IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 5, Ver. IV (Sep. – Oct. 2015), PP 82-87
www.iosrjournals.org

Secure seamless access to IP applications and IP service availability in VANET

[1]Sachin More, [2]Prof. Uma Nagaraj
[1]*M.E Student, Department of CE, MIT Academy of Engineering Pune, India*
[2]*Department of Computer MIT Academy of Engineering, Pune, India*

***Abstract**: Traditional Internet-based applications and driver assistance services, as well as peer-to-peer applications are services that will make traveling a more convenient and pleasant experience, that enable the instant sharing of information between vehicles. The multi-hop Vehicular Communications Network (VCN) appears as a promising solution for the ubiquitous access to IP services in vehicular environments. Longer bidirectional connections between road side access routers and vehicles can be established through multi-hop paths. The bi-directionality of links is a strong requirement of most IP applications, and it is difficult to be achieved when asymmetric links appear in the vehicular wireless network.*
***Keywords:** I2V2V, Handover, Symmetric Polynomials*

I. Introduction

The technology in Vehicular systems will be next domain where we will connect to the world. Traditional Internet-based applications and driver assistance services, as well as peer-to-peer applications are services that will make traveling a more convenient and pleasant experience. that enable the instant sharing of information between vehicles The multi-hop Vehicular Communications Network (VCN) appears as a promising solution for the ubiquitous access to IP services in vehicular environments. Longer bidirectional connections between road side access routers and vehicles can be established through multi-hop paths. The bi-directionality of links is a strong requirement of most IP applications, and it is difficult to be achieved when asymmetric links appear in the vehicular wireless network.

The deployment of seamless infotainment traffic faces unique challenges due to the characteristics of the highly-mobile and multi-hop Vehicular Communication Network. The standards for communications in vehicular environments suffer from limitations for the deployment of IP traffic, but also the IP mobility support in VCN has traditionally focused on vehicles using one-hop connections to the infrastructure.

To enable access to innovative services designed for vehicular environments, the infotainment applications are likely to incentive a faster adoption of the equipment and the supporting infrastructure required for vehicular communications. In fact, it has been widely accepted that this supporting infrastructure and communications technologies will be heterogeneous in nature. Large coverage access networks, such as 3G/4G cellular and WiMAX networks will be combined with wireless local area networks (WLAN), such as 802.11b/g/n.

A higher response from the IP mobility mechanism is achievable if more information from the applications side can be properly used. In fact, an adaptive mobility management scheme could be developed in which, by properly specifying the type of application, the mobility protocol determines if the IP addresses employed for the communications should be or not transferrable to other access networks. In this way,

Mobility signaling is reduced when the granularity of the IP prefix assignment allows for an also granular IP mobility provision. Consequently, as opposed to by default employing one single prefix or all communications, and generating oftentimes needless signaling for IP mobility, the mobility scheme will address only prefixes of applications for which mobility is a requisite.

II. Literature Survey

Current authentication schemes employed in multi-hop networks have two different approaches: 1) To use an RN to only forward the authentication credentials between MN and the infrastructure; and 2) To apply hop-by-hop authentication.

For the first case, in [6], the MN uses its public key certificate to authenticate itself to the foreign gateway. On the other hand, the scheme in [7] uses both a symmetric key for authenticating an N to its home network, and public key schemes for mutual authentication between home network and foreign network. However, the expensive computation involved with public key operations tends to increases the end-to- end delay.

A symmetric key-based authentication scheme for multi-hop Mobile IP is proposed in [8]. In that work, an MN authenticates itself to its home authentication server (HAAA), which derives a group of keys to be

used by the MN. Despite its low computation and communication overheads The symmetric key-based schemes cannot achieve strong levels of authentication.

For the second case, a mutual authentication scheme is proposed in [9], which depends on both secret splitting and self-certified schemes. However, they both are prone to DoS attack. Another scheme for hop-by-hop authentication called Alpha is presented in [10]. Alpha proposes that the MN signs its 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 it protects the network from insider attacks, Alpha suffers from a high end-to-end delay.

A hybrid approach, the adaptive message authentication scheme (AMA), is proposed in [11]. It adapts the strength of the security checks depending on the security conditions of the network at the moment of packet forwarding. Multi-hop 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 MN to have a direct connection to the MAG for two reasons. Firstly, the MAG is expected to detect new connections and disconnections based on one-hop communications. Secondly, the network-based mobility service should be offered only after authenticating and authorizing the mobile node for that service; however, those tasks are assumed to happen over the MAG {MN link, but not in the presence of intermediate routers. Therefore, it is still necessary to devise a solution in which the multi-hop links in the VCN are considered.

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

III. Methodology

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

A) Basic Operation:

The signaling of MA-PMIP for initial IP configuration follows the one defined by the standard PMIP. Once the vehicle joins the domain for the first time, it sends Router Solicitation (RS) messages, which are employed by the MAG as a hint for detecting the new connection. Once the PMIP signaling has been completed, the MAG announces the IP prefix in a uni-cast RA message delivered to the vehicle over the one-hop connection. In order to enable communications from the in-vehicle local network, the MR may obtain additional prefixes by means of prefix delegation or prefix division, as it is currently proposed at the IETF for network mobility support with PMIP.

Fig-1 shows Basic MA-PMIP signaling employed when a vehicle experiences a handover through a relay. The movement detection could be triggered by any of the following events:

1) The vehicle has started receiving AR geo-cast messages with a geo identifier different from the one registered in the default gateway table;

2) The vehicle has detected its current location falls outside the service area of the registered AR. If the vehicle losses one-hop connection toward the MAG, but it is still inside the registered service area, then no IP mobility signaling is required and packets are forwarded by means of the geo-routing protocol.

After movement detection, the RS message is an indicator for others (i.e., relay vehicle and MAG) of the vehicle's intention to re-establish a connection in the PMIP domain. Thus, an authentication is required to ensure that both nodes source and relay are legitimate and are not performing any of the attacks. Once the nodes are authenticated, the RS packet is forwarded until it reaches the MAG, and the PMIP signaling is completed in order to maintain the IP assignment at the vehicle's new location.

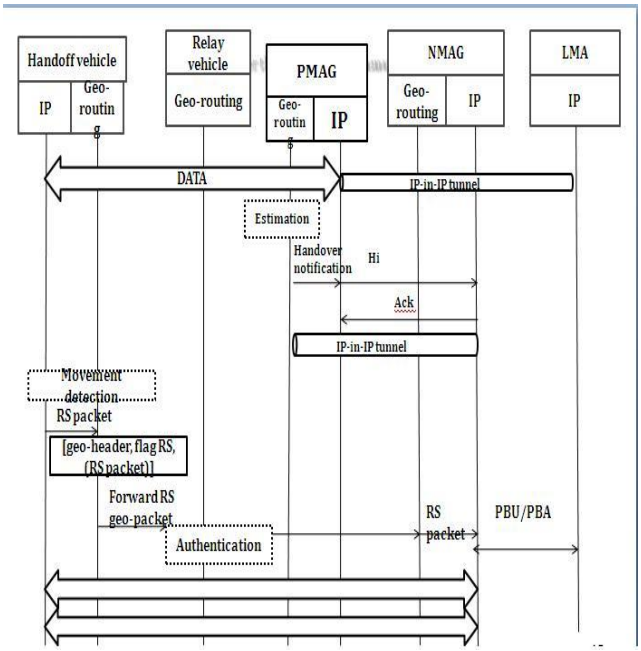

Fig 1 Methodology for fast handover

B) Authentication

- 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 MN requires (n log n) bits to store this list. We argue that such storage space can be adequately found in mobile networks, such as vehicular networks. The LMA is also authorized to replace the identity of any MAG with another unique identity (this is especially useful for the management of MN's revocation, as it will be illustrated in section IV-D). 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 in its domain. After collecting the network polynomials, fi(w; x; y; z), from all MAGs, the LMA computes the domain polynomial, F(w; x; y; z).

The LMA randomly chooses and sums l network-polynomials from the received n polynomials in order 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 * 2n-secrecy, and decreasing the revocation overhead at the time of MN's revocation. After constructing the domain polynomial F(w; x; y; z), the LMA evaluates it for each MAG's identity, IDMAG, individually. The LMA then securely sends to each MAG its corresponding evaluated polynomial. Later on, those evaluated polynomials, are used to generate shared secret keys among arbitrary nodes in the domain

- **MN Registration Phase**

When an MN firstly 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 RSA. After guaranteeing the MN's credentials, the MAG securely replies by evaluating its domain polynomial, F(IDMAG; x; y; z), using the MN's identity, to obtain F(IDMAG; IDMN; y; z). Afterwards, the LMA also sends the list of current MAGs's identities to the MN. The MN stores this list along with the identity of its first-attached MAG (IDFMAG). As a result, a mobile node a can establish a shared secret key with another mobile node b in the same PMIP domain, by evaluating its received polynomial F(IDFMAG-a; IDa; y; z) to obtain F(IDFMAG-a; IDa; IDFMAG-b; IDb). Similarly, b evaluates its received polynomial, F (IDFMAG-b; IDb; y; z), to obtain F (IDFMAG-b; IDb; IDFMAG-a; IDa). Since the domain polynomial F is a symmetric polynomial, the two evaluated polynomials result in the same value and they represent the shared secret key between mobile nodes a and b, K||b.

