Design and Implementation of Efficient Authentication Agent to Reduce Number of Hops in VANETs

Ramling Halmandge[1] Jeevan J[2] Pushpalatha S[3] Satish B Basapur[4]
[1,2]M.tech Student [3,4]Assistance Professor
[1,2,3,4]Department of ISE
[1,2,3,4]Dr. AIT Bengaluru

Abstract— Vehicular ad hoc network (VANET) is a network built among vehicles. Vehicular ad hoc network is attaining importance as it enhances the safety of passenger and also provides extra services which are useful to user. The key factor for success of VANETs lies in its mobility. VANETs are utilized by many users hence there is a need to provide authentication and authorization. PMIPv6 provides efficiently authentication and authorization. But it suffers from man in middle attack. It also impedes localized advantage due to long distance delivery. Billing is also a important issue in VANET which has been not focused in past. VANET is a network made up of different users hence it is difficult to motivate users to cooperate for data transmission. This project provides authentication in faster manner by making use of mutual authentication. It provides effective billing scheme. It motivates each vehicle in VANET to participate in transmitting data by providing incentive to them. It prevents the man in middle attack with the help of encryption. It uses a Proxy server which reduces the number of hops required to transmit the data.

Key words: VANET, Hops, PMIPv6

I. INTRODUCTION

VANET stands for vehicular ad hoc network and VANETs have been evolved for providing passenger safety and to provide more comfort level. If the nodes of a network are mobile in nature then that ad hoc network is called as Mobile Ad hoc Network (MANETs). If the nodes of MANETs are vehicles then that is called as Vehicular Ad hoc Networks (VANETs). So the VANET is the subset of MANETs. Vehicles consist of onboard unit residing with them to do network related services. The continuity of communication between the nodes (vehicles) is very challenging task since the vehicles have been provided with high speed mobility feature. Various protocols like Hierarchical mobile IPV6, Network mobility, mobile IP and Proxy mobile IPv6 (PMIPv6) proposed by Internet Engineering Task Force (IETF) for providing vehicular mobility support. Two types of available IP mobility mechanisms are Host based solution and Network based solution. The host based solution uses both mobile terminal (MT) as well as networks. For VANETs network based solution is the best suited approach. The IETF proposed PMIPv6 for providing the mobility support in which mobility management is taken care by networks but not by nodes, so that vehicles can freely travel. In the network based solution, the network takes charge of certain domain or region up to which it can contact with mobile terminals.

There are two types of communication in VANET:

(1) Vehicle to Vehicle communication (V2V)
(2) Vehicle to Infrastructure communication (V2I)

In vehicle to vehicle communication two nodes can communicate with each other without any aid of network but in vehicle to infrastructure communication two nodes uses network aid for communication. In order to achieve these communications Federal Communication Commission (FCC) has provided a bandwidth of 75MHz around 5.9Ghz band. This communication range is also known as Dedicated Short Range Communication (DSRC).

The vehicular networks are not only used for passenger safety but they are also provide the application like automated road traffic alerts, file like audio and video can be shared between moving vehicles and also dynamic packet routing can be achieved.

The traditional VANETs consist of mobile terminals (Vehicles) which are monitored by road side sensors so called Road side units. These road side units are placed along the roads and monitored by centralized Authentication/Authorization/Accounting (AAA) server which is located so far from the road side units. Communication between AAA server and road side unit happens over the internet. Every time when a vehicle comes under the communication range of road side unit then road side unit has to communicate with AAA server. In order to avoid this long distance communication, a intermediate server so called Proxy server is introduced between AAA and road side units.

Billing is important issue in the VANETs which is rarely considered in earlier approaches. In the VANETs not only providing security and fast delivery of data are important but cost or billing is also an important factor. In this approach the numbers of hops are less and hence the cost required to transverse the data is also less.

