Aggregation of Trustworthy Announcement Messages in Vehicular *Ad Hoc* Networks

Alexandre Viejo*†, Francesc Sebé† and Josep Domingo-Ferrer†
*Institute of Information Systems, Humboldt-Universität zu Berlin
Spandauer Str. 1, D-10178 Berlin, Germany
Email: alexandre.viejo@wiwi.hu-berlin.de
†Rovira i Virgili University, Department of Computer Engineering and Mathematics,
UNESCO Chair in Data Privacy, Av. Països Catalans 26, 43007 Tarragona, Catalonia, Spain
Email: {alexandre.viejo, francesc.sebe, josep.domingo}@urv.cat

***Abstract*—Vehicular ad hoc networks (VANETs) allow vehicle-to-vehicle communication and, in particular, vehicle-generated announcements. Vehicles can use such announcements to warn nearby vehicles about road conditions (traffic jams, accidents). Thus, they can greatly increase the safety of driving. However, their trustworthiness must be guaranteed. A new system for vehicle-generated announcements is presented that is secure against external and internal attackers attempting to send fake messages. Internal attacks are thwarted by using an endorsement mechanism based on multisignatures. Besides, this scheme ensures that vehicles volunteering to generate and/or endorse trustworthy announcements do not have to sacrifice their privacy.**

***Index Terms*—Aggregation, Multisignatures, Privacy, Security, Vehicular communications.**

I. Introduction and previous work

Vehicular *ad hoc* networks (VANETs) are formed by mobile nodes embedded in vehicles which are connected in a self-organized way without an underlying hierarchical infrastructure.

VANETs permit a vehicle to warn other vehicles about road conditions (traffic jams, accidents) so that the latter can take advantage of that information to select routes avoiding troublesome points. We name this kind of messages *announcement messages*.

Announcement messages require a long dissemination range. Nevertheless, their requirements regarding real-time processing are not strict. In this way, advanced cryptography can be used to make such messages secure and trustworthy.

Privacy is a key aspect in VANETs. A lot can be inferred on the driver's personality if the whereabouts and the driving pattern of a car can be tracked [1]. There are two layers of privacy: *anonymity* and *unlinkability*. A system preserves anonymity when it does not require the identity of its users to be disclosed. Unlinkability refers to the fact that different interactions of the same user with the system cannot be related. Unlinkability prevents user tracking and profiling.

Security in car-generated announcements sent over a VANET is fundamental. It is important that the system does not permit an intruder (external attacker) or a dishonest driver (internal attacker) to insert fake announcements or modify announcements sent by others. These attacks can seriously disrupt traffic or cause dangerous situations for other vehicles.

Security against external attackers is easy to achieve by requiring the sender of a message to access some secret key material only available to legitimate users (obviously, that key material is unavailable to external attackers).

On the other hand, dealing with internal attackers is a challenging problem. The reason is that legitimate users, and thus internal attackers, have access to the secret key material required to send authenticated fake messages. There are two classes of countermeasures against fake messages sent by internal attackers: *a posteriori* countermeasures and *a priori* countermeasures.

A posteriori countermeasures consist of taking punitive actions against users who have been proven to have originated fake messages (*e.g.* the offenders can be banished from the network). These countermeasures in anonymous systems require the presence of a trusted third party (TTP) able to revoke the key material of such dishonest users. In this way, they will be excluded from the system. There are several proposals in literature which rely on *a posteriori* countermeasures [2], [3], [4], [5], [6], [7].

A priori countermeasures attempt to prevent the generation of fake messages. According to that, this approach is compatible with driver privacy: false announcements are thwarted without resorting to punitive actions. Therefore, unconditional vehicle anonymity is allowable.

In a scheme based on *a priori* countermeasures, a certain announcement needs to be endorsed by a certain number of vehicles before being considered as valid. Those endorsers must be in a position to confirm what is reported in the announcement. This approach is based on the assumption that most users are honest and will not endorse any message containing false data. The use of a honest majority to prevent generation of fake messages has previously been proposed in [8], [9], [10], [11], [12].

