Boudec, "Adaptive message authentication for multi-hop networks," in *Proc. Int. Conf. Wireless On-demand Network Syst. Services*, Jan. 2011, pp. 96–103.

[29] R. Baldessari, C. J. Bernardos, and M. Calderon, "GeoSAC—Scalable address autoconfiguration for VANET using geographic networking concepts," in *Proc. IEEE PIMRC*, Sep. 2008, pp. 1–7.

[30] T. H. Luan, X. Ling, and X. Shen, "MAC in motion: Impact of mobility on the MAC of drive-thru Internet," *IEEE Trans. Mobile Comput.*, vol. 11, no. 2, pp. 305–319, Feb. 2012.

[31] A. Gupta, A. Mukherjee, B. Xie, and D. P. Agrawal, "Decentralized key generation scheme for cellular-based heterogeneous wireless ad hoc networks," *J. Parallel Distrib. Comput.*, vol. 67, no. 9, pp. 981–991, Sep. 2007.

[32] K. R. C. Pillai and M. P. Sebastai, "A hierarchical and decentralized key establishment scheme for end-to-end security in heterogeneous networks," in *Proc. IEEE Int. Conf. Internet Multimedia Syst. Arch. Appl.*, Dec. 2009, pp. 1–6.

[33] S. Taha, S. Céspedes, and X. Shen, " EM^3A: Efficient mutual multi-hop mobile authentication scheme for pmip networks," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2012, pp. 873–877.

[34] C. Sommer and F. Dressler, "Using the right two-ray model? A measurement based evaluation of PHY models in VANETs," in *Proc. ACM MobiCom*, Sep. 2011, pp. 1–3.

[35] T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for ad hoc network research," *Wireless Commun. Mobile Comput. (WCMC): Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications*, vol. 2, no. 5, pp. 483–502, Aug. 2002.

Sandra Céspedes (S'09–M'12) received the B.Sc.(Hons.) and Specialization degrees in Telematics Engineering and Management of Information Systems from Icesi University, Cali, Colombia, in 2003 and 2007, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2012.

She is currently a Faculty Member with the Department of Information and Communications Technology, Icesi University. Her research interests include routing and mobility management in vehicular communications systems, as well as IPv6 integration and routing in smart grid communications.

Dr. Céspedes has been a Fellow of the Internet Society since 2007, through which she participates in the standardization process of the Internet Engineering Task Force.

Sanaa Taha (S'13) received the B.Sc. and M.Sc. degrees from the Department of Information Technology, Faculty of Computers and Information, Cairo University, Cairo, Egypt, in 2001 and 2005, respectively. She is currently working toward the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada.

Her research interests include wireless network security, mobile networks security, mobility management, and applied cryptography.

Xuemin (Sherman) Shen (M'97–SM'02–F'09) received the B.Sc. degree from Dalian Maritime University, Dalian, China, in 1982 and the M.Sc. and Ph.D. degrees from Rutgers University, Newark, NJ, USA, in 1987 and 1990, respectively, all in electrical engineering.

From 2004 to 2008, He was the Associate Chair for Graduate Studies with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, where he is currently a Professor and a University Research Chair. He is a coauthor/editor of six books and is the author of more than 600 papers and book chapters on wireless communications and networks, control, and filtering. His research interests include resource management in interconnected wireless/wired networks, wireless network security, wireless body area networks, and vehicular ad hoc and sensor networks.

Dr. Shen is a registered Professional Engineer of Ontario, Canada, a Fellow of the Engineering Institute of Canada, and a Distinguished Lecturer of IEEE Vehicular Technology and Communications Societies. He served as the Technical Program Committee Chair for the IEEE 72nd Vehicular Technology Conference (IEEE VTC) in Fall 2010; the Symposium Chair for the IEEE International Conference on Communications (IEEE ICC) in 2010; the Tutorial Chair for the IEEE ICC in 2008 and for the IEEE VTC in Spring 2011; the Technical Program Committee Chair for the IEEE Global Communications Conference in 2007; the General Cochair for the International Conference on Communications and Networking in China in 2007 and the Third International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks in 2006; and the Chair for IEEE Communications Society Technical Committee on Wireless Communications and Peer-to-Peer Communications and Networking. He also serves/served as the Editor-in-Chief for IEEE NETWORK, the *Peer-to-Peer Networking and Application*, and the *Institution of Engineering and Technology Communications*; a Founding Area Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS; an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, *Computer Networks*, and the *Association for Computing Machinery (ACM) Wireless Networks*, etc.; and a Guest Editor for IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS, IEEE COMMUNICATIONS MAGAZINE, and *ACM Mobile Networks and Applications*. He received the Excellent Graduate Supervision Award in 2006; the Outstanding Performance Award in 2004, 2007, and 2010 from the University of Waterloo; the Premier's Research Excellence Award in 2003 from the Province of Ontario, Canada; and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo.