BRISK AND SECURE AD-HOC VEHICULAR COMMUNICATION

Miraj Shah[1], Imaad Ukaye[2], Narendra Shekokar[3]

[1, 2]Student, [3]Head of Department, Computer Engg, Dwarkadas J. Sanghvi COE

Abstract

The idea of Car-to-Car communication is a revolutionary phenomenon in the automobile industry. This idea will surely change the future of humanity for good. This technology will surely change the perception of how a traditional automotive was initially thought of by adding endless applications as a boon to mankind. The application of cars communicating with each other is enormous and has already been discussed by many researchers by now. But, the important thing here is how to put it in practice with the increasing demand for cars and making it safe to use it, at least improve the current condition by this new technology and not worsen the situation by digital hacking and other flaws. Since the nature of the Communication System is highly dynamic a strict security mechanism is mandatory for its seamless functioning. We propose to encrypt the communication taking place in C2C communication which is not the same as using the Internet security mechanism due to limitation of its speed and residing hardware servers. Symmetric Cryptography thus fails to incorporate the scope of various security disciplines and hence it is ineffective to use such techniques. Asymmetric Cryptography on the other hand provides an ideal trade-off among various security disciplines and hence it is considered as an alternative approach to accomplish a secure system but it fails when applied in an ad-hoc environment. However, the traditional Public Key Infrastructure (PKI) technique fails in several ways so we propose a modified form of communication and authentication technique along with rapid communication and group messages to fasten the speed of communication.

Keywords: *Protocol, Communication, Security, Privacy*

--***--

1. INTRODUCTION

The concept Car-to-Car(C2C) communication is now an evolving trend as a large portion of research funds has been invested all over the globe. Many major car manufacturers have responded positively and are actively working together in bringing this promising technology to fruition. After the concept of autonomous vehicle, cooperative control of multiple vehicles has receives substantial attention in the industry. The key techniques that are being considered include Vehicle-to-Vehicle (V2V), Car-to- Infrastructure (V2I) and Vehicle-to-C.A (V2CA).With advancements in technology in C2C communication various trending problems can be tackled such as automotive safety, user privacy, authentication and validation of vehicles, report to RSU about malevolent cars, etc. Roadside units (RSUs) can be deployed every few miles along the highway for users to communicate about road-safety and obtain other information. Vehicles can use RSUs to report real-time traffic information and request location- based services such as finding restaurants, gas stations, or available parking space. For the sake of cooperation among multiple vehicles effective communication medium is imperative. Although third-generation (3G) networks or satellite techniques can be used to achieve this goal, RSUs have the advantage of low cost, easy deployment, and high bandwidth. Although the primary purpose of system is to enable communication-based automotive safety applications like collision warning, it also provides for a range of business applications, thereby making this technology more cost effective. A Wireless adhoc network perfectly fulfills all the necessary requirements for such a system but at the same time its adhoc nature makes it highly vulnerable to various networking threats. So, securing communication and minimizing communication boundary must be considered for commercial and military applications. To provide a solution we propose a framework for communication among multiple vehicles. Our elucidation is to put forward a new way to visualize multiple vehicles with secure communication and to provide a distributed method to address the problem cooperatively.

Security mechanism will protect all traffic sent over the C2C communication network. While securing communication has its own advantages along with privacy and other security goals this high-rate communication would incur high overhead, both in terms of communication and processing. Consider, for example, a vehicle receiving digitally certificate, signing the message, verifying the receiver’s identity, RSU verifying its identity, safety messages from vehicles; it would need to validate a hundreds of vehicles within range within a short delay in the order of a hundred milliseconds [7]. Even if vehicle is effective under such dense network conditions, the additional security overhead could cause failure in meeting the delay and reliability requirements of safety applications. This is especially so because the vehicle environment lacks appropriate algorithm to reduce the load on processing and transfer the load to high speed internal or backbone communication network. The proposed rapid communication and group signing of messages solves these problems and meets the security goals with the help of a set of public keys for securing the communication and maintaining anonymity of users or vehicles.

First we outline why we actually need to secure car to car open wireless communication by stating various security threats from using open wireless communication or loosely structured security framework. Then in Section II we establish the security model i.e. security goals around which the security of every C2C communication should lie. The review of related work and its analysis along with its drawback is discussed in Section III. Then extending to our own security architecture for our proposed solution is followed by in Section III. Section IV discusses additional mechanism to hasten the authentication process, tracking intruders and closing any gaps in security framework.

