

Privacy Consideration for Trustworthy Vehicular Ad hoc Networks

Shabnam Khomejani
Department of Computer Engineering,
Sharif University of Technology,
Kish Island, Iran
Sh_khomejani@yahoo.com

Ali Movaghar
Department of Computer Engineering,
Sharif University of Technology,
Tehran, Iran
movaghar@sharif.edu

Abstract— For increasing safety of driving, intelligent vehicles in vehicular ad hoc networks (VANETs) communicate with each other by sending announcements. The existence of a system that guarantees the trustworthiness of these announcements seems necessary. The proposed approach generating announcements should be preserved from internal and external attackers that attempt to send fake messages. In this paper, we use a group-based endorsement mechanism based on threshold signatures against internal attackers. We choose NTRUSign as a public key cryptosystem for decreasing signature generation and verification times. This approach optimizes the network overhead and consequently its performance. In this scheme, also the privacy of signers and endorsers that generate or endorse trustworthy announcements is preserved.

Keywords- vehicular ad hoc network; threshold signatures; security; privacy; trustworthy announcement

I. INTRODUCTION

Every year, all over the world, many people are injured or killed in car accidents. Hence, the scientists try to employ new technologies and techniques for improving road safety. The analysis of accidents shows, if drivers have correct information about road condition, they can avoid dangers, one way to improve safety is to warn drivers of dangerous situations before drivers observe them.

Intelligent vehicles collect information about their near environment by their onboard sensors, but this information is not enough to warn the driver. Evaluating the road condition, detecting dangerous in a short time and exchanging information through Inter Vehicle Communication (IVC) can be useful [1].

The vehicles and road side units communicate over single or multiple hops in VANETs. A vehicle broadcasts two kinds of messages. A vehicle automatically warns near vehicles about its movement, these messages need very quickly processing (real time) but a limited dissemination that called alert messages. Also, vehicles send announcement messages about road conditions such as accidents or traffic jams to other vehicles that require a large dissemination range but real time processing is less strict than the alerts [2]. Moreover, any misbehavior and malicious behavior like a modification and replay on the sent messages can be fatal to other network's users. In addition, due to the unique features of VANETs, security and privacy in such

networks become more challenging. There are some solutions to establish security against inserting fake announcements by external and internal attackers, based on cryptographic authentication techniques that need the sender of a message have some secret keys as security materials that only available to legitimate users who registered by CA and therefore external attackers do not access to these keys [3,4]. In this paper, we focus on securing announcement messages by using advanced cryptography. In fact, we believe that in such a network like VANET and for many of its applications, security must focus on prevention of attacks, rather than detection and recovery. At the rest of this paper, in section II, we present the related work. In section III we describe the proposed scheme plan and the network model. Section IV studies the proposed protocol using simulations. Finally, Section V contains some concluding remarks.

II. RELATED WORK

There are some completed and ongoing projects on vehicular communication but the research on VANET security is still developing and there are very few academic publications that propose an efficient approach for achieving security and privacy simultaneously in VANETs. In addition there are more limited researches about privacy preserving; especially in its two layers such as anonymity and unlinkability. Most researches [5, 6, 7, 8] propose a general solution for VANET security or describe the problem statement. But to provide vehicle authentication, all these literatures agree on the need for a PKI and the use of digital signatures. Paper [9] focuses on detection and correction of malicious data and proposes a solution to validate received data. In this way, a vehicle receives some alerts from its neighbors and checks their correctness by comparing them with its own inference from a certain event. The main disadvantage of this approach is its high communication overhead, due to the lack of aggregation mechanisms. Paper [10] presents an overview of security primitives but does not explain a complete protocol. The focus of [11] is on received data warning and estimates the trustworthiness of a reported hazard. In fact, it takes vote on the received danger messages. It provides a good simulative analysis of different voting schemes but does not address privacy. Paper [12] explains an emergency message authentication scheme to validate emergency events. It uses cryptographic aggregation

techniques to reduce the transmission cost and uses a batch verification technique for verifying emergency messages efficiently. In this scheme vehicles form some clusters. The vehicle is on top of each cluster, aggregates and forwards data to the other clusters. This approach is suitable for highways, but when clusters change frequently like in cities, it suffers from high overhead communication. Paper [13] presents three variants offering a priori countermeasures against fake messages that reduce communication overhead by aggregation messages.