In [8] a framework is presented to validate received data in VANETs. In this approach, a vehicle receives alerts from several neighbors and compares them in order to infer the correctness of a certain event. This scheme suffers from high communication overhead due to the lack of aggregation

978-1-4244-2517-4/09/$20.00 ©2009 IEEE

techniques. The paper [9] presents a system that evaluates the plausibility of received danger warnings. This system estimates the trustworthiness of a reported hazard by taking a vote on the received danger messages. The paper provides a simulative analysis of different voting schemes, but privacy remains unaddressed and security is not completely covered. In [10] an emergency message authentication scheme is presented to validate emergency events. This proposal makes use of cryptographic aggregation techniques to reduce the transmission cost. It also uses a batch verification technique for efficient verification of emergency messages. This proposal relies on vehicles forming clusters. The vehicle at the head of every cluster is responsible for aggregating and forwarding the data to the next cluster. This approach works fine in a highway scenario where vehicles traveling on the same directed pathway can form interconnected blocks of vehicles which travel together for a significant period of time [13]. However, in less deterministic scenarios (*e.g.* a city) where natural clusters frequently change, this proposal suffers from high overhead [14]. We present a system for vehicle-generated announcements in [11]. This scheme uses an endorsement mechanism based on threshold signatures which prevents internal attackers from attempting to send fake messages. Three different privacy-preserving variants of the system are also described to provide message trustworthiness and vehicle unlinkability under different road conditions (both deterministic and non-deterministic environments). Anonymity is achieved by using pseudonyms. In order to be deployed in a real scenario, this proposal requires a trusted governmental authority and the existence of agreements between the different carmakers in a certain geographical area (carmakers are involved in key management). These requirements can be easily satisfied in well-organized and developed areas. However, other areas may require a protocol with a more straightforward deployment. Finally, [12] describes a detailed protocol with relaxed requirements regarding its deployment. This proposal systematically deals with security threats and reduces communication overhead by aggregating messages. This scheme can be used in both deterministic and non-deterministic environments.

Three variants offering *a priori* countermeasures against fake messages are presented in [12]: *concatenated signatures*, *onion signatures* and *hybrid signatures*. In the variant based on *concatenated signatures*, a vehicle generates an announcement and sends it, its signature and its public-key certificate to a nearby car which will endorse it by computing its own signature on it. This new signature and the corresponding public-key certificate will be appended to the frame that will be retransmitted to the next vehicle. An announcement is considered valid after it has been endorsed by at least the number of vehicles determined by the threshold. This approach has two main drawbacks:

- It does not offer unlinkability since different signatures made by the same user can be linked through the public key that verifies them. Anonymity is however feasible by using pseudonyms.
- It requires the verifier to check several signatures upon receiving an announcement (as many verifications as vehicles have endorsed the message).

Therefore, there is room for improvement both in terms of privacy and efficiency (communication and computation costs) while keeping a straightforward deployment.

The variants based on onion signatures and hybrid signatures are similar and designed to reduce the overall message length. Both variants use the so-called *oversignatures*: instead of appending its signature, each new endorsing car signs the signature by the previous endorsing car (this is called oversigning). As a result of this process, the verifier receives a message with the following structure

$$\{m, S_{n-1}, S_n(\dots(S_1(m))), C_1, \dots, C_n\},$$

where m stands for the announcement, S_i stands for the signature issued by vehicle i and C_i corresponds to the public key certificate of vehicle i.

In an oversignature, a verifier can check the last endorser's signature, but not the signatures by the previous endorsers. We argue that this is a serious design flaw. Thus, we will only consider the *concatenated signatures* variant in the rest of our paper.

A. *Contribution and plan of this paper*

In this work, a proposal is presented following the *a priori* protection paradigm. This scheme is suitable for deployment in both deterministic (*e.g.* a highway) and non-deterministic (*e.g.* a city) scenarios. This proposal outperforms [12] by reducing the length of announcements while keeping a straightforward deployment. This reduction is achieved by using a multisignature instead of a concatenation of signatures. The proposed system uses a mechanism to provide unlinkability to the vehicles. Anonymity is achieved by using pseudonyms. Note that the unlinkability level achieved by this scheme is not so good as the one provided by [11]. However, this new proposal improves on [11] in the following aspects:

- Our proposal minimizes the carmakers' responsibility: unlike in [11], carmakers are not involved in key management, so that no agreement is required between the carmakers selling cars in a certain geographic area.
- The trusted governmental authority assumed in [11] can be replaced by a standard certification authority able to deliver smart cards to the carmakers.

This paper is structured as follows. Section II presents some background on public key cryptography over Gap Diffie-Hellman groups. Section III describes the new scheme. Section IV studies the proposed protocol using simulations. Finally, conclusions are summarized in Section V.