2. SECURITY THREATS AND GOALS:

Unlike traditional wired/wireless system a C2C communication system is highly dynamic. Along with handling provisions for normal communication and keeping the system secure, it also has to tackle the system dependent problems such as handovers. Handover from one infrastructure to another can be costly as it requires verification of identity at the same time maintaining user-privacy and cost-effective communication.

Such a system can also be used for enhancement of road-safety by using various signaling techniques such as collision warning, intersection collision, emergency vehicle, brake-light warning, motorcycle warning, etc. In this communication, security plays a very important role as we discuss the attacks on vehicular communication.

1. *Phony information.* One or several legitimate members of the network send out false information to misguide other vehicles about traffic conditions.
2. *False location*. Transmission of a false position message by a malicious vehicle that pretends to be at a claimed position.
3. *Tracking identity:* A global entity can monitor trajectories of targeted vehicles and use these data for many purposes.
4. *False Messages:* Such attacks include aggressive transmission of fake messages like accident or traffic jam or emergency vehicle.
5. *Masquerade.* The attacker claims to be another vehicle by using false identities.

We propose modified public key communication and rapid communication technique for enhancing the speed of communication along with additional security specification and architecture. Also, we propose new C2C communication techniques such as group messaging and foreign-vehicle short-term key. We stress that every communication should ensure these security goals. [5]

- *Confidentiality:*
  Confidentiality is observed to protect sensitive information from getting manipulated and analyzed by eavesdropping as wireless communication medium is open and broadcasted over the air. By using end-to-end encryption, which requires the presence of mutual authentication and key agreement, the confidentiality objective can be achieved
- *Authentication:* Authentication techniques are observed to verify the identity of the vehicular nodes in communication. In particular, the authentication includes two levels: authentication between vehicles (V2V authentication) to provide link-to-link security, and authentication between the vehicle and RSU as well as the service provider (V2Iauthentication).
- *Privacy:* Privacy issues for service provisioning in VANETs regard primarily preserving the anonymity of a vehicle and/or the privacy of its location. Privacy protection tries to prevent adversaries (e.g., another vehicle or an external observer) from linking the vehicle to the driver's name, license plate, speed, position, and traveling routes along with their relationships to compromise the sender's privacy
- *Message Non-Refutation* Every message should be binded to the sender so that the sender cannot deny having sent a message. Anonymizer ensures anonymity of sender to other nodes and ensures privacy but does not compromise in security and its association with each sender.
- *Anonymity:* Privacy of vehicles can be protected by introducing a mapping between permanent key and temporary key as one approach, which is an anonymous key pair that can be changed frequently. Another approach is having a set of short-term public keys ,each being used for a random time called the dwell period. An alternative for providing anonymity in vehicular networks is the use of group signatures

3. SECURING COMMUNICATION

Although there were few studies regarding the security to different extents, they have all failed in taking the extension ability issue and resultant communication overhead, the time required in authentication of a vehicle versus the required response time into consideration. Authentication of messages must be implemented to allow vehicle users to differentiate reliable information from phony information and to defend against modification attacks and masquerading attacks. An appealing solution to this problem is to digitally sign messages before sending them; not only does this allow the receiver to identify the sender, but the signature also prevents the message contents from being modified in transit. Digital signatures[6] are the basic tool to secure communications, used for all messages. In terms of authentication and integrity-check, digital signature in conventional public key infrastructure (PKI) [1] is a good accepted choice. However, it may cause problem when a vehicle is required to verify the signatures of other vehicles by itself and hence trusted authorities are required. Each Certification Authority (C.A) is responsible for a region (national territory, district, county, etc.) and manages identities and credentials of all nodes registered with it. Each node is registered with only one CA, and has a unique long-term identity which may be an Electronic License Plate (ELP) with a long-term key and a certificate. To satisfy both the security and anonymity requirements, we rely on a short-term key authentication approach. Also, further we discuss how tradition PKI is unsuitable for communication and we will use short-term public key pairs instead.