- **Authentication Phase**

When an MN roams to a relayed connection, the neighbor discovery messages for movement detection in the multi-hop enabled PMIP scheme will go through an RN. The goal of the authentication phase is to support mutual authentication between the roaming MN and the RN. After a successful authentication phase, the RN ensures that the MN is a legitimate user, and the MN ensures that the RN is a legitimate relay.

1) The MN broadcasts a Router Solicitation (RS) that includes its identity, IDMN and its first attached MAG's identity, IDFMAG-MN.
2) Upon receiving the RS, the RN checks its stored list of MAGs to see if IDFMAG-MN is currently a valid identity. If there is no identity equals to IDFMAG-MN, the RN rejects the MN and assumes it is a revocated or malicious node. Otherwise, if IDFMAG-MN is a valid identity, the RN generates the shared key KMN-RN as described in the registration phase. The RN then constructs a challenge message, which includes its own identity, IDRN, the MN's identity, a random number NonceRN, and a time stamp tRN. This information is encrypted in the challenge message using the shared key, KMN-RN, and it is sent by the RN, along with IDRN and its first attached MAG's identity, IDFMAG-RN, to the MN.
3) After receiving the challenge message, the MN checks if IDFMAG-RN is a valid identity using its stored MAGs' identities list. The MN then reconstructs the shared key, by using the RN's identity and IDFMAG-RN, and decrypts the received challenge message. The MN accepts the RN as a legitimate relay if the RN's decrypted identity is the same as the identity received with the challenge message, i.e., IDRN.
4) The MN constructs a reply message, which includes RN's identity, NonceRN, tRN, a new random number NonceMN, and a time stamp tMN. The MN then encrypts the reply message using the shared key, and sends it to the RN, which accepts the MN as legitimate user if the decrypted NonceRN equals to the original random number that the RN sent in the challenge message.

- **Mobile Node Revocation**

When an MN is revocated, the LMA replaces this MN's first-attached MAG's identity, IDFMAG-MN, with another unique identity, IDNFMAG, and sends the new one to all legitimate nodes in the domain. Subsequently, each legitimate node updates its stored list of MAGs. The LMA also sends a message to each MAG in the domain, which includes a list of the mobile nodes that have IDNFMAG as their first attached MAG's identity, along with an evaluated polynomial, F (IDNFMAG; x; y; z) that uses the FMAG's new identity. Afterwards, the MAGs send the evaluated polynomial for those MNs that are in the received list and under MAGs' coverage areas. Eventually, each mobile node, in the MNs list, receives a new evaluated polynomial, F (IDNMAG; IDMN; y; z), for both its identity and the new first-attached MAG's identity. Therefore, instead of changing the entire domain keys, only the MNs that share the same IDFMAG-MN need to change their evaluated polynomials and keys.

IV. System Overview/ Architecture

The signaling of MA-PMIP for initial IP configuration follows the one defined by the standard PMIP. Once the vehicle joins the domain for the first time, it sends Router Solicitation (RS) messages, which are employed by the MAG as a hint for detecting the new connection. Once the PMIP signaling has been completed, the MAG announces the IP prefix in a uni-cast RA message delivered to the vehicle over the one-hop connection. In order to enable communications from the in-vehicle local network, the MR may obtain additional prefixes by means of prefix delegation or prefix division, as it is currently proposed at the IETF for network mobility support with PMIP.
The movement detection could be triggered by any of the following events:
1) The vehicle has started receiving AR geo-cast messages with a geo identifier different from the one registered in the default gateway table;
2) The vehicle has detected its current location falls outside the service area of the registered AR. If the vehicle losses one-hop connection toward the MAG, but it is still inside the registered service area, then no IP mobility signaling is required and packets are forwarded by means of the geo-routing protocol.
After movement detection, the RS message is an indicator for others (i.e., relay vehicle and MAG) of the vehicle's intention to re-establish a connection in the PMIP domain. Thus, an authentication is required to ensure that both nodes source and relay are legitimate and are not performing any of the attacks. Once the nodes are authenticated, the RS packet is forwarded until it reaches the MAG, and the PMIP signaling is completed in order to maintain the IP assignment at the vehicle's new location.