II. Cryptography over Gap Diffie-Hellman groups

The construction we propose uses multisignatures over a Gap Diffie-Hellman group [15]. Next, we briefly introduce its mathematical background. A Gap Diffie-Hellman (GDH) group G is an algebraic group of prime order q for which no efficient algorithm can compute g^{ab} for random $g^a, g^b \in G$, but such that there exists an efficient algorithm $D(g^a, g^b, h)$ to decide whether $h = g^{ab}$. GDH groups are suitable for public-key cryptography. The secret key is a random value $x \in \mathbb{Z}_q$ and its corresponding public key is $y \leftarrow g^x$. The signature on a message m is computed as $\sigma \leftarrow \mathcal{H}(m)^x$ ($\mathcal{H}$ is a cryptographic one-way hash function). In the rest of the paper we will denote such a signature on m as $\{m\}_x$. The validity of a signature can be tested by checking $D(y, \mathcal{H}(m), \sigma)$.

GDH groups are convenient to compute multisignatures. Given two signatures of the same message m under two different public keys y_1, y_2, a signature of m under the combined public key $y \leftarrow y_1 \cdot y_2 = g^{(x_1+x_2)}$ can be obtained as $\mathcal{H}(m)^{x_1} \cdot \mathcal{H}(m)^{x_2} = \mathcal{H}(m)^{x_1+x_2}$.

III. Our proposal

Our system requires a trusted Certification Authority CA to generate public/private key pairs (PK/SK). It also requires the CA to deliver smart cards to the carmakers. Secret keys are always held in smart cards. Note that the CA is no longer needed when executing the proposed protocol.

In our scheme, an announcement will only be considered valid if it has been endorsed by at least t different vehicles.

We next detail how our protocol works. Later, we will discuss its security and privacy properties.

A. Protocol steps

- *Set-up:* When each car P_i is manufactured by a carmaker, it receives d different public/private key pairs $(PK_{i,1}/SK_{i,1}, \ldots, PK_{i,d}/SK_{i,d})$. The on-board computer in P_i stores the d public keys (and their digital certificates) while the d private keys are held in a smart card plugged into the vehicle (tamper-resistance is assumed for the card in what follows). On input of a hash value $\mathcal{H}(m)$ of a message m, the smart card returns a signature on that hash value issued under one of the private keys held by the card, that is, $\sigma_i(m) = \mathcal{H}(m)^{SK_{i,j}}$, where $j \in 1, \ldots, d$. The private key $SK_{i,j}$ is selected following a procedure detailed in Section III-A1.
  Anonymity is obtained by not linking the private key $SK_{i,j}$ with the identity of vehicle P_i; this makes sense for other reasons too because, smart cards being removable, several smart cards each holding a different secret key share could alternatively be used with the same vehicle (like several cards can be used with a cellphone).
- *Request for endorsement:* When a vehicle P_i wishes to warn other cars about a certain event e, it does the following:
  1) P_i constructs message m which contains the event and a timestamp indicating the moment when e has been observed:

  $$m \longleftarrow \{e \mid\mid TimeStamp\}$$

  2) P_i computes signature $\sigma_i(m)$ and broadcasts m and $\sigma_i(m)$. We name this transmission *request for endorsement.*

  A *request for endorsement* should only reach vehicles which are close enough to the originating vehicle so as to be able to check the validity of the announced condition. Since they do not need to reach distant points, *request for endorsement* messages are not relayed by VANET nodes and they travel only up to the range of the broadcast technology used (typical ranges from 300 to 500 meters on highways and about 100 meters in cities are mentioned in [16]).
- *Announcement endorsement:* When vehicle P_w receives a *request for endorsement* from P_i, first of all it uses the timestamp embedded in m to check whether the announcement is up-to-date. If that is the case and P_i wishes to endorse e, then it does:
  1) P_w computes its own signature on m, that is, $\sigma_w(m) = \mathcal{H}(m)^{SK_{w,j}}$.
  2) P_w sends back to P_i its signature $\sigma_w(m)$, together with the corresponding public key $PK_{w,j}$ and its digital certificate.
- *Signature composition:* Once P_i (the vehicle which launched the request for endorsement) collects $t-1$ answers, it aggregates the $t-1$ received signatures in a final signature σ_f:

