Volume 3, Issue 8, August 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Location Tracking for VANET

A. Manikandan
Asst.Prof / ECE Department & MKCE
India

Abstract—In this paper, we proposed locate and track a vehicle in VANET, based on its transmissions, during communication with other vehicles or the road-side infrastructure to tracking of vehicles based on their broadcasts, and proposed a solution called CARAVAN. We identified that by combining neighboring vehicles into groups, it is possible to reduce the number of times a vehicle needed to broadcast for V2I applications such as probe vehicle data. Using group the vehicles can be provided with an extended silent period, which in turn enhances their anonymity.

Keywords— Privacy, traceability ,CARAVAN, vehicular ad hoc

I. INTRODUCTION

Vehicular ad hoc networks (VANET) enable vehicles to communicate among themselves (V2V communications) and with road-side infrastructure (V2I communications). Such net-works present various functionalities in terms of vehicular safety, traffic congestion reduction, and location based service (LBS) applications. Recognizing the potential of VANET, there has been concerted efforts [1], [2], [3] to network vehicles. However, many challenges including the security and privacy issues remain to be addressed [4], [5], [6].

The unique requirements of maintaining liability of vehicles involved in accidents, and ensuring the safety rendered by the communication between vehicles, challenge the network connectivity, privacy, and certain security aspects (discussed later in Section III-D) in VANET. Moreover, advances in localization and tracking techniques enable accurate location estimation and tracking of vehicles in VANET. By tracking a vehicle, it becomes possible to identify the locations visited by the vehicle, thereby, breaching the privacy of the user of the vehicle. Furthermore, the location tracking information about a user can be misused by an adversary. Additionally, identifying the LBS applications accessed by a vehicle, provides private information of the vehicle's user.

In this paper, we address the *problem of allowing any vehicle to be able to achieve unlinkability between two or more of its locations in the presence of tracking by an adversary*. For developing a suitable solution, unlike previous approaches for location privacy in mobile networks (see Section V-C), we account for the constraints posed by vehicular mobility and vehicular applications in VANET (see Section II-D). Contributions of this paper are the following. (1) We identify that the *group navigation* of vehicles can be used for providing location privacy in VANET. (2) We propose a location privacy scheme called *CARAVAN*, that combines the group navigation with a random silent period enhancement technique, to miti-gate tracking of a vehicle. (3) We leverage the group to provide anonymous access to LBS applications, and show when such a solution can preserve a vehicle user's privacy.

The rest of the paper is organized as follows. Section II describes the VANET system model and the adversary model considered, and presents the unique constraints of VANET. Section III describes the proposed location privacy enhancement scheme. Section IV evaluates the performance of the proposed solution. Section V covers the related work, and Section VI presents our conclusions.

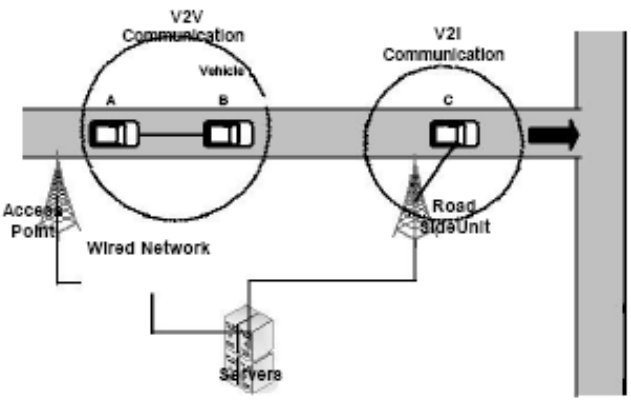

Fig. 1. Illustration of inter-vehicle communication and the components involved. The circles indicate communication between the enclosed nodes.

II. SYSTEM MODEL

A. VANET System Model and Assumptions

Fig. 1 illustrates a typical VANET that consists of vehicles, access points on road side, and a collection of location servers. Vehicles move on roads, sharing collective environmental information between themselves, and with the servers via access points.

