International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 31951-31958
© Research India Publications
http://www.ripublication.com

Meshing VANEMO Protocol into VANETs

[1]M. Dileep Kumar, [2]M. Trinath Basu,[3]T. Gunasekhar

[1]Senior Software Engineer, Tech Mahindra, Hyderabad
[2]Assistant Professor, Dept. of CSE, K L University
[3]Research Scholar, Dept. of CSE, K L University

Abstract

The mobile IP solution is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address. So we propose VANEMO Protocol. Where each mobile node is identified by its home address regardless of its current location in the Internet. While being at remote locations, a mobile node is associated with a Care-Of-Address (COA), which gives information about its current location. Using mobile IP, mobile devices will communicate without interruption while roaming, and this allows mobile nodes to connect seamlessly to the Internet.

Keywords: VANETs, COA, Unauthorized insider, Vulnerability, NEMO

I. INTRODUCTION

While safety applications are the main focus of DSRC technology. Mobile infotainment applications are excepted to provide comfort and convenience during driving. Among these infotainment applications, many require the mobile IP solution and Network Mobility (NEMO) protocols. Each mobile node has two addresses: a permanent home address, which is used when the mobile is on its home network and CoA, which is used in foreign networks. On the home network, a Home Agent (HA) stores information about mobile nodes whose permanent home address is in the home agent's network. In foreign networks, a foreign agent stores information about mobile nodes visiting its network. The mobile nodes home agent recognizes the node's movement and maintains the COA of the mobile node in its foreign network. Another node intending to communicate with the mobile node uses its permanent home address as the destination address for sent packets. Once the home agent receives data packets for the mobile node, it redirects these packets toward the foreign agent using the home agent's lookup table. This is done by tunneling the packets to the mobile node's CoA. The packets are decapsulated at the end of the tunnel and are delivered to the mobile node. When acting as sender, the mobile node simply sends packets directly to the other communicating node through the foreign agent, without going through the home agent. Built upon the mobile IP concept, NEMO supports mobility for entire mobile networks that move and attach to different points in the Internet.

As with the mobile IP solution, NEMO shields the nodes in the mobile network from the movements, and this enables compatibility with devices that and not provided with any mobility support. Moreover, the NEMO technology aggregates the handover signaling procedures for all nodes, resulting in reduced administration overhead. Though mobile IP and NEMO have been extensively studied in generic wireless networks, the study of mobile IP solutions in VANET scenarios is still an early stage. In a high-level challenging paper, Baldessari et al. combine the idea of VANET and NEMO and propose a deployable system architecture called VANET and NEMO (VANEMO).The VANEMO deployment approach meets the functional and performance requirements better than the pure NEMO driven. Another open question attracting the attention of the research community is the development of reliable and fast IP address acquisition protocols. It has been shown that neither addresses configuration protocols in the internet nor the mobile IP solution for MANET's can be directly applied to VANET scenarios. For example, Bychkovsky et al. (2006) revealed that in city driving environments, after a vehicle associates with an Access Point (AP) and acquires an IP address, common connection times range from 5 to 24 seconds. However, the Wi-Fi Dynamic Host Configuration Protocol (DHCP) often requires 2 to 5 seconds once association is complete. In other words, DHCP can consume up to 100% of a vehicle's available connection time. Fazio et al. propose to exploit the predictable topology of VANETs and use dynamically elected leader vehicles to run distributed DHCP protocols. This way, these leader vehicles can provide unique IP addresses to moving vehicles and reduce the frequency of IP address reconfiguration. It is shown that this proposed scheme only requires a reasonably low configuration time to acquire an IP address. Arnold et al. (2008) propose an alternative solution to allow precedent vehicles to pass their own IP addresses to the following vehicles in the same geographic region. As an example, as node A leaves an AP's coverage area, node B, which is behind node A, will reuse node A's IP address to access the Internet via the same AP. It is shown that the proposed protocol will significantly improve efficiency, reduce latency, and increase vehicle connectivity.

II.MOBILE IP

The Mobile IP protocol allows location-independent routing of IP datagram's on the Internet. Each mobile node is identified by its home address disregarding its current location in the Internet. While away from its home network, a mobile node is associated with a *care-of* address which identifies its current location and its home address is associated with the local endpoint of a tunnel to its *home agent*. Mobile IP specifies how a mobile node registers with its home agent and how the home agent routes datagram's to the mobile node through the tunnel.

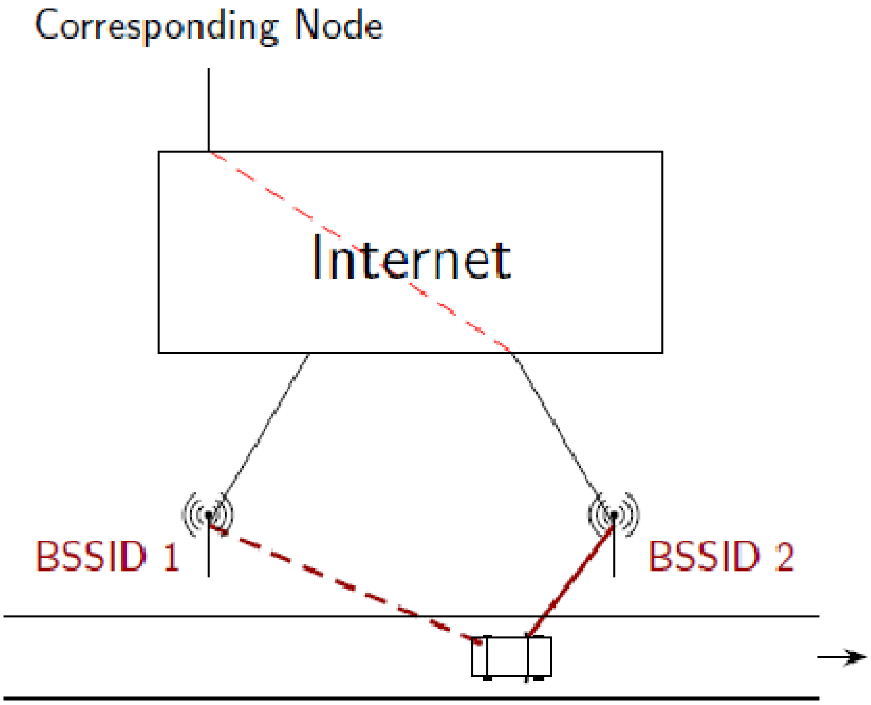

Fig 1: Without Mobile IP: Change of IP address implies disconnection with Corresponding Node

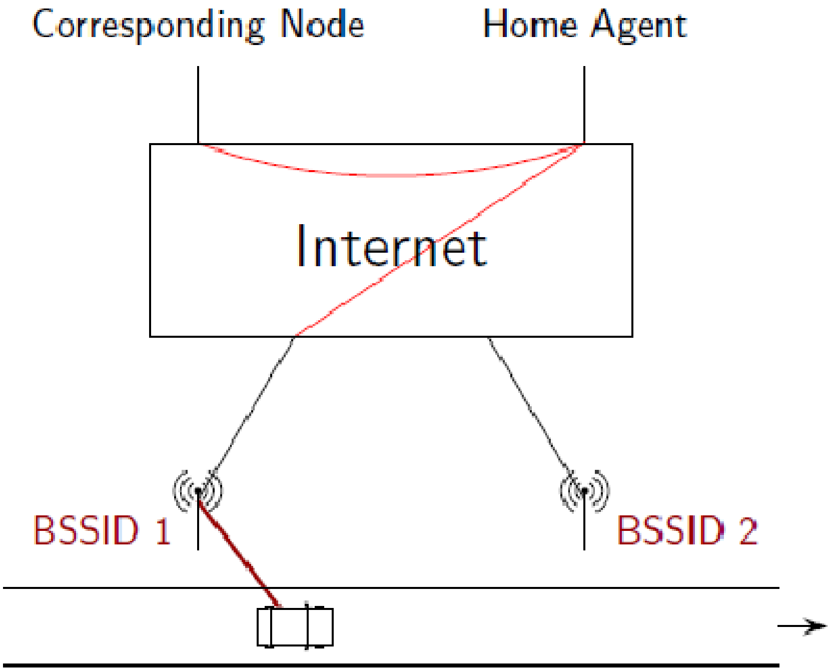

Fig 2: With Mobile IP

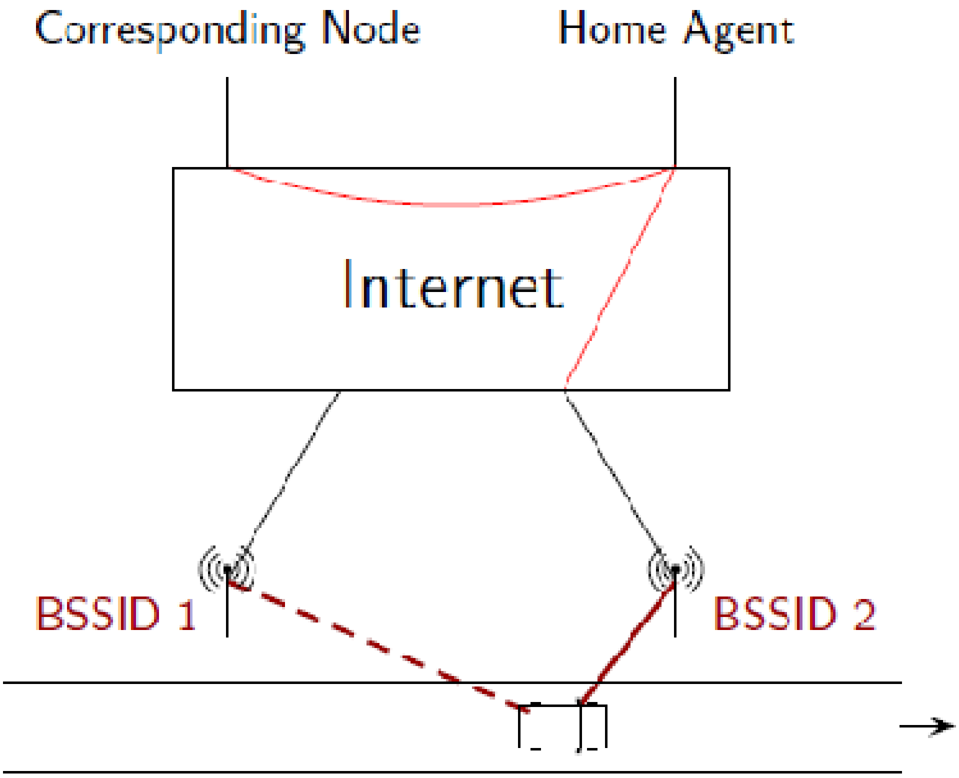

Fig 3: With Mobile IP: Change of IP address OK, seamless for Corresponding Node.

III. Scenarios and Characteristics of Network Mobility

A mobile network consists of one or more mobile IP-subsets formed by one or more mobile routers (MR). This MR, which can change its point of attachment, provides Internet connectivity to mobile network nodes (MNNs) within the network. IETF defines three types of MNNs, i.e., local fixed node (LFN), local mobile node (LMN), and visiting mobile node (VMN). LFN is a fixed node belonging to mobile network without mobility support. LMN and VMN are MNNs with mobility support. The home link of LMN belongs to the mobile network while that of VMN does not. An MNN can be either a host or a router and either fixed or mobile. A mobile network is called nested if there is another attached mobile network inside. The nested mobility is unique for network mobility. For network mobility, there is no size limitation for mobile networks. The simplest network may only consist of a mobile router and MNNs. A mobile network can also consist of hundreds of mobile routers and several nested mobile networks.

(i) Group of nodes move as a unit: From Internet perspective, the entire mobile network changes its reach ability in relation to the fixed Internet topology as a group or unit.

(ii) Various sizes and moving speeds: Mobile networks have various sizes and moving speeds. For example, pedestrian with PAN may walk at speed of 5km/h while access networks accommodating hundreds of devices in a train may move at speed of 100km/h.

(iii) Various mobile network nodes: Mobile network nodes have various types, i.e., mobile host and mobile router, local nodes and visiting nodes, mobility aware nodes (e.g. MIPv6- enabled nodes) and mobility unaware nodes (e.g., standard IPv6 nodes).

(vi) Arbitrary nested level: The mobile network can be nested with arbitrary number of levels.