III. THRESHOLD SIGNATURE SCHEME PLAN

The trustworthy VANET is a VANET that the generation of fake messages is prevented in it. In fact, this scheme relies on a priori countermeasures against internal attackers for secure announcements in VANETs. Also, in proposed approach, digital signature is used as a cryptographic authentication technique against external attackers because this technique needs the sender of announcement has access to secret key that this is available for legitimate users, but for thwarting internal attackers, an endorsement mechanism based on threshold signatures is used. This a priori countermeasure is based on the fact that an announcement is not valid unless it is endorsed by a member of vehicles above a certain threshold and the basic assumption is the most users are honest which they do not endorse any announcement that contains false data. Also, by using threshold signature, this scheme can be better in message length and computational cost. In addition, this kind of countermeasure also satisfies the requirement of privacy as the other goal of this paper because it does not need to disclosure of dishonest vehicles. Due to it is not fair if the privacy of the vehicles and drivers that cooperate in generating trustworthy announcements compromises, group formation can be useful.

In this work, two layers of privacy are considered: anonymity and unlinkability. A system preserves anonymity when it does need the identity of its users to be disclosed. Unlinkability apply the different interaction of the same user with the system cannot be related. In fact, unlinkability is stronger than anonymity and prevents user tracking and profiling [14].

A. Choice of Cryptosystem

The implementation overhead is a very important factor in choosing the public key cryptosystem (PKCS) in the vehicular networks. According to DSRC [15], the resulting processing time overhead from safety messages that sent every 100 – 300 ms is shown as follows [7]:

$$T_{oh}(M) = T_{sign}(M) + T_{tx}(M | Sig PrKv [M]) + T_{verify}(M)$$

Where $T_{sign}(M)$ is duration of signing, $T_{tx}(M)$ is duration of transmit and $T_{verify}(M)$ shows the duration of verification. $Sig PrKv [M]$ is the vehicle V 's signature on M and includes the CA's certificate. According to this equation, there are two important factors in choosing a proper PKCS:

1. The execution speeds of the signature generation and the verification operations
2. The key, signature and certification sizes

In addition, the overhead of messages are constant for a PKCS because on the one hand the size of a safety message is between 100 – 200 bytes [7, 15] and on the other hand, the messages are hashed before being signing. According to DSRC, the minimal data rate is 6Mbps and its maximal value that used for safety messages is 12 Mbps. Table 1 shows the size and transmission time of two PKCSs and gives a comparison between signature generation and verification times of ECDSA [16] and NTRUSign [17, 18] as two standardized systems.

TABLE I. COMPARISON BETWEEN PKCSS' SIZE, TRANSMISSION; SIGNATURE GENERATION AND VERIFICATION TIMES.

PKCS	Key, Sig size(bytes)	Transmission time (ms)	Generation time (ms)	Verification time (ms)
ECDSA	28	0.019	3.255	7.617
NTRUSign	197	0.131	1.587	1.488

Table I concludes that the advantage of ECDSA is its compactness and NTRUSign is its speed, thus the use of them depends on the case sensitive evaluation. In this work, we use NTRUSign as an efficient and computationally inexpensive PKCS and due to its features such as easily created keys, high speed and low memory requirements.

B. Network model

This network contains vehicles with equipments such as TPD (includes a smart card) to store the secret materials, sign and verify announcements and also a positioning device like GPS. Generally, SK_i (secret key share) is kept in a smart card that prevents learning SK_i by the drivers. Otherwise, colluding drivers can recover the secret key SK and also any one of the vehicles can sign and verify messages, so without any endorsement, it is known as trustworthy. In addition to vehicles, the network includes GA (Government Authority) and roadside base stations. The basic security law in this network is foreseen mainly by the means of digital signatures. With the existence of a vehicular PKI, each vehicle needs to have at least a set of public / private key pairs that will use to sign transmitted announcements. Thus, it ensures that other vehicles can authenticate a received announcement if it contains a digital signature and the corresponding certificate which is issued by a CA (Certificate Authority).