II. RELATED WORK

IP [1]mobility has been very emerging topic in past few years. The role of IP has been used in 3G network. Many popular organizations like IEEE and IETF are working on IP mobility concept. Earlier IP mobility concepts like mobile IPv4 or IPv6 have been used for communication. But these were not used for movement support. Now different approaches are evolving for providing mobility support with the help of network based operation. One of such approach is proxy mobile IPv6. This PMIPv6 provides mobility support where network provides mobility functionality without relying mobility functionality on mobile nodes. Standard organizations have made different extensions and enhancement on Proxy Mobile IPv6. These extensions provide flow mobility, network mobility support and multicasting. Mobility support has gained lot of attention. Previously these IP network were used to provide service like voice support and now the role of IP in 3G network is considered. Traditional IPv4 or IPv6 are terminal based where terminals are responsible for mobility and terminals have to do operation for keeping the ongoing communication alive.

Distributed certificate scheme[2] (DCS) gives flexible interoperability for certificate in non homogeneous administration. An on board unit updates its certificate at available roadside unit or MAG. In DCS, certificate based signature are authenticated by aggregating batch verification. This technique reduces verification overhead. DCS scheme reduces certificate management complexity and provides high security and vehicular communication efficiency.

Vehicular ad hoc networks have gained popularity because of promising transportation system. VANET consist of vehicles on roadside units. V2V and V2I are two types communication modes in VANET. Because of open medium nature of VANET, security requirements such as message integrity, authentication and privacy preservation have been identified. Any misbehavior of user such as sending false information, doing modification and replying with illegitimate messages could be problem to other users. The privacy of the user maintained to avoid tracking user location, inferring sensitive data and disclosing user identification. Hence to fulfill these security requirements, security and privacy protocols have been designed for vehicular networks.

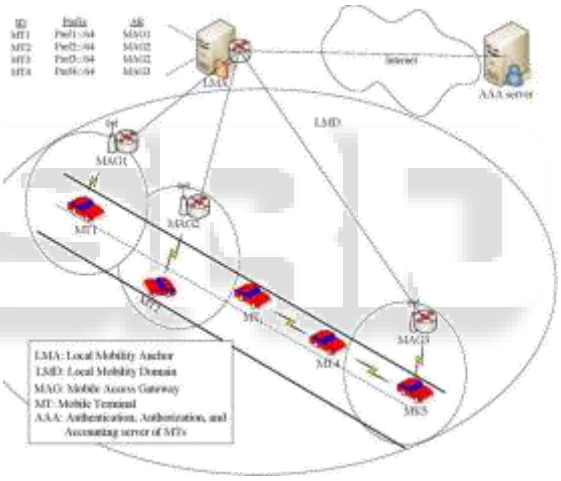
Vehicular networks have[3] been implemented few years before. VANET is a form of mobile ad hoc network. Many security issues encountered during implementation. Earlier, vehicles are considered as realm of mechanical engineer. But with inexpensive electronic components and to increase roadside safety, a differentiation made between manufacturers from their compotators. Vehicles are becoming computer on wheel. A modern car consist of several interconnected processors, a central computer, Event data recorder (EDR), black box and it has a optimal GPS system for navigation. The vehicle manufacturer took a further step by letting the vehicle to communicate with other vehicle. This enhances road safety and awareness of their environment, thereby increasing the passenger safety and traffic optimization. With the proper integration of OBU and other devices such as GPS receiver with communication capabilities, creates commercial opportunities but also faces tremendous research challenges. Security is one of these challenges and less attention has been given to security. But, it is very crucial. For example, it is important to make sure that any illegitimate information cannot be inserted by the jammer. In the same way the system should reduce the burden on the drivers but simultaneously, it has to preserve passenger as well as driver information.

Timed efficient and Secure Vehicular Communication[4] (TSVC) with privacy preservation scheme aimed to provide overhead in terms of signature overhead and data packets with preserving security by attaching a message authentication code (MAC) to packet significantly reduces computation and communication overhead. From various demonstrations it has been proved that TSVC provides very less packet overhead. The TSVC reduces packet loss ratio when compared with that of Public Key Infrastructure (PKI) schemes. With the aid of advance wireless technologies, it has proved that vehicles are able to interact with each other as well as they can communicate with road side units located along the road. Roadside unit and vehicles with on board units will form a self organized network which is called as Vehicular ad hoc network.