V. Mathematical Model

A) Key Establishment Phase
Each MAG in the domain generates a four-variables symmetric polynomial f (w, x, y, z), network

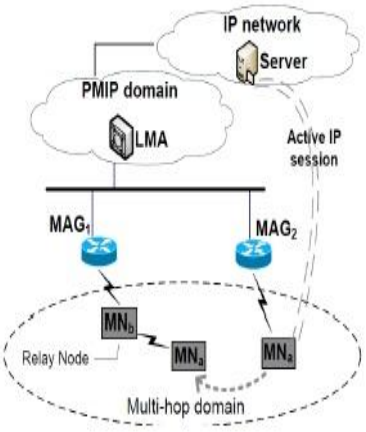

Fig 2 Infrastructure-connected multi-hop mobile network

Polynomial, and then sends this polynomial to the LMA .Domain Polynomial:
F (w, x, y, z) = Xi=1
fi(w, x, y, z), $2 \leq l \leq n$
The LMA evaluates F (w, x, y, z) for each MAGs identity, IDMAG, and then securely sends each individual MAG its own evaluated polynomial
F (IDMAGi, x, y, z), i = 1, 2, ..., n

B) MN Registration Phase
MN authenticates itself to the MAG to which it is directly connected.

MAG → MN:
F (IDMAG, IDMN, y, z)
LMA → MN: The list of current MAGs identities
MNa ↔ MNb:
F (IDFMAGa, IDa, IDFMAGb, IDb) = F(IDFMAGb, IDb, IDFMAGa, IDa)

C) Authentication Phase

When an MN roams to a relayed connection, the neighbor discovery messages for movement detection in the multi-hop enabled PMIP scheme will go through an RN. The goal of the authentication phase is to support mutual authentication between the roaming MN and the RN.

D) Mobile Node Revocation

LMA replaces IDFMAG−MN, with another unique identity, IDNFMAG, and sends the new identity to all legitimate nodes in the domain. Each legitimate node updates its stored MAGs list by replacing the old identity with the new one.

LMA → MNj
F (IDNMAG, IDMNj , y, z)

Only MNs that share the same IDFMAG−MN need to change their evaluated polynomials and keys proposed system consists of three main phases: key establishment phase for establishing and distributing keys, mobile node registration phase for MN's first attachment to the PMIP domain, and authentication phase for mutually authenticating the MN and RN.

VI. Conclusion

We evaluate an authentication scheme, has been proposed to be employed between a mobile node and a relay node in a multi-hop-enabled PMIP domain. Performance of Proxy Mobile IP (PMIP) over multi-hop asymmetric VCN such an enhanced version integrates a predictive handover mechanism, and considers the security issues of employing I2V2V communications. The proposed authentication scheme has the smallest computation overhead among other schemes, because EM3A requires only two symmetric-key encryption operations.

References

[1]. A. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6," IETF RFC 5213, August 2008.

[2]. M. Asefi, S. Cespedes, X. Shen, and J. W. Mark, "A Seamless Quality-Driven Multi-Hop Data Delivery Scheme for Video Streaming in Urban VANET Scenarios," in Proc. of IEEE ICC 2011, pp. 1–5.

[3]. C. Tang and D. Wu, "An Efficient Mobile Authentication Scheme for Wireless Networks," IEEE Trans. Wireless Commun., vol. 7, no. 4, pp.

[4]. A. Al Shidhani and V. C. M. Leung, "Secure and Efficient Multi-Hop Mobile IP Registration Scheme for MANET-Internet Integrated Architecture," in Proc. of IEEE WCNC 2010, pp. 1 –6.

[5]. 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, 2006.

[6]. S. Pack, X. Shen, J. Mark, and J. Pan, "Mobility management in mobilehotspots with heterogeneous multihop wireless links," Communications Magazine, IEEE, vol. 45, no. 9, pp. 106 –112, september 2007.

[7]. N. Moore, "Optimistic Duplicate Address Detection (DAD) for IPv6," IETF RFC 4429, Apr. 2006..

[8]. N. Banerjee, W. Wu, and S. K. Das, "Mobility Support in Wireless Internet," IEEE Wireless Commun., vol. 10, no. 5, Oct. 2003, pp. 54–61.

[9]. Koodli, R. and Perkins, C. E., "Fast handovers and context transfers in mobile networks," ACM Mobile Computing and Commun. Rev., vol. 31, no. 5, Oct. 2001.

[10]. Magagula, L. and Anthony, H., "Early Discovery and Pre- authentication in Proxy MIPv6 for Reducing Handover Delay", Third International Conference on Broadband Communications, Information Technology & Biomedical Applications, pp. 23-26 Nov. 2008.

[11]. Managua, L. and Anthony, H., "IEEE802.21 optimized handover delay for Proxy Mobile IPv6", 10th International Conference on Advanced Communication Technology, pp. 1051-1054, Feb 2008

[12]. Kim, S., Lee, J., and Chung, T., "Performance Analysis of Fast Handover schemes for Proxy Mobile IPv6", The Fourth International Conference on Systems and Networks Communications, pp. 37-48, Sept 2009.