Fig. 1 shows security architecture for vehicular communication in which a large set of relevant security concepts [3] exists, including concepts for

- Node identification,
- Digital signatures and certificates,
- Anonymizer for location privacy protection,
- Detection of protocol violation,
- Plausibility checks,
- Tamper-resistant devices,
- Access control policies,
- Software certification,
- In-vehicle network security,
- secure positioning, and more.

For enhancing the security, the header is divided into variable and invariable fields. Invariable are those fields thatremain unchanged from sender to destination , e.g., destination and source addresses and source position. Variable fields, such as sender location and time-to-live (TTL), are allowed to be altered by intermediate nodes. For packets being sent via multiple wireless hops, two signatures are added: an end-to-end signature is created by the sender node over the invariable fields of the packet header. Additionally, a hop-by-hop signature is added for the variable fields. On reception of a data packet a node verifies both signatures, and replaces the hop-by-hop signature by a new one for the altered variable fields and keeps the end-to-end signature. Eventually, the combination of end-to-end signatures results in a trusted forwarding chain [2].

In order to identify a particular vehicle taking part in communication there is a unique identifier. The Electronic License Plate (ELP) may serve as a unique identifier and acts as identity check mechanism. However, sending the original identifier may be prone to several risks such as masquerading attacks and hence the ELP needs to be mapped to a temporary identifier to be used for communication. There is a trusted authority namely the Certification Authority (C.A.) which keeps track of these unique identifiers and performs the job of mapping into a temporary unique identifier. This original solution however, had many problems like synchronization of different C.A's and constant communication between V2I (vehicle to Infrastructure) causing further delay and loss of information. Hence the new proposed solution consists of a set (atleast 2) of permanent identifiers stored in each vehicle. Each vehicle consists of atleast 2 unique identifiers or public key. Each car communicates with only one of these stored keys for a certain period of time. This time during which it communicates with a single key is known as dwell time which is a pseudo-random number generated by its own hardware mechanism. It also acts as an added privacy mechanism for hiding user's identity and making it difficult to track by an intruder.

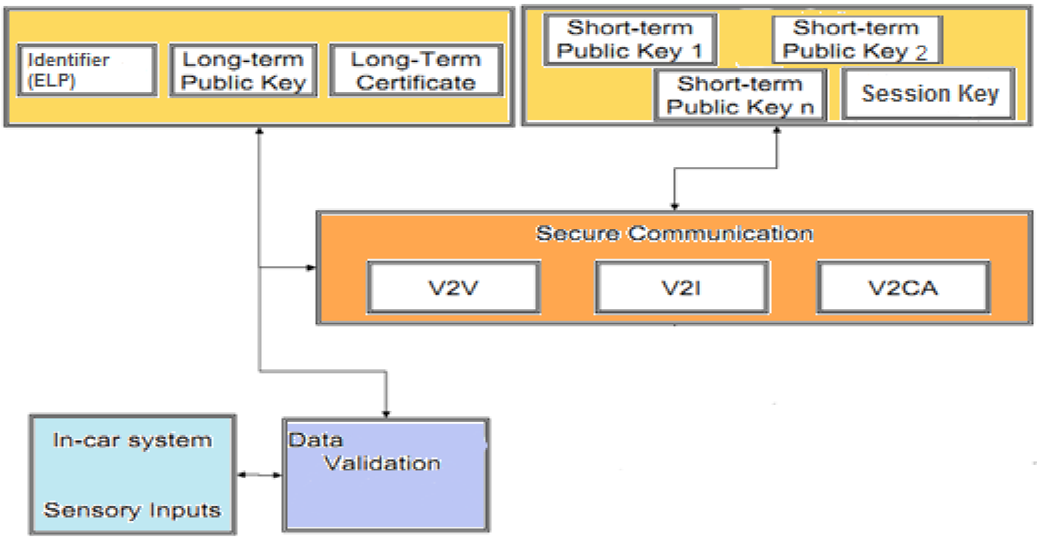

Fig – 1: Security Architecture

The Fig. 2 shows that every vehicle utilizes multiple short-term public key pairs instead of the old approach of using the same long-term public key for securing communications. The mapping between the long-term keys and the short-term credentials of each node (car) is maintained by the C.A. The main idea is that (i) every vehicle will be equipped with multiple certified public keys (anonymizers) that do not reveal the car's identity, and (ii) the node uses every one of them for dwell time

The multiple-anonymizer technique is adopted to attain location privacy. Particularly, vehicles are assigned with a set of identifiers, and the public keys that are alternatively used. Cars frequently change their key values or temporary identifiers used for authentication over time, and due to the unlinkability of old and new messages their location confidentiality preservation is attained.