As per Dedicated short range communication (DSRC), each vehicle can broadcast traffic related messages along with position information, current time information, navigation information, acceleration/deceleration traffic related event and emergency messages are broadcasted to all vehicles. When emergency situation encounters, an emergency message is broadcasted through multihop. Currently the IEEE 802.11p group is working to support efficient wireless communication between vehicle and RSU. The broadcasted traffic related message helps the driver to get a better awareness of driving environment.

III. PROXY SYSTEM

In the proposed approach a proxy server is placed in between centralized AAA server and roadside unit (RSU). This proxy server is designed to monitor some set of roadside units (RSU). The proxy server has the domain knowledge that is proxy server knows the exact location of the vehicles which all come under its RSU's communication range. When a vehicle wants to communicate with another vehicle then, this proxy server distributes the vehicle information to the all road side units. This approach reduces authentication delay as well as number of hops between source and destination vehicle.



IV. DESIGN

A. Algorithm for Vehicle deployment

Input: Xmin, Xmax, Ymin, Ymax, Nnodes
Output: Vehicle deployment Matrix
Step 1: Start
Step 2: Initialize k=1
Step 3: If k<=Nnodes
Generate X and Y position of Vehicle
Else
Stop
Step 4: Form a triplet of node ID, X_k, Y_k
Step 5: Store at K^{th} row
Step 6: [STOP]

B. Algorithm for Four way lane formation

Step 1: Start
Step 2: Initialize m=1
Step 3: If m <= N_{lanes}
N_{lane} = 4
Lane 1: {0, 100, 0, 100}
Lane 2: {150, 250, 150, 250}

Lane 3: {0, 100,150, 250}
Lane 4: {150, 250, 0, 100}
Else
Stop
Step 4: Generate Lane ID
Step 5: Execute vehicle deployment algorithm
Step 6: Increment m
Step 7: go to Step 3

C. Algorithm for Path Determination using Centralized AAA

Input: Source vehicle ID and Destination vehicle ID.
Output: Path between source and destination vehicle.
Case I:
Step 1: Start
Step 2: If $Node_{source}$ Lane ID =$Node_{Dest}$ Lane ID
$Node_{source}$ communicates $Node_{Dest}$
Else
Node not found
Step 3: Stop

Case II:
Step 1: Start
Step 2: If $Node_{source}$ Lane ID = $Node_{Dest}$ Lane ID
$Node_{source}$ communicates $Node_{Dest}$
Else
Go to next lane
Step 3: Initialize k= source node lane ID
Step 4: Scan all vehicles in lane
Step 5: If Destination vehicle found
Establish path
Else
K=k+1
goto Step 4
Step 6: Stop

D. Algorithm for Proxy server path determination

Input: $Node_{source}$ ID and $Node_{Dest}$ ID.
Output: Path between $Node_{source}$ and $Node_{Dest}$
Step 1: Start
Step 2: If $Node_{source}$ Lane ID = $Node_{Dest}$ Lane ID
$Node_{source}$ communicates $Node_{Dest}$
Else
$Node_{source}$ communicates MAG_{Source}
Step 3: MAG_{Source} communicates MAG_{Dest}
Step 4: MAG_{Dest} communicates $Node_{Dest}$
Step 5: Stop

E. Algorithm for Proxy based encryption

Input: Data
Output: Encrypted data
Step 1: Start
Step 2: Generate public key
Step 3: Generate certificate
Step 4: Generate private key
Step 5: Encrypt data with the help of private key
Step 6: Stop

V. RESULTS

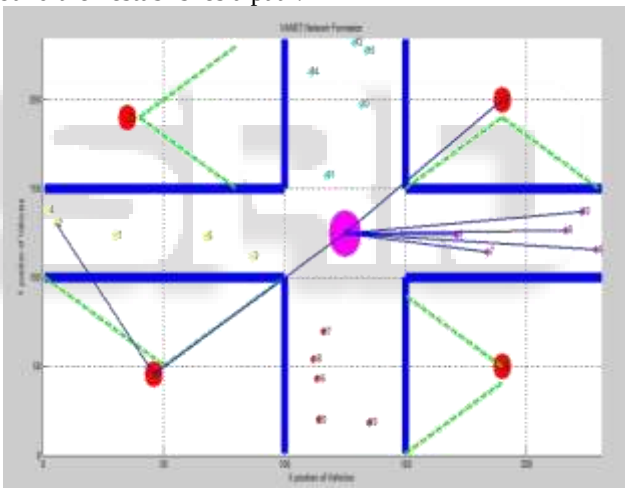
A. Choosing source and destination vehicle