C. NTRU Group Based Scheme

In proposed scheme, we consider highways with medium density of vehicles that travel at an arbitrary speed. In fact, it is not suitable for not crowded roads and sparse VANETs. Proposed network needs a GA in geographical area of deployment as a supervisor to ensure the correctness of set up phase. In fact, it works as a coordinator to distributing of

shares among the vehicles that are produced by different carmakers. In this way, GA partitions the n possible vehicles (from a VANET) into several subranges and assigns each of subranges to a carmaker. Also, it establishes a threshold signature scheme that generates n shares. A certain carmaker receives the shares that are corresponding to its assign subrange. In addition, GA establishes a signature scheme and divides the vehicles of the area to r groups. According to that signature scheme generates r shares and each share is linked to one group.

Set up phase: The VANET is formed of n vehicles that are divided to m groups, so each group contains n / m vehicles (the size of each group). In addition, the manufacture set up a (t, m) threshold signature scheme that generates a public key (PK) and g shares $(SK_j, j=1, \dots, m)$ of the secret key (SK) that is one share for each group. The manufacture keeps a copy of these r shares. Each vehicle P_i is assigned randomly to a group (j) by the manufacture. Then the vehicle is equipped with a PK and the secret key share SK_j that assigned to its group and keeps them in its TPD's smart card. This approach causes all the vehicles that belong to the same group, are assigned the same secret key share. Therefore, the partial signatures cannot be related to a single vehicle and can be related to any member of its group. In fact, the group makes the partial signature. In this way, this protocol provides unlinkability and by increasing the number of groups' members, the degree of this privacy is increased. On the other hand, the vehicles that belong to at least t different groups generate a valid signature $\sigma(m)$. That is in this protocol, a valid signature $\sigma(m)$ must be generated not just by any t vehicles, but by vehicles that belong to at least t different groups.

Announcement generation phase: To sending an announcement (m), a vehicle computes its signature on announcement and broadcasts m and its partial signature $\sigma_i(m)$. In this way, it uses a public one way hash function H that its input is a string with an arbitrary length but its output has a constant length. So, P_i 's partial signature is $\sigma_i(m) = H(m)^{SK_i}$. This announcement for checking the validity needs to reach to close enough vehicles to announcement generator. Generally, announcement messages are not relayed by VANET nodes and they move up to the range of the broad cast technology.

Endorsement phase: When vehicle P_j receives an announcement m with its partial signature that originate from P_i and wishes to endorse m . In this way, P_j computes its own partial signature on m . Then transmits $H(m)$ and $\sigma_j(m)$ to return them to P_i where $H(\cdot)$ is the same hash function used in the signature generation phase. As mentioned in previous phase, announcements with partial signatures are not relayed.

Signature composition phase: There are two steps for signature composition in our protocol: 1- Computing final signature in group level. 2- Computing final signature among r groups. As mentioned in set up phase, a valid signature $\sigma(m)$ must be generated not just by any t vehicles,

but by vehicles that belong to at least t different groups, so when the generator of announcement (P_i) receives the partial signatures on m , stores m and all the partial signatures (partial signatures on m are identifiable by the hash $H(\cdot)$ they carry). When P_i has collected t different partial signatures on m from all the groups, it can compute a final signature $\sigma(m)$ and broadcast it with m . In fact final signature is computed as follows [14]:

$$\sigma_f(m) = \prod_{i \in A} \sigma_i(m)^{\lambda_i^A} = H(m)^{\sum_{i \in A} \lambda_i^A SK_i} = H(m)^{SK}$$

Announcement verification phase: Vehicles will only considered as trustworthy when their announcements carry a final signature that can be verified by use of the public key. In the threshold signature scheme, vehicles can be sure that a final signature can only be computed if at least t vehicles have endorsed the announcement by computing their partial signature on m . By using the proposed scheme, this assurance will be increased because this threshold condition is applied in group's level. These announcements that contain a final signature will be relayed by VANET's nodes and can be reached to farther vehicles that will profit from their information.