  $$\sigma_f(m) = \prod_{a=1}^{t-1} \sigma_a(m)$$

  Then, P_i aggregates its own signature to the final signature: $\sigma_f(m) \longleftarrow \sigma_f(m) \cdot \sigma_i(m)$ and generates a final announcement α which is endorsed by t different vehicles:

  $$\alpha \longleftarrow \{m,\ (PK_{1,j}, \ldots, PK_{t,j}),\ \sigma_f(m)\}$$

  Finally, P_i broadcasts α to nearby cars. Each vehicle receiving α broadcasts it to its neighbours too. In this way, α will reach distant vehicles which will benefit from the information it conveys.
  Besides, vehicles can deduce from the timestamp embedded in the announcement how critical the received announcement is and whether it needs to be further broadcast or not. If the timestamp shows that m was generated long time ago, the announced event e is probably outdated and can be discarded.
- *Announcement reception and verification:* Vehicles in the VANET will only consider as trustworthy those announcements α carrying a recent timestamp and a multisignature issued by t vehicles that can be verified using the embedded public key chain $(PK_{1,j}, \ldots, PK_{t,j})$. Each public key can be verified using its digital certificate.

The reason for keeping the chain of secret keys $(SK_{i,1}, \ldots, SK_{i,d})$ in a smart card is to prevent the vehicle driver from using all of them to sign a certain announcement. If this situation was possible, an honest user would not be able to differentiate a signature issued by two different users from a signature issued with two secret keys from the same user. If $d >= t$ (which is very likely to happen), this situation would allow a single user to sign messages that would be accepted as trustworthy without any endorsement. If $d < t$, the endorsements needed to validate a certain announcement would be reduced to $t - d$. Obviously, this would affect the trustworthiness of any announcement.

1) Selecting the private key in use: The smart card embedded in each vehicle keeps d secret keys $(SK_{i,1}, \ldots, SK_{i,d})$. One of them is selected at random to sign the next n messages. If the smart card needs y milliseconds to generate a signature, this process guarantees that the same key will be used during a minimum period of $n \cdot y$ ms. Therefore, users cannot obtain two or more signatures issued under different secret keys at once. Instead of that, they have to wait until the corresponding periods of time expire. This prevents a dishonest user from generating by herself a *up-to-date* trustworthy message without any endorsement from other users. Note that a dishonest user who waits long enough can still generate an apparently trustworthy message (in the sense that it is endorsed by different secret keys all belonging to the same user). However, this process requires some time and the announcement is very likely become outdated in the meantime. Honest users will be able to discard this fake announcement by checking the timestamp embedded in it.

The cryptographic calculation progresses according to an externally supplied, and therefore untrusted, clock signal, which an attacker might accelerate (overclocking attack) in the hope of getting a faster response. We assume that the smart card has no built-in high-precision time base. Nevertheless, it is able to detect significant deviations from its nominal clock frequency [17]. Thus, this attack can be overcome.

Regarding the average time y required to sign a hash value, [18] states that this is a value between 55 and 514 ms. Obviously, this value is related to the computating power of the smart card in use. However, smart cards used by the vehicles are provided by a certification authority (carmakers install the smart cards provided by this entity), so we can assume that the average time required to sign a message is known. According to that, n can be fixed to obtain the desired period of time between each change of secret key.

B. Trustworthiness, privacy and availability

The choice of t is a trade-off between trustworthiness and availability. On one hand, t should be high enough so that the probability of there being t or more within-range colluding vehicles who could validly endorse fake messages is reasonably low (trustworthiness). On the other hand, t should not be so high that finding $t - 1$ additional within-range endorsers is too difficult for an honest announcement generator (availability).

Unlinkability is related to parameter d, the number of private keys which each user keeps in her smart card. Each secret key is selected at random and it is used to sign all the announcements issued in a certain period of time. It means that during that period, all announcements are easily linked to the same user (they are all issued with the same key). Nevertheless, when this period expires the key is changed. According to that, the probability that two participations by P_i in two different periods can be linked is $1/d$ (this happens if the same secret key is selected in both cases). Thus, even if not perfect, unlinkability improves with respect to schemes like [10] and [12] which do not provide it in any way.

IV. Simulations

Our scheme was simulated in a realistic environment where the range of car-to-car broadcasts was assumed to be 100 meters (the worst-case, urban range according to [16]). The goal of our simulations was to observe the degree of availability (probability of finding t different vehicles) of our system as a function of vehicle density and the minimum number of validating vehicles t.