Fig. 2 illustrates a detailed view of our system model. A vehicle is enabled with on-board communication unit for V2V and V2I communications, and sensor (for example, GPS) and database units to collect environmental information (for exam-ple, location, vehicle speed, tire pressure). The communication unit of the access points are called *Road Side Units (RSU)*, which are connected to *location server* by a wired network. The location server records all the *location data* forwarded by the RSUs, and processes the data together with information from other data sources for example, vehicle manufacturers, police, traffic management center, weather information center. The location server also provides an interface for the *location based Service Providers (SP)*. In addition, a trusted *Registra-tion Authority (RA)* provides authentication and authorization service to both vehicles and LBS providers.

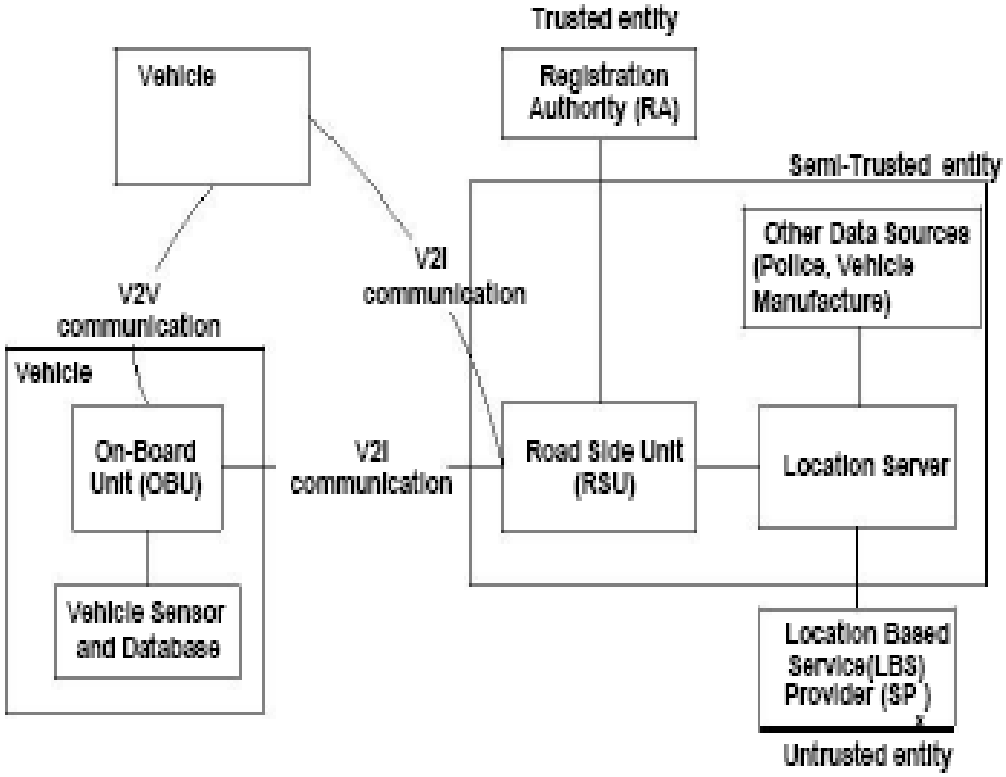

Fig. 2. Illustration of an inter-vehicle communication system.

B. Trust Assumptions and Adversary Model

We assume that the registration authority (RA) is a trusted entity in our model, as shown in Fig. 2. The infrastructure including the RSUs and the location server are only semi-trusted[2] to operate as expected. We additionally, assume that the RSUs are able to estimate location of a vehicle based on the vehicle's transmission signal.

In our model, we assume a *global passive adversary*. Such an adversary is able to overhear *all* the broadcasts of *all* the vehicles, and hence, able to estimate their locations.

C. Application Scenarios Considered

We consider three typical classes of VANET applications, *cooperative driving*, *probe vehicle data*, and *location based service (LBS)* in this paper. In the *cooperative driving* appli-cation, adequate equipped vehicles maintain a very short sep-aration (intra-convoy spacing) between each other and move smoothly with the same pre-defined speed (convoy speed). These vehicles communicate with each other frequently either directly or via communication equipments on road side. For example, in a prototype for cooperative driving in [7], vehicles broadcast their status information (e.g. speed, location, accel-eration) every 500 ms. The advantage of cooperative driving is the increase in both safety and highway capacity resulting from the automation and close coordination of vehicles.

