Strengthening Privacy Protection in VANETs

Mike Burmester
Department of Computer Science
Florida State University
Tallahassee, Florida 32306–4530
Email: burmester@cs.fsu.edu

Emmanouil Magkos and Vassilis Chrissikopoulos
Department of Informatics
Ionian University
Platia Tsirigoti 7, 49100 Corfu, Greece
Email:{emagos,vchris}@ionio.gr

***Abstract*—In the not so far future, vehicles are expected to be able to communicate with each other and with the road infrastructure, to enhance driving experience and support road safety, among others. Vehicular Ad-hoc Networks (VANETs) introduce a number of security challenges to the research community, mainly concerning the tradeoff between the privacy of the drivers and the accountability of misbehaving vehicles. Another challenge is how to satisfy privacy in the presence of an adversary that has access to all communication (a global observer), and that can perform traffic analysis in order to link messages and identify vehicles.**

In this paper we attempt to address such issues and propose a set of cryptographic mechanisms that balance the tradeoff between privacy and accountability in a VANET. Furthermore, we examine techniques for location privacy against adversaries that perform a Bayesian traffic analysis, and propose a strategy to strengthen location privacy in VANETs.

I. Introduction

Vehicular Ad-hoc Networks (VANETs) are receiving increasing attention in industry and academia, as they are considered by many to be the most challenging implementation of Mobile Ad-Hoc Networks (MANETs). In the not so far future, vehicles are expected to be equipped with sensors, short-radio wireless interfaces and computational capabilities, thus being able to communicate with each other and with the road infrastructure. Inter-vehicle networks are expected to enhance driving experience and to support road safety, traffic efficiency, automatic toll collection, infotainment and context-oriented personalized services, among others ([1], [2], [3]).

In a typical application of a VANET, vehicles broadcast safety messages such as emergency information (*e.g.*, concerning accidents, dangerous road conditions, sudden braking, lane changing, etc) or traffic avoidance warnings, in a one-hop or multi-hop fashion. Messages can also be routed to/from the road infrastructure (*e.g.*, in response to traffic jams reports, bad road conditions, requests for assistance, as well as non-safety related applications [1], [3], [4]). Two or more vehicles can also establish more permanent relationships (*e.g.*, create a platoon, drive cooperatively, engage in transactional communication, etc) [5].

The inherent characteristics of VANETs, such as the relatively uncontrolled operations environment, the high mobility of the nodes and the wireless medium, make them likely targets for abuse and introduce a number of security challenges to the research community. A number of passive and active attacks against the vehicular nodes and the infrastructure, have already been pointed out in the literature (see *e.g.*, [1], [5], [6], [7]). Examples of such attacks are: Denial of Service (DoS) at the physical or application layer, fabrication and substitution at the protocol layer, and eavesdropping at the wireless (physical) layer of the network. In view of the projected large scale applications of VANETs, these challenges urge the adoption of a set of security requirements: availability guarantees, message authentication, accountability (non-repudiation), privacy (anonymity and unlinkability), and in some scenarios confidentiality as well.

Of particular interest to the research community is the *tradeoff* between privacy and accountability: while we desire that it is hard to track (monitor) a vehicle within a group of other vehicles, a faulty vehicle or a vehicle that has caused an accident, may have to be properly identified so as to provide assistance and/or establish forensic evidence ([1], [2], [6]).

Our Contribution: In this paper we discuss the design requirements and present mechanisms for balancing the tradeoff between privacy and accountability in a VANET. We consider both pairwise and group communication among vehicles in the network, as well as communication between a vehicle and the road infrastructure. Our approach is hybrid, *i.e.*, we use symmetric and public key operations for message authentication and encryption. For strong privacy we require vehicles to use pseudonyms that are changed with a frequency that minimizes the overhead, while guaranteeing anonymity (that is, pseudonyms are changed only when needed). In addition, we elaborate on the unlinkability aspect of privacy and show how privacy-preserving mechanisms and pseudonym changing can often be defeated by adversaries who perform a Bayesian traffic analysis. To this end we propose a specific strategy to strengthen unlinkability in VANET communication.