A. Simulation set-up

The network simulator *ns-2* [19] was used. The VANET scenario was built using the scenario generator presented in [20]. The road network considered covered an area of 2.4 km by 2.4 km and is shown in Figure 1.

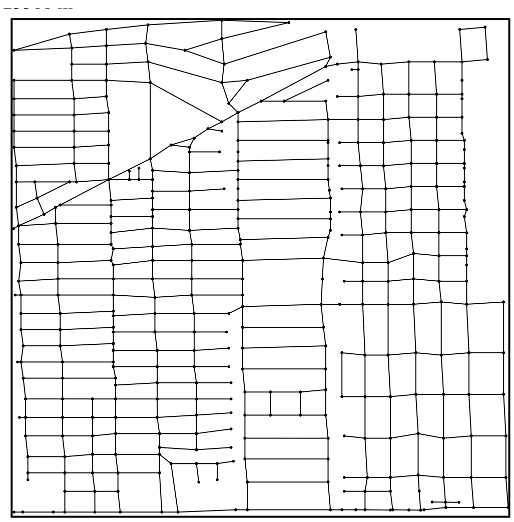

Fig. 1. Simulation scenario

In our simulations, the probability for a certain announcement to get validated is evaluated. An announcement is validated when its endorsed by t different cars.

Vehicle density is expressed in *vehicles/*km^2. This value is changed by varying the total number of vehicles in the scenario represented in Figure 1.

B. Results obtained from the simulations

It can be observed in Table I that validation probability decreases as t increases, no matter whether the VANET is sparse or dense. This is not surprising because validation is ”easier” for smaller t; however, the price paid is that for smaller t the trustworthiness of a validated message is lower. Following this argument, it is also expected that for very sparse networks (vehicle density of 6.94) and high t values (t = 6

TABLE I

AVERAGE VALIDATION PROBABILITY p AS A FUNCTION OF VEHICLE DENSITY AND THE MINIMUM NUMBER OF VALIDATING VEHICLES t.

Vehic. dens.	$t = 4$	$t = 5$	$t = 6$
6.94	0.55	0.36	0.04
8.68	0.66	0.38	0.08
12.15	0.71	0.44	0.31
15.62	0.72	0.48	0.46
17.36	0.76	0.77	0.60
24.31	0.94	0.78	0.83
31.25	0.96	0.92	0.86
38.19	0.96	0.94	0.89
45.14	1.00	0.94	0.92
52.08	1.00	1.00	0.96

for instance) the proposed scheme is unable to work properly (0.04 for a vehicle density of 6.94). As a trade-off between trustworthiness and availability, it is suggested to take $t = 4$ or $t = 5$ depending on the desired trustworthiness level for the announcements. In fact, $t = 5$ is the highest reasonable value because, even though $t = 6$ works fine for dense VANETs (vehicle density above 38.19), it does not for medium-density (0.60 for a density of 17.36) and sparse VANETs. Since a number of endorsers must be chosen which works properly under several road conditions, it is better to select $t < 6$.

All simulations performed reflect that with $t = 4$ our proposal provides message trustworthiness and vehicle unlinkability under different road conditions. Results show that our scheme performs best in medium- to high-density VANETs (densities from 12.15 to 52.08). Nevertheless, it works fair enough in very sparse environments as well:

- For a vehicle density 6.94, our scheme achieves a success probability of 0.55 in announcement validation.
- For a vehicle density 8.68, the success probability increases to 0.66.

The low success in validation for sparse VANETs should be put in context: in an area with very low traffic, it is often less critical to get announcements on road conditions, as there is hardly anyone who can benefit from them.

V. CONCLUSION AND FUTURE RESEARCH

In this paper, a new system has been presented for trustworthy vehicle-generated announcements on VANETs that relies on a priori measures against internal attackers (vehicles in the VANET sending fake messages). Our system uses multisignatures over a Gap Diffie-Hellman group to aggregate announcements and reduce communication overhead. Besides, this proposal is suitable for deployment in both deterministic and indeterministic scenarios and it provides a straightforward deployment.

Regarding privacy, the proposed scheme uses a mechanism to provide some unlinkability to the vehicles. Anonymity is achieved by using pseudonyms. How to further improve unlinkability is a topic for future research.