Moreover, the anonymizers can be linked to a specific vehicle by the CA so that the CA is able to trace and regulate the vehicle's behavior.

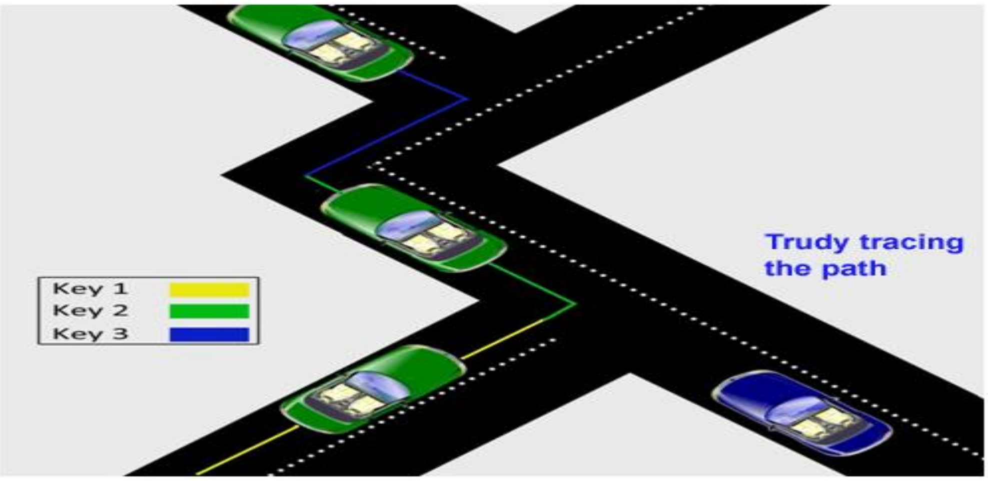

Fig- 2 Road map of vehicle using different keys

4. ADDITIONAL FEATURES

4.1 Group Message

Furthermore, the signatures and public key certificates radically increase the packet length to cause intense message overhead. Furthermore, these cryptographic operations can incur very high computation and communication overhead. When V2V communication is performed in an urban area with many vehicles in each other's communication range, this becomes a particularly serious problem.

Each node M is equipped with a group vehicle key GVK , with the group members comprising all vehicles registered with the CA. A group key GVK generated by a group member allows for the validation (by any node) of any group signature with the help of CA. Intuitively, a group signature scheme allows any node V to sign a message on behalf of the group, without V 's identity being revealed to the signature verifier. Moreover, it is impossible to link any two signatures of a legitimate group member. Note that no public key or other credentials need to be attached to an anonymously authenticated message.

4.2 Foreign Vehicle-short-term key

Taking an analogy of a tourist place it is easy to spot a local person from the crowd as they look different from others. Taking the inverse in our case a foreign person is easier to be identified and more prone to threats. In C2C communication we use the identifier to relate a particular message to a particular car. However, the mapping between the permanent and temporary credentials also takes place by home C.A and hence this mapping will be completely different from the credentials assigned by a foreign C.A. Say, a car from United States comes to Canada with its permanent and temporary key pairs protecting the car's identity. However, from a group of say hundred cars these temporary keys that will be used are still easy to distinguish from the keys used locally by the Canadian cars and hence easy to track its location and failing to protect its identity. These keys are like I.P addresses assigned to computers which itself tell its location like country, region, etc. Hence we propose to use new short term but permanent key pairs assigned to them whenever a foreign location is visited i.e. they register themselves with a foreign C.A first which in turn informs the home