Prior to routing of data, we need to choose source and destination vehicles. In addition to that other parameters are also entered.

```
Enter the Number of Vehicles in the 1Lane = 5
Enter the Number of Vehicles in the 2Lane = 5
Enter the Number of Vehicles in the 3Lane = 5
Enter the Number of Vehicles in the 4Lane = 5
Enter the Source Vehicle Node ID = 4
Enter the Destination Vehicle Node ID = 19
Enter the Energy required for Packet Generation [1-10] mJ =  5
Enter the Energy required for Packet Transmission [11-20] mJ =  12
Enter the Attenuation Factor [0.1 to 1]  =  0.5
Enter the Number of Iterations = 20
```

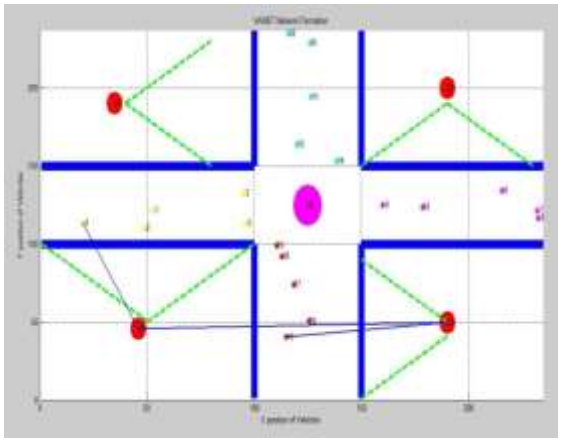
B. Path determination using centralized AAA server

Vehicle 2 is chosen as source vehicle and vehicle 10 is chosen as destination vehicle. Vehicle 2 communicates with MAG 21, MAG 21 communicates with AAA server, AAA server communicates with next MAG which is MAG 22. Then scans all vehicles in that particular lane. If vehicle is found then establishes a path.



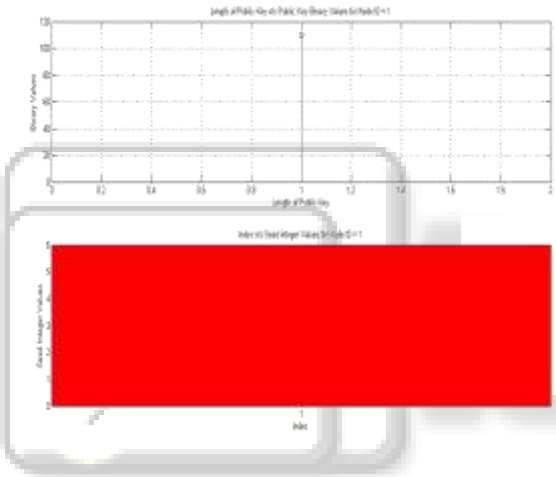
C. Path determination using proxy server

Vehicle 4 is chosen as source vehicle and vehicle 19 is chosen as destination vehicle. Vehicle 4 communicates with MAG 21, MAG 21 communicates with MAG 24 then finally MAG 24 contacts vehicle 19 to set a path. Here the proxy server 25 distributes vehicle information to all MAGs. Here all MAGs know positions and lane ID of every vehicle. Therefore MAG can directly contact to one another in order to do communication.



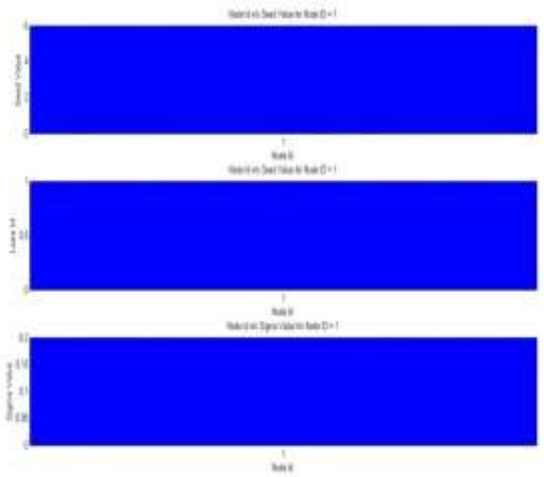
D. Random seed generation

For encryption process keys are necessary. The proxy server generates random seeds and distributes seeds to all vehicles. These vehicles generate a public key on basis of received random seed. Each seed is unique so resulting key will also be unique.