This paper is structured as follows. Section II presents a brief summary of related work on security and privacy in VANETs. In Section III we model the network, discuss the threat model and examine design requirements for a privacy infrastructure. In Section IV we present a set of privacy-preserving protocols for VANETs. Section V discusses security and analyzes the performance of the proposed protocols. In Section VI we examine privacy and unlinkability against traffic analysis. Section VII concludes the paper.

II. Related work

During recent years, the challenges for security and privacy in VANETs have stimulated a number of introductory and survey papers (*e.g.*, [1], [3], [6], [7]). The literature has also provided several security mechanisms for inter-vehicle communications. More specifically, a few research papers discuss the need to balance privacy and accountability by using cryptographic techniques ([1], [3], [6], [8], [9], [10]). In ([1], [3]) for example, digital signatures for message authentication are combined with short-lived pseudonyms to establish conditional anonymity for the vehicular nodes.

Group formation is also proposed as an alternative strategy to strengthen privacy and hinder traffic analysis in VANETs ([5], [4], [11]), or to augment communication efficiency [12]. In [3] symmetric session keys are established between pairs of nodes or among a group of nodes in order to reduce the overhead in message authentication between vehicles that establish more permanent relations (*e.g.*, platoons).

The need for confidentiality in specific scenarios of VANET implementations has also been discussed in recent works ([7], [9], [13]). Specifically in [13], the protocols of [3] are extended: session keys for pairs of vehicles are established by using the Diffie-Hellman key agreement protocol [14] while group session keys are established using the key transfer approach of [3]. These keys are used for both message authentication and confidentiality [13].

III. Design Requirements

VANETs are typically *hybrid* networks ([8], [7]), *i.e.*, communication takes place between two or more vehicles in an ad-hoc setting (*Vehicle to Vehicle - V2V*) and/or between vehicles and the road infrastructure (*Vehicle to Infrastructure - V2I*). All vehicle nodes of the network are assumed to have unique identifiers (*e.g.*, this could be an Electronic License Plate number issued by an authority). Furthermore, vehicles are assumed to have sufficient power and computational/storage resources to run the required cryptographic mechanisms, and to be equipped with a tamper-resistant component ([1], [7]) that manages the cryptographic material and records a history of emergency events and messages.

A. Vehicle-to-Vehicle communication (V2V)

Vehicles are able to communicate with each other either directly, while they are in wireless range, or indirectly in multi-hop mode, with vehicles acting as both routers and end nodes. For example, safety messages concerning traffic congestion can be propagated through the network by neighbors traveling in opposite directions. We distinguish two modes of of communication:

- *Heart-beat* communication. In this mode a vehicle sends messages containing its current position and speed, or other safety-related information, to any neighbor in broadcast range—in either direction of the road. This mode requires the lowest overhead.
- *Group* communication. This mode covers scenarios where two or more vehicles decide to establish a more permanent relation, (*e.g.*, cooperative driving, platooning etc).

In proximity groups of more than two nodes, a group leader may temporarily manage group membership and group session key distribution. We do not discuss the details of group formation and group leader election as these are beyond the scope of this paper, but refer the reader to other works (*e.g.*, [4], [12]).

B. Vehicle-to-Infrastructure communication (V2I)

Vehicles are also able to exchange messages with the road infrastructure. At the front end, the infrastructure consists of *Road Station Units* (RSUs), which are base stations that handle the bulk of communication with the vehicles. At the back end, a *Registration Authority* (RA) is responsible for managing the network (*e.g.*, identity and certificate management, authorization control, auditing etc). The RA may be a single public entity or a set of entities or cooperating corporations ([1], [2], [10]). However we shall abstract away the specific structure of the RA, as well as the existence of a network infrastructure that mediates trust relations with other service providers.

In the *V2I* setting, communication can be either *uni-directional* (*e.g.*, vehicles send heart-beat messages to the RSU) or *bi-directional*, where for example a vehicle responds to RSU probes or, an interactive protocol is run between the vehicle and the RSU for updating the vehicle's list of pseudonyms. At the link layer, *V2I* communication can be either one-hop or multi-hop, where vehicles can also route information towards the RSUs if needed.