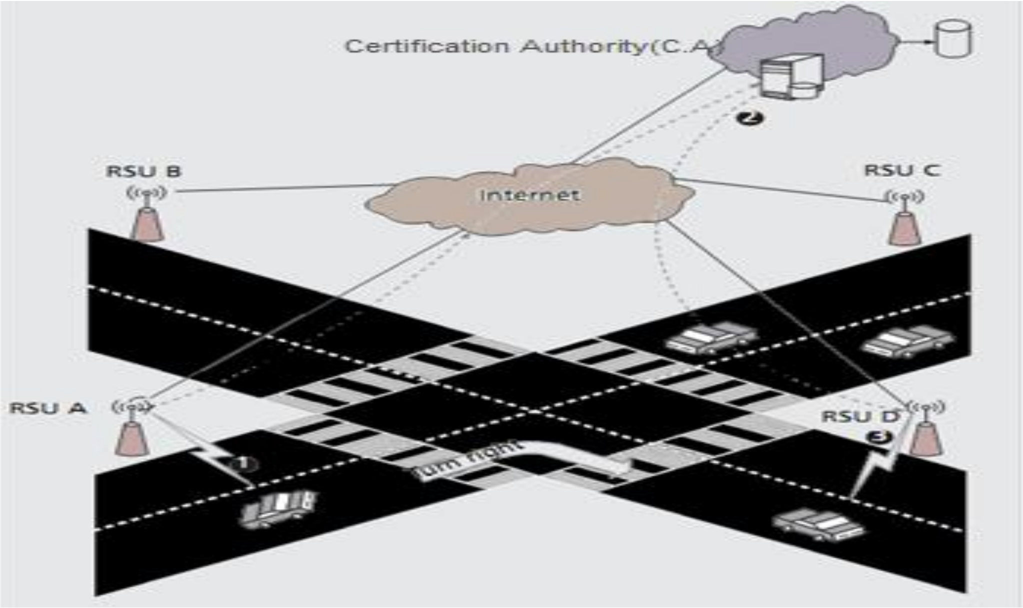

Fig- 3 Communication in Vehicular Network

C.A of the change of keys as long as they are in that region. This makes it difficult for an intruder to attack a specific foreign car.

4.3 Rapid Authentication

To enable progress to authentication in C2C communication fast access or connectivity to infrastructure is highly needed. The speed with which the vehicle travels may exceed the speed with which the communication takes place between a car and a RSU (Road-Side Unit).The main cause of this delay is authentication mechanism and user privacy.Currently, there are a few strategies to improve this overhead by reducing the handoff latency in which the initial messages are protected and authenticated thereafter, the communication takes place unencrypted making it more prone to replay attacks, hijacking, masquerading and many more attacks.

It may take time once for the RSU to authenticate the car then the communication takes place instantly. However, the range of one particular RSU is pretty limited compared to the distance the car covers and hence repeat authentication takes place. This repeated authentication cannot be avoided simply to speed-up the communication however; it can be facilitated with a shared secret key passed from one RSU to another. This shared secret has its own lifetime and the node (car) can be authenticated rapidly with the help of this key. The key is not known to any other car and changes frequently to avoid replay attacks. Here, the added security layer that has been provided is that the shared key may not be broadcasted to all RSU's in vicinity but only to one that will be next in the range of the car. Hence, a prediction is made based on the messages broadcasted by the car: the direction, speed, brake light and turnsignal. Say there is a message broadcasted as presented below[4]: <Direction, Speed, Acceleration,Turn-Light, Traffic-Light>, where Direction denotes the direction a vehicle turns, such as east or west, and Speed denotes the velocity of a driving vehicle. Acceleration denotes whether a driving vehicle accelerates or decelerates. If the value of this field is positive, the vehicle is speeding up; otherwise, the vehicle is slowing down. The fourth field, Turn-Light, denotes signals of the turn light of a vehicle, particularly when a vehicle is going to turn at an intersection.

If the car is travelling on highway with some speed then it's easy to predict the next RSU and the next after that, saving time on authentication and improving road safety. If the car is travelling in a neighborhood area and suddenly the cars turns, A message will be broadcasted regarding this turnsignal and the RSU may predict the next RSU based on this turnsignal. This prediction may be added cost to RSU however it also reduces the burden of messages that other RSU services. In an ideal condition the authentication takes place the first time with one RSU using the lengthy authentication mechanism and thereafter all communication takes place using rapid authentication speeding up the communication process to almost double the original speed.