III. PROPOSED LOCATION PRIVACY SCHEME FOR VANET

In this section, we present CARAVAN, the proposed loca-tion privacy scheme for VANET, and describe the enhancement techniques that constitute CARAVAN.

A. Use of Silent Period to Provide Unlinkability Between Locations

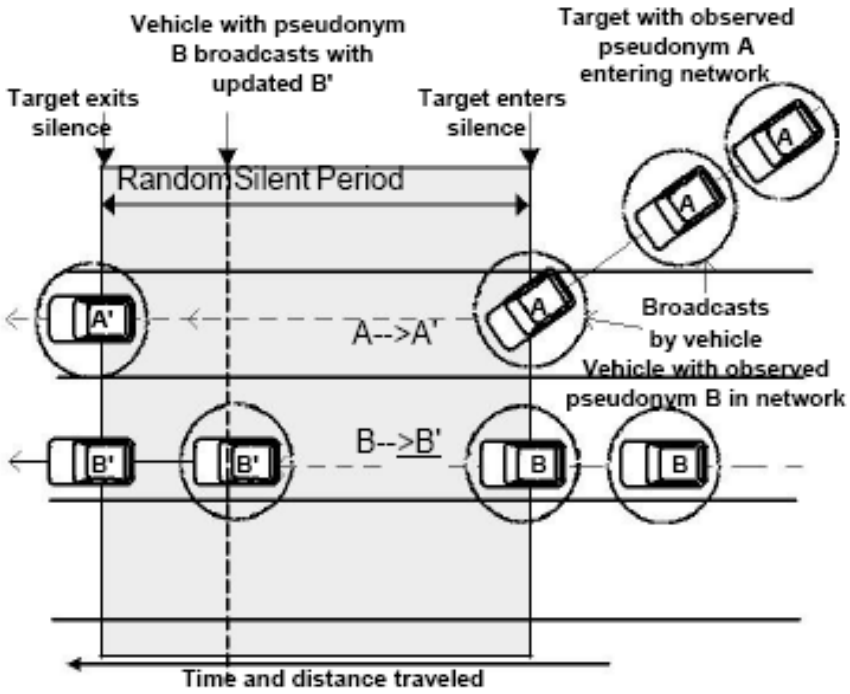

Fig. 3. Illustration of the effect of random silent period when used by a vehicle during network join. A target vehicle entering the network, broadcasts with pseudonym *A*, and then goes into silence. If a neighboring vehicle updates its pseudonym from *B* to B^0 during this silent period, then an adversary can be misled to consider pseudonym B^0 (and hence, the associated neighbor vehicle's location) to be that of the target vehicle, provided the target vehicle updates to A^0 before its next broadcast.

Fig. 3. Illustration of the effect of random silent period when used by a vehicle during network join. A target vehicle entering the network, broadcasts with pseudonym *A*, and then goes into silence. If a neighboring vehicle updates its pseudonym from *B* to B^0 during this silent period, then an adversary can be misled to consider pseudonym B^0 (and hence, the associated neighbor vehicle's location) to be that of the target vehicle, provided the target vehicle updates to A^0 before its next broadcast despite pseudonym update, it is still possible to link the new and old pseudonyms of a node using temporal and spatial relation between the new and old locations of the node. As a solution the use of a random silent period between update of pseudonyms was proposed in [12]. We make use of *silent period* to provide unlinkability to a vehicle entering the network, by enforcing that the vehicle will remain silent for a randomly chosen period of time.

B. Use of Group Concept to Avoid Overhearing Pseudonyms

We make the following observations that motivate the group concept applied in our solution.

1) Vehicles in geographical proximity often share redun-dant information such as road and traffic conditions. Hence, in V2I based applications, such as probe vehicle data, where the vehicles respond to requests received from the infrastructure, not all vehicles need to send replies.
2) As observed in Section II-D, the mobility of vehicles is spatially restricted and spatially dependent. Hence, vehicles in geographical proximity can navigate as a group, with the same average velocity due to the spatial dependency, and with similar direction due to the spatial restrictions, over a period of time.

We make use of the above observations, and propose to enable vehicles to form a *group*. In order to form a group, we restrict the *vehicles to be in a group if each group member can hear broadcasts of every other group member*. Since vehicles in a group will move relative to each other, and on average have the same velocity, a group can be represented by a single vehicle that we refer to as the *group leader*. Then for most of the V2I communication based VANET applications, it is sufficient if only the group leader communicates on behalf of the group. Consequently, the remaining vehicles in the group are able to remain *silent for an extended period* of time that is bounded by the time they remain in the group.