(v) Mobility transparency to mobile network nodes: In most cases, the internal topology of mobile network is relatively stable. For example, a laptop attached to a mobile router in a moving bus will not change its point of attachment frequently. Therefore, the link layer connection of the laptop and the mobile router can be maintained even when the mobile router changes its point of attachment to the Internet. The mobile network nodes do not need to be aware of location change with respect to the Internet. Advantages and Requirements of Network Mobility with NEMO, once attached to a mobile network, the mobility management for the MNNs is fully performed by the mobile router. In particular, the mobility management is transparent to the mobile network nodes.

The advantages can be summarized as follows:

(i) Scalability: A mobile network may consist of hundreds of MNNs. Without a network mobility solution, these MNNs have to handle mobility independently. For one node, several signaling messages need to be exchanged with the point of attachment. On the other hand, using basic network mobility solutions, mobility is handled only by the mobile router and hence the signaling overhead can be reduced significantly.

(ii) Reduced handoff: Due to the relatively stable internal topology of mobile network (e.g., topology among mobile router and MNNs), mobile network nodes do not change their points of attachment and hence can avoid link layer

(iii) Reduced complexity: Mobile network can provide mobility support to standard IPv6. The IP addresses of MNNs will not change even if the mobile router changes its point of attachment. Therefore, the complexity of software and hardware used in MNNs can be reduced.

The requirements of NEMO solution can be summarized as follows:

(i) Global reach ability and session continuity of MNN: This is the fundamental requirement for network mobility. Mobile network nodes must be globally reachable given a permanent IP address. During the movement of mobile router, ongoing sessions of MNNs must be maintained.

(ii) Minimum changes: For basic network mobility support, no modifications should be required to any entities other than mobile router and its home agent.

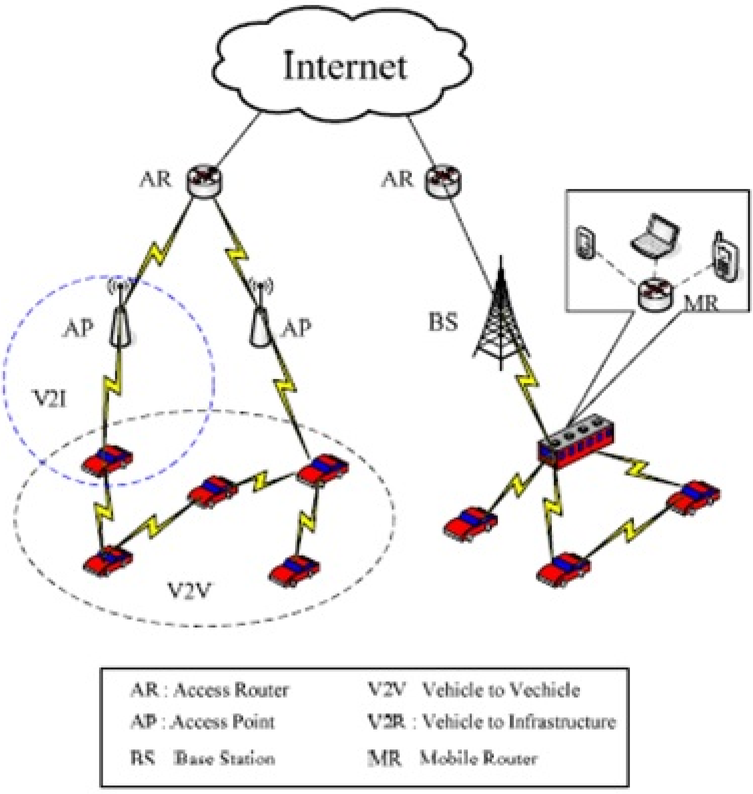

Fig 3: General model of vehicular Networks

(iii) Support for different nodes: Basic network mobility solutions must support all types of mobile network nodes mentioned above.

(vi) Compatibility: The solutions must be compatible with existing Internet standards. For example, it should not affect the operation of MIPv6 or standard IP addressing and routing schemes.

(v) Nested mobility support: The solutions should support mobile network nodes which are located in nested mobile networks at different levels.

(vi) Internal configuration transparency: The internal configurations (e.g., topology) should be transparent to the solutions. In other words, the solutions can be applied to mobile networks with arbitrary internal topologies.