4.4 Revocation

The revocation is concerned with excluding nodes from the system. The CA will contain a database of revoked node's identifier and distributes this data to all nodes in the system if necessary, depending on the scale of the revocation decision and the extent to which the malicious activity has been performed. A reaction to detected attacks carried out by a node is to exclude this node from the system. Moreover, verification of this malicious activity is also important as, due to flaws in security an intruder can perform such activity and masquerade itself as another node in which case the victim suffers unnecessarily. Also, depending on various factors the threat of that particular vehicle is detected. Factors like the number of nodes reporting the same malicious activity about the node, traffic density, validation of messages, authentication of nodes and position. For example, messages like emergency vehicle are broadcasted so if Trudy broadcasts this false message repeatedly in an urban area with say traffic density of 125 vehicles and only 1 or very few reports comes in then Trudy may not be included in the revocation list instead could be maintained in a temporary warning list for a certain amount of time by the C.A. till which further complaint comes in then appropriate and fast response could be achieved otherwise the node is simply ignored and deleted from temporary warning list . Other reasons not directly related to operation of system, such as a stolen unit or prevention of criminal activity may also require a revocation service.

5. CONCLUSIONS

In this paper we propose the security framework for establishing communication and authentication along with privacy in ad hoc Car to Car communication. The different requirements of each user and car were studied and hence it is not appropriate to design a specific security framework for the System. Hence we established rapid authentication mechanism along with group messages to speed up the communication process and make C2C communication in ad hoc environment feasible. The proposed system establishes and maintains communication in the mentioned ad-hoc environment and also it provides a rigorous security infrastructure as a whole. Since these communication systems are to be used in high-end automobiles, cost of implementation and maintenance of Public key infrastructure is financially feasible. Our work will provide a new way to look at the security issues in C2C consortium.

REFERENCES

[1]. “Securing vehicular ad hoc networks,” Journal of Computer Security - Special Issue on Security of Ad-hoc and Sensor Network, vol. 15

[2]. “Cross-Layer Privacy Enhancement and Non-Repudiation in Vehicular Communication,” in Proceedings of 4th Workshop on Mobile Ad-Hoc Networks (WMAN), Bern, Switzerland

[3]. ”On the Performance of Secure Vehicular Communication System” - IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 6,

[4]. Fast and Secure Multihop Broadcast Solutions for Intervehicular Communication- Wafa Ben Jaballah, Mauro Conti, Mohamed Mosbah, and Claudio E. Palazzi

[5]. “The Car-to-Car Communication Consortium,” http://www.car-to-car.org, 2010.

[6]. D. Chaum , “Security without Identification: Transaction Systems to Make Big Brother Obsolete,” Comm. ACM, vol. 28, no. 10,

[7]. “DSRC: Dedicated Short Range Communications,” http://grouper.ieee.org/groups/scc32/dsrc/index.html, 2009.

[8]. J. Blum, A. Eskandarian, and L. Hoffman, “Challenges of intervehicle adhoc networks,” IEEE Trans. Intell. Transp. Syst., vol. 5, no. 4, pp. 347–351, Dec. 2004.

[9]. J. Blum and A. Eskandarian, “The threat of intelligent collision,” IEEE IT Prof., vol. 6, no. 1, pp. 24–29, Jan./Feb. 2004.

[10]. A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, R. Kroh,

[11]. “Dedicated Short Range Communication at 5.9 GHz StandardsGroup,” http://www.iteris.com/itsarch/html/standard/dsrc5ghz-b.htm,2009.

[12]. “ISO TC204 Working Group 16,” http://www.calm.hu/, 2010.

[13]. P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, “Certificate Revocation List Distribution in Vehicular Communication Systems,” Proc. Fifth ACM Int’l Conf. Vehicular Ad Hoc Networks(VANET ’08), Sept. 2008.

[14]. Y.-W. Lin, Y.-S. Chen, and S.-L. Lee, “Routing protocols in vehicular adhoc networks: A survey and future perspectives,” J. Inf. Sci. Eng., vol. 26, no. 3, pp. 913–932, May 2010.

[15]. A. Broggi, P. Cerri, S. Ghidoni, P. Grisleri, and H. G. Jung, “A new approach to urban pedestrian detection for automatic braking,” IEEE Trans. Intell. Transp. Syst., vol. 10, no. 4, pp. 594–605, Dec. 2009.

[16]. M.-T. Sun, W.-C. Feng, K. Fujimura, T.-H. Lai, H. Okada, and K. Fujimura, “GPS-based message broadcasting for inter vehicle communication,” in Proc. ICPP, Aug. 2000, pp. 279–286.