C. Threat model

The adversary is modeled as a traditional *Byzantine* adversary [15], *i.e.*, is able to observe (eavesdrop) or tamper (modify) the contents of the communication channels, provide inputs to honest parties and observe their outputs, and coordinate the actions of all corrupted parties. All components of the VANET (the vehicles, the RSUs, and the RA) including the adversary are modeled by probabilistic, polynomial-time Turing machines.

In this paper we consider a *privacy* adversary, that is a *global passive observer* that monitors communications within the VANET to extract or infer private information. This information may be used to link past and future message exchanges in order to track vehicles. To facilitate tracking, the adversary may compromise some vehicles and RSUs, and extract their logs. We allow for insider attacks (in which some RSU's may get compromised), but assume that the RA is a trusted entity, that cannot be compromised.

D. Privacy and unlinkability

We shall consider privacy threats involving communication with both, other vehicles and the road infrastructure. As in ([8], [1], [3]), our privacy protection mechanisms will be based on the use of short-lived *pseudonyms* that prevent direct

correlation of broadcast messages. These are anonymous key pairs (PK, SK) for both encryption and signatures, together with the corresponding certificates (*CERT*), issued by the RA and distributed to the vehicle nodes either *statically* or *dynamically*. In the static case ([1], [3]) a number of pseudonym key pairs $\{(PK^j_{V_i}, SK^j_{V_i})\}_{j\in J}$ are pre-loaded to the vehicles V_i offline (*e.g.*, by the manufacturer). In the dynamic case, anonymous key pairs are updated by executing an online protocol between the vehicles and the RSU's [6]. The anonymity gained is conditional, in the sense that the pseudonyms bear information that allows the RA, or a number of cooperating authorities ([8], [9]), to establish accountability against a misbehaving node.

E. Key distribution and management

To establish message authentication and accountability, we require that all messages are digitally signed by vehicular and infrastructural nodes. We leave the exact mechanism of establishing a vehicular Public Key Infrastructure (*PKI*) out of scope of this work, and instead refer the reader to other works on the subject ([2], [16], [10]). In the pairwise and group modes of communication, it is also allowable for nodes to establish symmetric session keys to reduce the overall overhead. Such symmetric keys may subsequently be used to protect the confidentiality of the exchanged messages. However we require that established keys are not used for message authentication, as this would weaken the non-repudiation requirement.

IV. Privacy-preserving protocols for VANETs

A. V2V privacy-preserving protocols

Heart-beat communication: Throughout this section we follow the notation used in [3]. We assume that when a vehicle V detects the presence of a new neighbor V^* at the link layer, it broadcasts its encryption certificate $CERT^e_V$, *i.e.*, a public encryption key and the corresponding signature of the RA. Before V^* sends a safety or traffic related message M^*, it signs this with its private signature key $SK^s_{V^*}$ attaches the corresponding signature certificate, and encrypts these with the public encryption key of the receiver PK^e_V. Thus, the exchanged messages should contain at least:

$$V \rightarrow * : CERT^e_V$$

$$V^* \rightarrow V : \{SIG_{SK^s_{V^*}}(M^*||T^*), CERT^s_{V^*}\}_{PK^e_V}$$

where T^* is a timestamp, "||" is concatenation, $SIG_{SK^s_{V^*}}(M^*||T^*)$ is the string consisting of consists of $M^*||T^*$ in cleartext followed by a signature on the hash of $M^*||T^*$ with the private signature key $SK^s_{V^*}$, $CERT^s_{V^*}$ is the signature certificate of node V^*, and $\{\}_{PK^e_V}$ represents encryption with the public key of V.