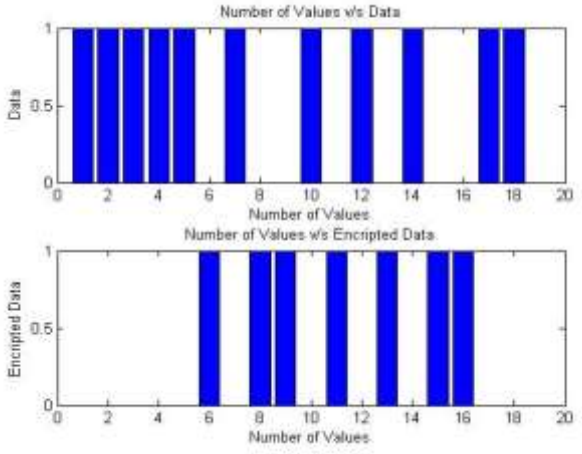
E. Requirements for certificate generation

For certificate generation lane ID and sigma values are very important. Sigma value will be fixed and lane ID will be different for different lanes. For vehicle 1, the seed value is 6, lane ID is 1 and sigma value is 0.2.



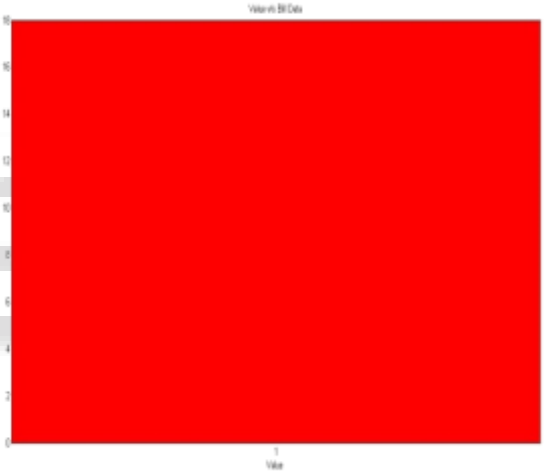
F. Data encryption

Prior to data transmission the data is encrypted at sender side. At the receiver side encrypted data is decrypted to get original data. The original data as well as encrypted data.



G. Billing

In order to use network services the user need to pay the billing value.

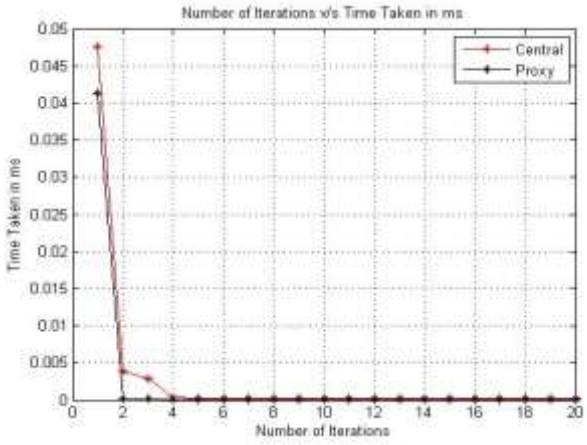


VI. COMPARISON

Proxy server and centralized AAA server are compared with the help of few parameters they are end to end delay, number of hops, energy consumption, routing overhead and complexity.