We consider the probe vehicle data application, where typically, the vehicles send probe replies once in several tens of seconds. By using vehicular groups, we offer the following benefits: (1) The *silent period* of a group member vehicle is *extended*, if the vehicle does not change group between two probe data requests. (2) Unnecessary *overhead and re-dundancy* of the neighboring vehicles broadcasting possibly redundant probe data is reduced, since only the group leader replies to the RSU with probe data. (3) A reduced *number of pseudonym updates* (and hence, the number of pseudonyms) are needed to provide the same level of anonymity achieved when the vehicle updates after every broadcast.

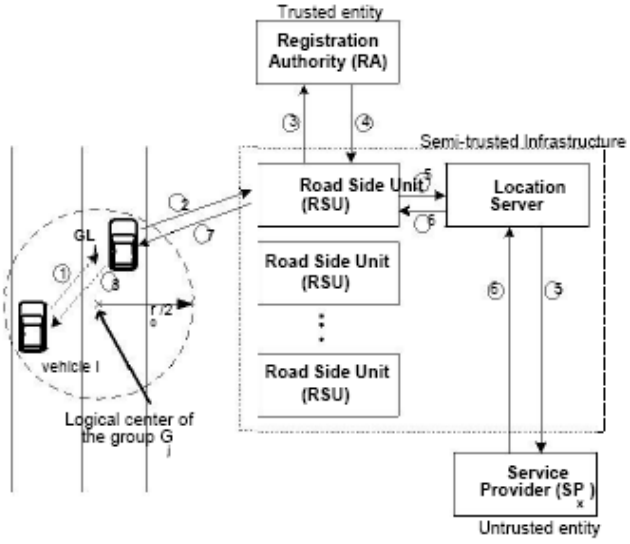

Fig. 4. Illustration of the anonymous access to LBS application provided to a vehicle *i* which is member of the group G_j with the group leader vehicle being GL_j. The sequence of steps in the protocol are indicated in the figure.

C. Leveraging Group to Provide Unlinkability Between Pseudonym and LBS Application

1) Protocol description: Fig. 4 shows the anonymous ac-cess protocol and the steps involved. Upon receiving the application request from vehicle *i* (in Step 1), the group leader GL_j of *i*'s group G_j forwards the request with its own address, to the registration authority *RA* via the RSU (in Step 2-3). The *RA* validates the application request, and then provides a session key $k_{x;i}$ to both the service provider (SP_x) and vehicle *i* (Step 4-7). This key is used to encrypt the entire communication that takes place between *i* and the SP_x. GL_j broadcasts the communication received from SP_x (via RSU) to the group. On termination of the application, the SP_x as well as vehicle *i* provide the transaction details to the *RA*, which acts as the arbitrator and resolves any disputes. We note that in order to lower the load of the *RA*, anonymous payment based protocols can be used in the LBS application access. However, we do not provide such a payment scheme here, since it is out of scope of this paper.

2) Group Key and Application Address Range: In generat-ing the application request, vehicle *i* performs the following two steps: (1) randomly chooses an available address A_{aa} from a known *application address range* of the group G_j, (2) broadcasts the application request encrypted with the *group key* k_{Gj} and with A_{aa} as source address. The group key and the address range are obtained by the group members of G_j from GL_j, when joining the group (see Group Join protocol in Appendix). These two parameters *prevent trace back from* GL_j *to i*. Since the *random address* A_{aa} is not associated with vehicle *i*, the application request from *i* cannot be associated with any of its pseudonym. This particular feature allows the vehicle *i* to access the LBS application even in any identifiable area, while also simultaneously broadcasting safety messages with its pseudonym $PID_{i;k}$. The *group key* k_{Gj} on the other hand, prevents tracing *i* based on the format of application request message that is broadcast to GL_j in Step 1 of the protocol.