In a typical 3-step extension of the protocol for *mutual* heart-beats, vehicle V^* would also encapsulate its encryption certificate in the second step, in order for vehicle V to submit its own heart-beat, as shown next:

$$V \rightarrow * : CERT^e_V$$

$$V^* \rightarrow V : \{SIG_{SK^s_{V^*}}(M^*||T^*), CERT^s_{V^*}, CERT^e_{V^*}\}_{PK^e_V}$$

$$V \rightarrow V^* : \{SIG_{SK^s_V}(M||T), CERT^s_V\}_{PK^e_{V^*}}$$

where $M||T$ is a heart-beat message and timestamp of V.

Pairwise keys: We assume that each vehicle will broadcast its encryption certificate when it detects a new neighbor. Vehicles V and V^* establish a symmetric secret key K as follows. One of the vehicles, say V^*, chooses a random key K, appends a timestamp T^* and signs the message with its private signature key $SK^s_{V^*}$. It then sends the result to V, encrypted with its public encryption key PK^e_V. V decrypts the message, verifies the signature to obtain the session key K, then confirms the receipt of the session key by signing an acknowledgement with its private signature key SK^s_V, appends its certificate $CERT^s_V$ and returns the result encrypted with the session key K. The protocol should thus contain at least the following messages:

$$V \rightarrow * : CERT^e_V,$$

$$V^* \rightarrow V : \{SIG_{SK^s_{V^*}}(K||T^*), CERT^s_{V^*}\}_{PK^e_V}$$

$$V \rightarrow V^* : [SIG_{SK^s_V}(K||T), CERT^s_V]_K,$$

where $[\,]_K$ denotes encryption with the symmetric key K. On completion of the key transfer protocol, vehicles V and V^* will be able to further communicate with message authentication and secrecy. For example vehicle V^* can send privately to V the authenticated message M^* with a timestamp T^* as follows:

$$V^* \rightarrow V : [SIG_{SK^s_{V^*}}(M^*||T^*)]_K$$

Group keys: We assume that a group leader vehicle L periodically broadcasts its encryption certificate. All other members V_i, $i = 1, 2, \ldots, m$, of the group return their encryption certificates $CERT^e_{V_i}$ encrypted with the public key of the group leader, PK^e_L, who then chooses a (random) group session key K, signs it with its private signature key SK_L and transmits this privately to the group members. The protocol should contain at least the following messages:

$$L \rightarrow * : CERT^e_L$$

$$V_i \rightarrow L : \{CERT^e_{V_i}\}_{PK^e_L}$$

$$L \rightarrow V_i : \{SIG_{SK_L}(K||T), CERT^s_L\}_{PK^e_{V_i}}$$

where $PK^e_{V_i}$ is the public encryption key of vehicle V_i and T a timestamp.

B. V2I privacy-preserving protocols

Heart-beat communication: We assume that each RSU periodically broadcasts its encryption certificate $CERT^e_{RSU}$. As in the *V2V* setting, a vehicle V signs a safety or traffic-related message M with its private signature key SK^s_V, appends its certificate $CERT^s_V$ and then encrypts the result with the public key PK^e_{RSU} of RSU:

$$RSU \rightarrow * : CERT^e_{RSU}$$

$$V \rightarrow RSU : \{SIG_{SK^s_V}(M||T), CERT^s_V\}_{PK^e_{RSU}}$$

We assume that if the RSU is not in the wireless range of V, other vehicles in the vicinity of V will relay heart-beat messages to RSU in multi-hop mode.

Certificate update: Vehicle V detects the presence of an RSU, then constructs a message $M = \{PK^e_{Vj}||PK^s_{Vj}\}_{j\in J}$ that contains a set of new encryption and signature pseudonyms. Vehicle V then signs the request for updating its pseudonyms with its private signature key SK^s_V and encrypts the result with the public encryption key of the RSU, PK^e_{RSU}. The RSU forwards the request to an online RA which signs the pseudonyms with its private signature key SK^s_{RA}, and sends them via the RSU to V encrypted with its public key, PK^e_{RSU}:

$$RSU \rightarrow * : CERT^e_{RSU}$$

$$V \rightarrow RSU : \{SIG_{SK^s_V}(M||T), CERT^s_V, CERT^e_V\}_{PK^e_{RSU}},$$

$$RSU \rightarrow V : \{SIG_{SK^s_{RA}}(CERT^s_{Vj}||CERT^e_{Vj}||T)\}_{PK^e_V}$$