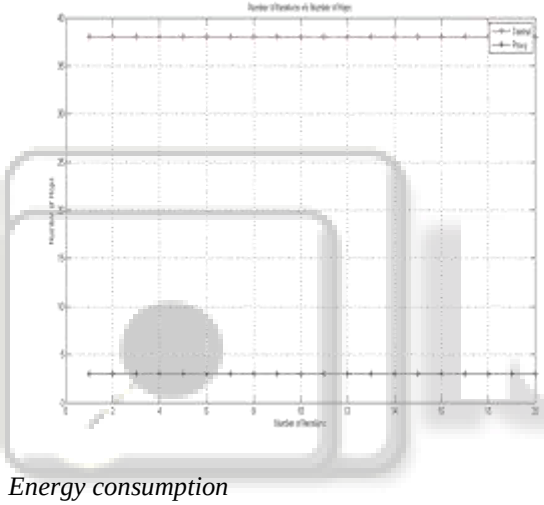
A. End to End Delay

Since the AAA server doesn't have domain information it takes more time to find the destination vehicle so end to end delay of AAA server is more than proxy server.



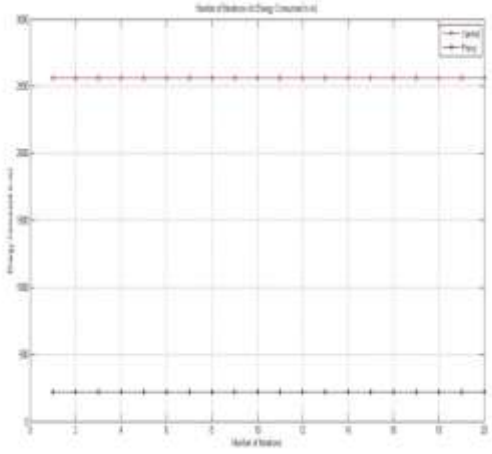
B. *Number of Hops*

Since the AAA server doesn't have domain information it takes more hops to find the destination vehicle so number of hops for AAA server will be more when compared to proxy server.



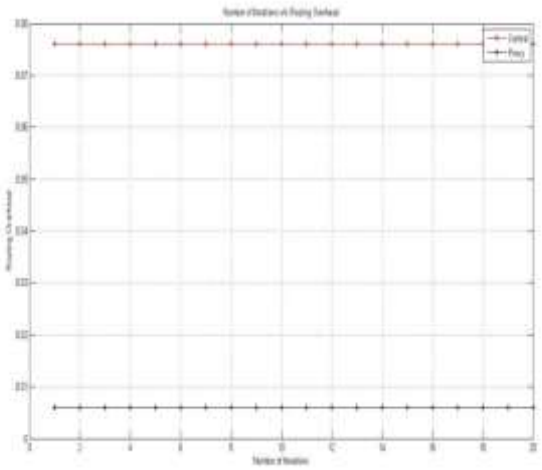
C. *Energy consumption*

The energy required to transmit a packet is significantly more in AAA server.



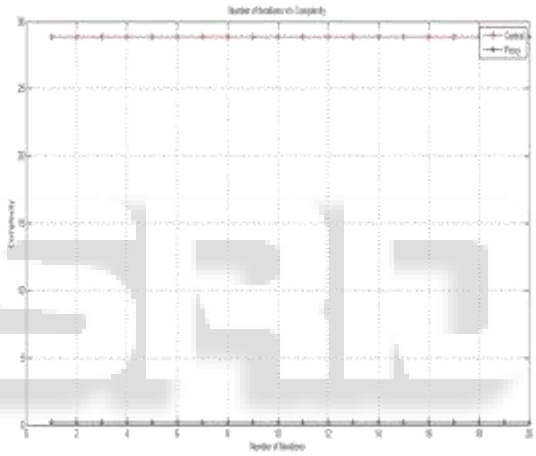
D. *Routing overhead*

The routing overhead is measured in terms of control packets and message packet. The centralized AAA server requires more number of control packets so routing overhead will be more in centralized AAA.



E. *Complexity*

The complexity is measured in terms of routing overhead and number of hops. Routing overhead in proxy server is less so the complexity will also be less in proxy server.



VII. CONCLUSION

The proposed approach reduces number of hops and mitigates total energy consumed while data transmission. Previous approach ignored the delay occurred during transmission of data. The proposed project considers an intermediate server that helped to deliver the packet. This server knows location of vehicles so the packet is directly delivered to intended destination node. This scheme not only preserves the security but also reduces long distance packet overhead between MAG and centralized AAA server. A certificate based encryption mechanism is designed to provide the security for data to be transmitted. The billing scheme also has been proposed. In overall, the proposed system reduces Number of hops, Delay, complexity, Routing Overhead and Energy consumption.