DISCLAIMER AND ACKNOWLEDGMENTS

The authors are with the UNESCO Chair in Data Privacy, but they are solely responsible for the views expressed in this paper, which do not necessarily reflect the position of UNESCO nor commit that organization. This work was partly supported by the Spanish Government through projects TSI2007-65406-C03-01 ”E-AEGIS” and CONSOLIDER INGENIO 2010 CSD2007-00004 ”ARES”, and by the Government of Catalonia under grant 2005 SGR 00446.

REFERENCES

[1] F. Dötzer, “Privacy issues in vehicular *ad hoc* networks”, *Lecture Notes in Computer Science*, vol. 3856, pp. 197–209, 2006.

[2] M. Raya, P. Papadimitratos, and J.-P. Hubaux, “Securing vehicular communications”, *IEEE Wireless Communications Magazine*, vol. 13, no. 5, pp. 8–15, 2006.

[3] M. Raya and J.-P. Hubaux, “Securing vehicular *ad hoc* networks”, *Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks*, vol. 15, no. 1, pp. 39–68, 2007.

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

[5] F. Armknecht, A. Festag, D. Westhoff and K. Zeng, “Cross-layer privacy enhancement and non-repudiation in vehicular communication”, *4th Workshop on Mobile Ad-Hoc Networks - WMAN*, 2007.

[6] J. Guo, J.P. Baugh and S. Wang, “A group signature based secure and privacy-preserving vehicular communication framework”, *Mobile Networking for Vehicular Environments*, pp. 103–108, 2007.

[7] X. Lin, X. Sun, P.-H. Ho and X. Shen, “GSIS: A secure and privacy preserving protocol for vehicular communications”, *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[8] P. Golle, D. Greene and J. Staddon, “Detecting and correcting malicious data in VANETs”, *Proceedings of the 1st ACM international workshop on Vehicular Ad Hoc Networks*, pp. 29–37, 2004.

[9] B. Ostermaier, F. Dötzer and M. Strassberger, “Enhancing the security of local danger warnings in VANETs - A simulative analysis of voting schemes”, *Proceedings of the The Second International Conference on Availability, Reliability and Security*, pp. 422–431, 2007.

[10] H. Zhu, X. Lin, R. Lu, P.-H. Ho and X. Shen, “AEMA: An Aggregated Emergency Message Authentication Scheme for Enhancing the Security of Vehicular Ad Hoc Networks”,*IEEE International Conference on Communications - ICC’08*, 2008.

[11] V. Daza, J. Domingo-Ferrer, F. Sebé and A. Viejo, “Trustworthy Privacy-Preserving Car-Generated Announcements in Vehicular Ad Hoc Networks”, *IEEE Transactions on Vehicular Technology*, to appear.

[12] M. Raya, A. Aziz and J.-P. Hubaux, “Efficient secure aggregation in VANETs”, *Proceedings of the 3rd International Workshop on Vehicular Ad hoc Networks - VANET’06*, pp. 67–75, 2006.

[13] T. D.C. Little and A. Agarwal, “An Information Propagation Scheme for VANETs”, *IEEE Conference on Intelligent Transportation Systems*, 2005.

[14] P. Basu, N. Khan, and T. Little, “A Mobility Based Metric for Clustering in Mobile Ad Hoc Networks”, *21st International Conference on Distributed Computing Systems*, 2001.

[15] A. Boldyreva. “Efficient threshold signatures, multisignatures and blind signatures based on the Gap-Diffie-Hellman-group signature scheme”, *Lecture Notes in Computer Science*, vol. 2567, pp. 31–46, 2003.

[16] I. Berger, “Standards for car talk”, *IEEE The Institute*, vol. 31, no. 1, Mar. 2007.

[17] G.P. Hancke, M.G. Kuhn, “An RFID Distance Bounding Protocol”, *First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pp. 67–73, 2005.

[18] H. Handschuh, P. Paillier, “Smart Card Crypto-Coprocessors for Public-Key Cryptography”, *Lecture Notes in Computer Science*, vol. 1820, pp. 372–379, 2000.

[19] *The Network Simulator - ns*, http://nsnam.isi.edu/nsnam/index.php/Main_Page

[20] A. K. Saha and D. B. Johnson, “Modeling mobility for vehicular *ad hoc* networks”, in *Proceedings of the 1st International Workshop on Vehicular Ad Hoc Networks-VANET’2004*, ACM: Philadelphia, USA, pp. 91–92, 2004.