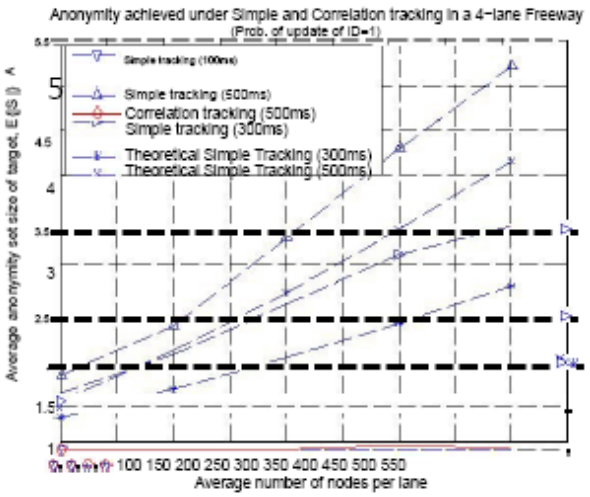

Fig. 5. Average anonymity provided to a target when it updates pseudonym in a 4-lane Freeway, for different number of vehicles (nodes) per lane.

In the following section, we address the different attacks on the proposed scheme, and we suggest suitable solutions.

D. Discussion of Attacks and Solutions for Proposed Scheme

1) *Injecting false data:* A compromised vehicle in the VANET can misbehave and broadcast incorrect data, with the malicious intent of attacking its neighboring vehicles. How-ever, since each vehicle signs the broadcast safety messages, the identity of any misbehaving vehicle can be verifiably determined.
2) *Local active attacker:* If the group leader colludes with the adversary, then the anonymity of the vehicle accessing the LBS application can be breached under the global adversary

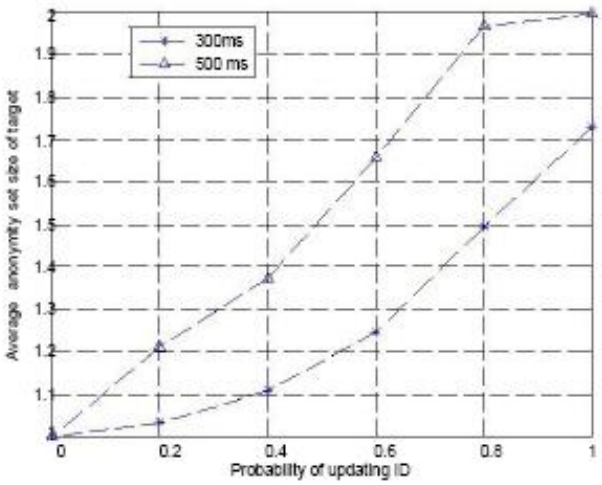

Fig. 6. Average anonymity provided to a target in a 4-lane Freeway, for different probability of updating pseudonym.

IV. EVALUATION OF VANET LOCATION PRIVACY

In this section, we first describe potential tracking methods that can be employed to link two locations of a vehicle.

A. Tracking of Vehicles

1) Simple tracking: In this method, the adversary obtains the target vehicle's location l_{known} and *speed* at time *t*, and then estimates, based on possible movement directions, a reachable area A_r around l_{known}, in which the vehicle's actual location l_1 at a future time t_1 can lie. Fig. 5(a), illustrates the simple tracking of a vehicle, and shows the reachable area of the vehicle determined by the achievable speed and silent period ranges.

2) Correlation tracking: As illustrated in Fig. 5(b), in correlation tracking, the adversary uses a vehicles last known location l_{known}, *speed*, and *direction* at time *t* to estimate the entity's location l_{est1} at a future time t_1. The estimation is repeated till the maximum silent period is reached.

B. Analytical Evaluation of Anonymity

We use two performance measures to evaluate the level of anonymity (unlinkability) achieved in a VANET: (i) the size of the *anonymity set* (ii) the *maximum tracking/identifiable time* . Anonymity set was introduced by Chaum [16], and the size of anonymity set was shown to be a good indicator of how much anonymity is provided. The *anonymity set* of a target, denoted by S_A, is defined as the set of pseudonyms that are indistinguishable from the target pseudonyms to an adversary, and the set includes the target pseudonyms themselves. The size of anonymity set, denoted by jS_Aj, depends on the knowledge and the tracking method of an adversary. The second measure, *maximum tracking time* of a target, denoted by T_{track}, is defined as the maximum cumulative time that the size of anonymity set of the target remains as one. We assume that vehicles are uniformly distributed on city streets or freeways with density ½.