V. Security and performance

In the *V2V* and *V2I* protocols of Section IV, the vehicles are equipped with short-lived pseudonyms for both encryption and digital signing. The protocols make use of typical public key and symmetric cryptosystems, for example with key sizes of $\ell = 1024$ and $t = 128$ bits respectively. The candidates could be: the ElGamal scheme [19] for public key encryption, the DSA algorithm for creating and verifying digital signatures, the AES encryption scheme for symmetric encryption and a hash function in the SHA family of functions.

For authentication, messages are digitally signed by the vehicular nodes, and the receivers are able to corroborate any legitimate message to an authorized pseudonym. We assume that there is a mechanism by which a pseudonym can be later traced back (*e.g.*, by the RA) to a true identity (*e.g.*, by using forensic evidence). We omit further discussion on this issue since it is not a key factor in our analysis.

Freshness and liveness is assured by incorporating timestamps in the signed messages. Alternatively, the protocols can be easily adapted to support challenge-response mechanisms with random nonces. We assume the underlying primitives are secure.

Our *V2V* and *V2I* protocols for heart-beat, pairwise and group communication extend the protocols discussed in ([1], [3], [13]). Privacy is *strengthened* by requiring the encryption, when possible, of all identifying information (*i.e.*, pseudonyms and signatures) with a (semantically) secure encryption scheme. In this way privacy is strengthened, and the requirement that a pseudonym needs to be changed at the end of each session is relaxed. Below we discuss the implication of this strategy for the performance of the system. In Section VI, we elaborate on the privacy criterion and argue that updating a pseudonym is not always enough to establish unlinkability for a given node.

Performance analysis

As discussed in Section IV, at the beginning of each session, every vehicle that responds (*i.e.*, *a responder*) to a hello message encrypts its credentials and authorized pseudonym, timestamp and other traffic data with the public key of *the initiator* of the session. If nodes are engaged in further conversation, a symmetric session key K is established and from that point all authentic messages are encrypted with the established key K.

Our solution, compared with related work in the field (*e.g.*, [1], [3], [13]), minimizes the overhead of the pseudonym changing/updating subtasks, since a responder in a session does not have to change its pseudonym in the following session. This has an implication in terms of storage, communication and computation. In static schemes for example, the cost of storing a large number of pre-loaded pseudonyms is reduced significantly, *i.e.*, the key set size per user is reduced by half, on average, compared with the key set size in [3]. On the other hand, in dynamic schemes the communication cost is also kept low since the node is not involved in a large number of interactive protocols with RSUs for updating its pseudonyms.

Communication: In the *V2V* heart-beat mode, each vehicle sends information with a minimum size of $6\ell + m + t$ bits, where t is the length of the timestamp, m is the length of the message to be sent and 6ℓ is computed as follows (*e.g.*, concerning node V): 2ℓ for the certificate $CERT^e_V$, ℓ for $SIG_{SK^s_V}$, 2ℓ for $CERT^s_V$, and ℓ for encryption with $PK^e_{V^*}$. Similarly, in the pairwise key establishment protocol the vehicle V sends $5\ell + 2t$ bits of information, while in the group key transfer protocol the cost is $k \times 3\ell$ for the group of k vehicles and $k \times (4\ell + 2t)$ for the group leader.

In the *V2I* heart-beat mode, the cost for V is $4\ell + m + t$ while the cost for the RSU is 2ℓ bits. Similarly, the cost for V in the certificate update is $6\ell + t + (J \times 2\ell)$, where J is the number of pseudonyms that V requests to be registered.