D. Cost Analysis

In this section, the cost analysis of this protocol will be computed in terms of: Announcement length, announcement generation time and announcement verification time. To compute these, the values of table I. The size of announcements' information is assumed "c" bits. As mentioned before, both partially and finally signed announcements contain one signature, thus the length of announcements is $O(1)$ and it does not depend on parameter t . Consequently, announcement length = $c + 197$ bits.

In this protocol, an announcement is endorsed by the vehicles in parallel. Thus for computing announcement generation time, we assume "g" is the necessary time for an announcement to execute in one hop (in milliseconds). Generating a valid message needs data transmission that has some delay. This delay is fixed to the time that execute in two hops, one from generator to endorsers and another from endorsers to generator plus the time to compute two NTRU signature. So this delay is $2 * (g + 1.58)$.

In addition, when t endorsement announcements have been collected (partial signatures), they compose a final signature. In fact the cost of computing a final signature from t partial signatures is an $O(t)$ cost. So the composition time is $t * 1.58$.

Consequently, the overall generation time is $2 * (g + 1.58) + t * 1.58$ ms or if we want write it better, is $2 * g + 1.58 * (g + t)$ ms.

In addition, to verifying an announcement, only one signature (final signature) is required to be checked by the same public keys ($O(1)$ cost). So for NTRU, the announcement verification time is 1.48 ms

IV. SIMULATION RESULTS

The goal of this performance analysis is to determine the effect of having different traffic loads and cryptographic algorithm processing speed on message delay and message loss ratio.

A. Simulation Setup

We used NS2 [19] as a network simulator. It is important to use a realistic mobility model that its simulation results can correctly reflect the real world performance of a VANET. In this work, we use a tool MOVE (MObility model generator for VEhicular networks) [20] to generate realistic mobility models for VANET simulation rapidly. MOVE is built on top of SUMO (Simulation of Urban Mobility) [21] as an open source traffic simulator. In fact SUMO is used for simulating mobility models in urban that enables generating a vehicular network in details. In fact, proposed scheme is evaluated on two different road systems: city area and highway area. Fig.1 shows the designed city area which its length is 7 kilometers and 8 kilometers wide approximately, used in evaluation.

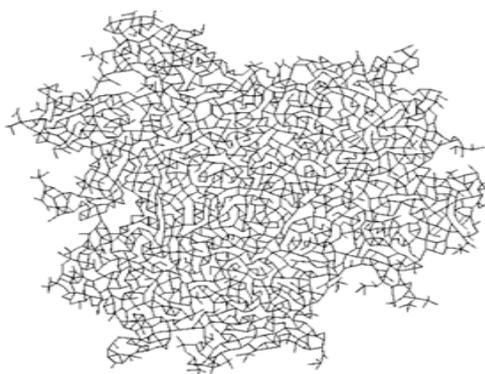


Figure1. Simulation environment

The speed of vehicles changes randomly in range of 30 – 70 km/h with ± 5 as tolerance. In high way scenario, a certain number of vehicles start to move with random start times and their speed is different from 95 km/h to 105 km/h. Table 2 contains of simulation parameters:

TABLE II. SIMULATION CONFIGURATION

Simulation scenario	City and highway environment
Communication range	300 m
Simulation time	100 sec
Chanel bandwidth	6 Mbps
Message size of proposed scheme	197 + c

B. Evaluation Results

In the following, the effects of traffic load and signature verification delay on average message delay and average message loss ratio as two evaluation parameters are experienced in two scenarios.