V. CONCLUSIONS

In this paper, we addressed the location privacy threats that arise in VANET due to tracking of vehicles based on their broadcasts, and proposed a solution called CARAVAN. Taking into account the mobility, and the application features in VANET, we identified that by combining neighboring vehicles into groups, it is possible to reduce the number of times a vehicle needed to broadcast for V2I applications such as probe vehicle data. Using group the vehicles can be provided with an extended silent period, which in turn enhances their anonymity. Assuming the global adversary model, and under the safety application constraints of VANET, we evaluated the enhancement of anonymity achieved by our proposed solution. We also suggested an enhancement technique that takes into account the separation between RSUs, and the transmission power control capability of vehicles. Further, we proposed an anonymous access protocol to address threats to privacy that arise due to access to LBS applications, and found that it was robust under the global adversary model, as

well as under the safety application constraints. Future work includes evaluation of proposed location privacy solutions under more realistic mobility for vehicles, combined with map data, and with communication traffic models.

REFERENCES

[1] 5.9GHz DSRC. [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html
[2] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a future vehicular network," in *European Wireless*, 2002.
[3] J.-P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy*, vol. 2, no. 3, pp. 49–55, 2004.
[4] M. Raya and J.-P. Hubaux, "Security aspects of inter-vehicle communi-cations," in *Swiss Transport Research Conference*, 2005.
[5] ——, "The security of vehicular ad hoc neworks," *Proc. of the ACM Workshop on Security of Ad hoc and Sensor Networks (SASN)*, 2005.
[6] F. Dotzer,¨ "Privacy issues in vehicular ad hoc networks," in *Proc. of the Workshop on Privacy Enhancing Technologies (PET)*, 2005.
[7] R. Hochnadel and M. Gaeta, "A look ahead network (LANET) model for vehicle-to-vehicle communications using DSRC," in *Proc. of the ITS World Congress*, 2003.
[8] ITS probe vehicle techniques. [Online]. Available: http://tti.tamu.edu/documents/FHWA-PL-98-035 c5.pdf
[9] T. Fushiki, T. Yokota, K. Kimita, M. Kumagai, and I. Oda, "Study on density of probe cars sufficient for both level of area coverage and traffic information update cycle," in *Proc. of the ITS World Congress*, 2004.
[10] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. of the ACM MobiSys*, 2003, pp. 31–42.
[11] R. W. Rothery, "Car following models," in *In N.H. Gartner, C. Messer, and A.K. Rathi, editors, Traffic Flow Theory, Chapter 4.* , 2002.
[12] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2005, pp. 1187–1192.
[13] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in *Advances in Cryptology - EUROCRYPT 2001*, ser. LNCS, vol. 2045. Springer, 2001, pp. 93–118.
[14] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, 1981.
[15] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in vanets," in *Proc. of the ACM Workshop on Vehicular Ad hoc Networks (VANET)*, 2004, pp. 29–37.
[16] D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, pp. 65–75, 1988.
[17] I. Seskar, S. Maric, J. Holtzman, and J. Wasserman, "Rate of location area updates in cellular systems," in *Proc. of the IEEE Vehicular Technology Conference*, 1992, pp. 694–697.
[18] A. M. Mathai, *An Introduction to Geometrical Probability: Distribu-tional Aspects with Applications*. CRC Press, 1999.
[19] M. Gruteser and D. Grunwald, "Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis," in *Proc. of the ACM Workshop on Wireless mobile applications and services on WLAN hotspots (WMASH)*, 2003, pp. 46–55.
[20] F. Dotzer,¨ F. Kohlmayer, T. Kosch, and M. Strassberger, "Secure communication for intersection assistance," in *Proc. of the International Workshop on Intelligent Transportation (WIT)*, 2005.
[21] ISO/TC204:transport information and control systems (TICS). [Online]. Available: http://www.sae.org/technicalcommittees/tc204.htm
[22] F. Bai, N. Sadagopan, and A. Helmy, "IMPORTANT: A framework to systematically analyze the impact of mobility on performance of routing protocols for adhoc networks," in *Proc. of the IEEE Infocom*, 2003, pp. 825–835.