Computation: All messages in the *V2V* and *V2I* protocols are digitally signed and accompanied by the corresponding signature certificate. Thus, each vehicle performs at least two public-key operations for the creation and verification of a digital signature in each session. To enhance privacy, signed messages and corresponding certificates are encapsulated into an encrypted message. Encryption can be either asymmetric

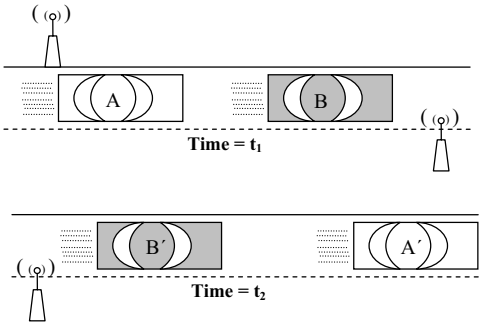

Fig. 1. Linkability in a road without junctions

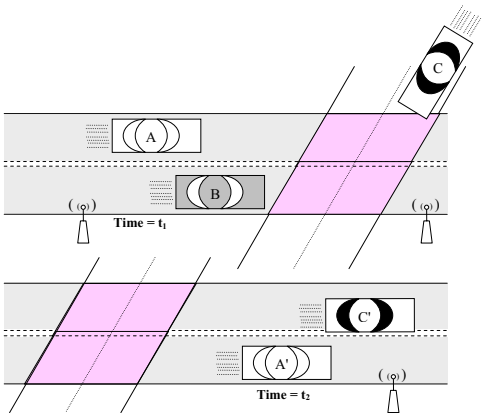

Fig. 2. Unlinkability in a road with junctions

(in heart-beat mode and pseudonym update) or symmetric (in group/pairwise communication). These costs may be justified in VANETs, where vehicles are considered energy-rich nodes. Elliptic Curve Cryptography (ECC) [20] could also offer equivalent security with substantially smaller keys *e.g.*, a 160-bit key is expected to offer comparable security with an RSA 1024-bit key.

VI. Privacy and traffic analysis

In our threat model, the adversary has access to all the wireless traffic of the VANET and can use this information to conduct a traffic analysis and trace a particular vehicle or a group of vehicles, thus compromising their privacy. The intercepted messages of vehicles can be linked to the RSUs that received them, thus making it possible to estimate the location of each vehicle and reconstruct the route taken. Ultimately, the only strategy available for a vehicle to avoid being traced is to make itself indistinguishable from other vehicles by '*hiding in the crowd*'.

Several mechanisms have been proposed in the literature to implement this approach (*e.g.*, [1], [17]). In these, vehicles use pseudonyms that are regularly updated based on spatial and/or temporal criteria. Clearly there are situations when such an approach cannot provide unlinkability. For example, on a clear stretch of road with no junctions, a vehicle can always be linked to its group, however many times it changes its pseudonym—see Fig. 1. The same applies to stationary vehicles, or to vehicles traveling at constant speed. In general, privacy can only be supported for moving vehicles while they cross a *Junction Point* (*JP*) or crossroads, as other vehicles enter or exit the junction. The scattering of vehicles makes it harder to identify the routes that vehicles take—see Fig. 2.

Random silence has also been proposed as a mechanism to protect the privacy of vehicles (*e.g.*, [4], [18]): in this approach a vehicle does not transmit any messages while it is traversing a *silent zone*. Assuming the silent period is random, it should be hard to link the vehicles exiting the silent zone from those entering it. However these mechanisms are subject to a Bayesian traffic analysis in which the adversary can link vehicles exiting a silent zone to those that have entered it by using information regarding the prior state of the system. Observe that random silence defeats the operations goal of VANETs and must therefore be restricted to short periods.

A. Bayesian estimators

Bayesian analysis uses probability and statistical methodology to estimate a distribution outcome, based on an observed (a priori) distribution. For our traffic application, this involves assessing the most likely outcome of a vehicle identification procedure, given prior traffic observations. A Bayesian estimator is a decision rule that maximizes (or minimizes) the a posteriori expectation of a utility (or loss) function.