(vii) Scalability: To support large mobile networks, the solution needs to be scalable.

(viii) Security: The solutions must have sufficient protection from the attack. Network Mobility Solutions

Similar to host mobility, solutions for network mobility can be designed and implemented in different layers. In the following, we mainly focus on network layer and application layer solutions.

Network layer solutions: Network Mobility Basic Support (NEMO BS) protocol was proposed by IETF to provide basic network mobility support. To minimize the change to existing architecture and to maintain backward compatibility, NEMO BS was designed based on MIPv6 with minimal extensions. Similar to mobile host in MIPv6, mobile router has home address and home agent (i.e., HA-MR). NEMO BS specifies operation of mobile router and home agent, while the details of mobile network nodes are the same as that in MIPv6. In NEMO BS, when a visiting MNN connects to the mobile network using with MIPv6, the MNN will receive a subnet prefix (i.e., network prefix (MNP)) advertised by the mobile router. Then, the MNN establishes new care-of-address (CoA) based on MNP.

Once the address configuration is done, the MNN sends a binding update (BU) message to its home agent. The home agent sends binding acknowledge back to finish the location update procedure.

When the mobile router changes its point of attachment, it also acquires a CoA from the visiting network and updates the binding cache of its home agent. Since the CoAs of MNNs remain unchanged, location update messages do not need to be sent to the home agent of the MNNs. Once the binding procedure is completed, a bi-directional tunnel between mobile router and home agent is established based on IP-in-IP encapsulation [3]. However, route optimization is not considered in NEMO BS due to the security and incompatibility issues. All packets to and from mobile network nodes need to be tunneled by the home agent of the mobile router. Packets from the MNNs to the correspondent nodes (CNs) are encapsulated by mobile router and then tunneled to home agent of mobile router. Then the home agent decapsulates these packets and forwards them to the destinations. In the opposite direction, packets from CNs to MNNs will be first received by the home agent of the mobile router. The home agent tunnels these packets to mobile router which then forward them to mobile network nodes. However, the binding cache of home agent only contains home address of mobile router. The addresses of mobile network nodes are not bound with current CoA of mobile router. As a result, packets cannot be tunneled to the mobile router correctly.

To solve this problem, prefix scope binding update (PSBU) [51] was proposed. Using PSBU, the mobile router sends binding update message to home agent associating with mobile network prefix rather than the home address with current CoA. Having the prefix information, the home agent can tunnel packets to the correct mobile router.

IV. CONCLUSION

We have proposed a new protocol known as VANAMO. This is obtained by combining the Mobile IP and Network Mobility. We have classified the mobility management solutions for vehicular networks based on vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communications. The traditional Internet and mobile ad hoc network mobility management techniques and their suitability to vehicular networks have been discussed.

V. REFERENCES

1. Hartenstein H, Laberteaux KP. A tutorial survey on vehicular ad hoc networks. IEEE Communications Magazine 2008; 46(6):164–171.
2. Manifesto for the car-to-car communication consortium, Sept 2007.
3. Devarapalli V, Wakikawa R, Petrescu A, Thubert P. Network Mobility (NEMO) Basic Support Protocol. RFC 3963, Jan 2005.
4. Xie J, Wang XD. A survey of mobility management in hybrid wireless mesh networks. IEEE Network 2008; 22(6):34–40.
5. Manner J, Kojo M. Mobility Related Terminology. RFC 3753, June 2004.
6. Ernst T, Lach HY. Network Mobility Support Terminology. RFC 4885, July 2007.
7. Baldessari R, Festag A, Abeille J. Nemo meets vanet: A deployability analysis of network mobility in vehicular communication. In Proceedings of ITST, 2007; 1–6.
8. Perkins CE, Malinen JT, Wakikawa R, Nilsson A, Tuominen A. Internet connectivity for mobile ad hoc networks. Wireless Communications and Mobile Computing 2002; 2(5):465–482.
9. Gustafsson E, Jonsson A. Always best connected. IEEE Wireless Communications Magazine 2003; 10(1):49–55.
10. Bechler M, Wolf L. Mobility management for vehicular ad hoc networks. In Proceedings of VTC 2005-Spring, vol. 4, 2005; 2294–2298.