REFERENCES

[1] X. Lin, X. Sun, X.Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: Timed efficient and secure vehicular communications with privacy preserving," IEEE Trans. Wireless Commun., vol. 7, no. 12, pp. 4987–4998, Dec. 2008.

[2] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," IEEE Commun. Mag., vol. 46, no. 4, pp. 88–95, Apr. 2008.
[3] D. Johnson, C. Perkins, and J. Arrkko, "Mobility support in IPv6," Internet Eng. Task Force, Fremont, CA, USA, IETF RFC 3775, Jun. 2004.
[4] H. Soliman, C. Castelluccia, K. El-Malki, and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)," Internet Eng. Task Force, Fremont, CA, USA, IETF RFC 4140, Aug. 2005.
[5] V. Devarapalli, R. Wakikawa, A. Pertrescu, and P. Thubert, "Network Mobility (NEMO) basic support protocol," Internet Eng. Task Force, Fremont, CA, USA, IETF RFC 3963, Jan. 2005.
[6] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy mobile IPv6," Internet Eng. Task Force, Fremont, CA, USA, IETF RFC 5213, Aug. 2008.
[7] I. Soto, C. J. Bernardos,M. Calderon, A. Banchs, and A. Azcorra, "Nemoenabled localized mobility support for internet access in automotive scenarios," IEEE Commun. Mag., vol. 47, no. 5, pp. 152–159, May 2009.
[8] K. Zhu, D. Niyato, P. Wang, E. Hossain, and D. I. Kim, "Mobility and handoffmanagement in vehicular networks: A survey,"Wireless Commun. Mobile Comput., vol. 11, no. 4, pp. 459–476, Apr. 2011.
[9] S. Cespedes, N. Lu, and X. Shen, "Vip-wave: On the feasibility of IP communications in 802.11p vehicular networks," IEEE Trans. Intell. Transp. Syst., vol. 14, no. 1, pp. 82–97, Mar. 2013.
[10] C. Huang, Y. P. Fallah, R. Sengupta, and H. Krishnan, "Inter-vehicle transmission rate control for cooperative active safety system," IEEE Trans. Intell. Transp. Syst., vol. 12, no. 3, pp. 645–658, Sep. 2011.
[11] Y.-C. Chu and N.-F. Huang, "An efficient traffic information forwarding solution for vehicle safety communications on highways," IEEE Trans. Intell. Transp. Syst., vol. 13, no. 2, pp. 631–643, Jun. 2012.
[12] J. Song and S. Han, "One-time key authentication protocol for PMIPv6," in Proc. ICCIT, 2008, pp. 1150–1153.
[13] C. Vogt and J. Kempf, "Security threats to Network-based Localized Mobility Management (NETLMM)," Internet Eng. Task Force, Fremont, CA, USA, IETF RFC 4832, 2007.
[14] L.-Y. Yeh, J.-G. Chang, W.-H. Huang, and Y. L. Tsai, "A localized authentication and billing scheme for proxy mobile IPv6 in vanets," in Proc. IEEE Int. Conf. Commun., 2012, pp. 993–998.
[15] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in Proc. IEEE INFOCOM, 2008, pp. 1903–1911.
[16] Dedicated Short Range Communications (DSRC), O. A. [Online]. Available: http://www.etsi.org/index.php/technologies-clusters/technologies/intelligent-transport/dsrc
[17] S. Kent and R. Atkinson, "Security architecture for the internet protocol," Internet Eng. Task Force, Fremont, CA, USA, RFC 2401, 1998.
[18] D. Hankerson, A. Menezes, and S. Vanstone, Guide to Elliptic Curve Cryptography. Berlin, Germany: Springer-Verlag, 2004.
[19] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in Proc. ASIACRYPT, 2001, pp. 514–532.
[20] M. Scott, "Computing the tate pairing," in Topics in Cryptology. Berlin, Germany: Springer-Verlag, 2005, pp. 293–304.