Consider the following basic example. Suppose that vehicles $V_1, V_2, \ldots, V_m$ enter a silent zone at entry points $P_1, P_2, \ldots, P_m$ (not necessarily distinct) at time $t_1, t_2, \ldots, t_m$ with speed $v_1, v_2, \ldots, v_m$, respectively, and that vehicle W exits at point P at time $t > t_i$, $i = 1, 2, \ldots, m$. Then, if R_i is the set of all routes that link P_i to P, the conditional probabilities, $\mathrm{Prob}\,[W = V_i \mid \{P_j, t_j, v_j, R_j\}_{j=1,\ldots,m}; P, t]$, can be used to link the vehicles that exit a silent zone to those that have entered it. In our case we may take the likelihood that $W = V_i$ to be

$$p_i = \frac{a}{1 + min_{r_i^k \in R_i} |t - t_i - t_i^k|} \ ,$$

where t_i^k is the time that V_i would take to reach the exit point P if it used route $r_i^k \in R_i$ with speed v_i, and a is such that $\sum p_i = 1$. (Note that if V_i actually uses route r_i^k, then $t - t_i = t_i^k$ and $|t - t_i - t_i^k| = 0$.)

For a more interesting estimator we may use a decision rule that optimizes the expectation taken over m vehicles $W_1, W_2, \ldots, W_m$ that exit the silent zone. This would involve probabilities $\mathrm{Prob}\,[V_i = W_j]$ and the optimization of sums $\sum_{i=1,\ldots,m;\pi \in S_m} (\mathrm{Prob}\,[V_i = W_{\pi(i)}])^2$, where S_m is the symmetric group on $\{1, 2, \ldots, m\}$ and $\pi \in S_m$. As in the previous case we could use,

$$p_{i,j} = \frac{a}{1 + min_{r_{i,j}^k \in R_{i,j}} |t_j' - t_i - t_{i,j}^k|} \ ,$$

as an estimator for $\mathrm{Prob}\,[V_i = W_j]$, where $R_{i,j}$ is the set of all routes that link the entry point of V_i to the exit point of W_j, t_j' is the time that W_j exits the silent zone, and $t_{i,j}^k$ is the time that V_i would take to reach the exit point of W_j if it

were to use route $r_{i,j}^k \in R_{i,j}$ (again $|t'_j - t_i - t_{i,j}^k| = 0$ if V_i uses route $r_{i,j}^k$).

These are rather simple estimators that do not fully exploit the prior distribution of the traffic. For instance the speed v_i of vehicle V_i is not usually constant, and should be treated as a stochastic parameter. Earlier traffic observations can be used to get an approximation of its distribution.

Clearly with any such Bayesian analysis the primary constraints that make it hard to disambiguate vehicles are the complexity of the road topology, the traffic density, the vehicle proximity and the unpredictable behavior of drivers.

B. Privacy based on road complexity

Our approach to privacy for vehicles in a VANET combines the 'hiding in the croud' and 'random silence' strategies, and is based on the complexity of the road topology. Privacy (unlinkability) can only be guaranteed if the route taken by a vehicle crosses several *JP*s and the local traffic conditions make it hard to link the vehicles that exit a junction from those that have entered it. For this purpose, pseudonyms are only updated when a vehicle crosses a *JP*, during which a short period of silence is observed.

VII. Discussion

VANETs can be seen as one of the most promising implementations of MANETs, and it is expected that they will develop rapidly, as they gain increased attention from both academia and the industry. For VANETs to become a reality, a number of security issues need to be addressed. Research in VANET security has focused on privacy-preserving solutions that also establish accountability for misbehaving vehicles. Another important issue is whether privacy can be protected against a global adversarial observer who performs traffic analysis in order to link messages to specific vehicles in motion.

In this paper we presented mechanisms for balancing the tradeoff between privacy and accountability in VANETs. We considered both *V2V* and *V2I* communication for heart-beat messages or for updating a vehicle's pseudonym list. For non-repudiation and privacy, we required that all messages are digitally signed by sending vehicles, and then encrypted with the public key of the intended receiver. We believe that in this way privacy is strengthened and moreover the efficiency of changing pseudonyms becomes optimal (pseudonyms are not changed at the beginning of each session but only when needed). For a more permanent relationship, we also described mechanisms for establishing symmetric session keys in pairwise or groupwise *V2V* communications.

Furthermore, we elaborated on the unlinkability aspect privacy and showed how privacy preserving mechanisms and the changing of pseudonyms can often be defeated by adversaries who perform a Bayesian traffic analysis. To this end we proposed a specific strategy to strengthen unlinkability in VANET communication: vehicles that cross a junction point or a crossroads stay silent for short random periods, during which they also change their pseudonym.

While in its infancy, research in VANET security must be pursued, and practical solutions that balance the tradeoff between efficiency and security must be sought.

References

[1] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *SASN '05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*. New York, NY, USA: ACM, 2005, pp. 11–21.

[2] P. Papadimitratos, A. Kung, J.-P. Hubaux, and F. Kargl, "Privacy and identity management for vehicular communication systems: a position paper," in *Workshop on Standards for Privacy in User-Centric Identity Management*, 2006.

[3] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[4] K. Sampigethaya, L. Huang, K. Matsuura, R. Poovendran, and K. Sezaki, "Caravan: Providing location privacy for vanet," in *Escar 2005: 3rd Embedded Security in Cars Workshop*, 2005.

[5] J. Blum and A. Eskandarian, "The threat of intelligent collisions," *IT Professional*, vol. 6, no. 1, pp. 24–29, Jan.-Feb. 2004.

[6] B. Parno and A. Perrig, "Challenges in securing vehicular networks," *Workshop on Hot Topics in Networks (HotNets-IV)*, 2005. [Online]. Available: http://sparrow.ece.cmu.edu/ parno/pubs/vehicles.pdf

[7] P. Papadimitratos, V. Gligor, and J. Hubaux, "Securing Vehicular Communications - Assumptions, Requirements, and Principles," in *Workshop on Embedded Security in Cars (ESCAR) 2006*, 2006.

[8] J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing auditability and privacy in vehicular networks," in *Q2SWinet '05: Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*. New York, NY, USA: ACM, 2005, pp. 79–87.

[9] J. Sun, C. Zhang, and Y. Fang, "An id-based framework achieving privacy and non-repudiation in vehicular ad hoc networks," *Military Communications Conference, 2007. MILCOM 2007. IEEE*, pp. 1–7, 29-31 Oct. 2007.

[10] S. Rahman and U. Hengartner, "Secure crash reporting in vehicular ad hoc networks," in *Third International Conference on Security and Privacy in Communication Networks (SecureComm 2007)*. New York, NY, USA: To appear, 2007.

[11] P. Cencioni and R. Di Pietro, "Viper: A vehicle-to-infrastructure communication privacy enforcement protocol," *IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems, 2007. MASS 2007.*, pp. 1–6, 8-11 Oct. 2007.

[12] M. Raya, A. Aziz, and J.-P. Hubaux, "Efficient secure aggregation in vanets," in *VANET '06: Proceedings of the 3rd international workshop on Vehicular ad hoc networks*. New York, NY, USA: ACM, 2006, pp. 67–75.

[13] N.-W. Wang, Y.-M. Huang, and W.-M. Chen, "A novel secure communication scheme in vehicular ad hoc networks," *Computer Communications, Elsevier*, 2008.

[14] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976. [Online]. Available: citeseer.ist.psu.edu/diffie76new.html

[15] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, pp. 198–207, 1983.

[16] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *Selected Areas in Communications, IEEE Journal on*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.

[17] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in vanets," in *ESAS*, 2007, pp. 129–141.

[18] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," *Wireless Communications and Networking Conference, 2005 IEEE*, vol. 2, pp. 1187–1192 Vol. 2, 13-17 March 2005.

[19] T. E. Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Proceedings of CRYPTO 84 on Advances in cryptology*. New York, NY, USA: Springer-Verlag New York, Inc., 1985, pp. 10–18.

[20] SECG, "Standards for efficient cryptography group. SEC 1: Elliptic curve cryptography," Available at: http://www.secg.org/download/aid-385/sec1_final.pdf, 2005.