1) Effect of traffic load on end to end message delay:

The density of the vehicles is the main factor that has a major impact on the system performance in addition it is related to the total number of messages received by each vehicle. Fig. 2 illustrates effect of traffic load on the average message delay for proposed scheme under NTRUsign for city and highway scenarios. In this figure can be seen that although with the increase of traffic load, the message end to end delay is increased, it does not vary a lot (about 20 ms). In fact this average value is smaller than the maximum allowable message end to end transmission delay of 100 ms.

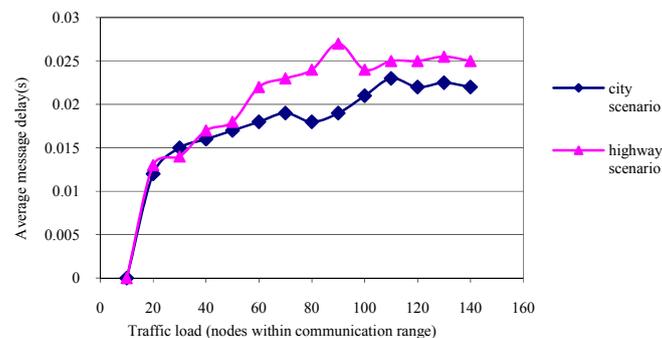


Figure2. Effect of traffic load on the message end to end delay under NTRUsign

2) Effect of traffic load on message loss ratio:

Fig. 3 shows the effect of traffic load on message loss ratio under our approach, according to this figure, the message loss ratio increases when the traffic load is increased. It is notable that the loss ratio reaches to 63 % when the traffic load is up to 150 and this traffic load is experienced when there is a hard traffic jam which according to the relationship between the communication range and the inter vehicle distance [58]. Generally, literatures like assume the inter vehicle space about 30 m and vehicles are mobile and transmit DSRC messages every 300ms over a 300 m communication range. In this condition, may a large number of messages are lost because most of the messages are sent by each vehicle repeatedly. In fact traffic load value below 50 is the normal traffic load happens where loss ratio is 19%.

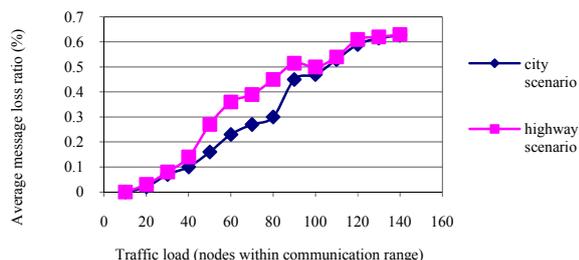


Figure 3. Effect of traffic load on loss ratio under NTRUsign

3) Effect of cryptographic signature verification delay on end to end message delay:

The latency that is taken by the cryptographic operations in the protocol is an important factor that determines the performance of a security protocol. It is notable that the power of hardware facility has a main role in determining the speed of implementing a cryptographic algorithm. On the other hand as mentioned before there is no limitation in using powerful hardwares in VANET, thus in this thesis is assumed that each vehicle is equipped with a powerful processor which can achieve very high processing speed. In addition for simulating this section, normal traffic load is assumed an average of 60 vehicles in the communication range. Simulation result in fig. 4 shows the message end to end delay is increased when the cost of verification operation increases.

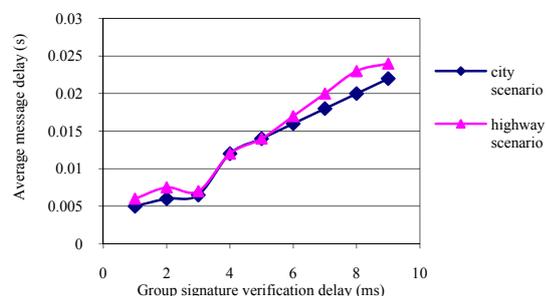


Figure 4. Impact due to signature verification delay on the message end to end delay under NTRUsign

4) Effect of cryptographic signature verification delay on the message loss ratio:

The lower value for this parameter indicates lower rate of losing packets in Mac layer. Fig. 5 shows the message loss ratio increase when the cryptographic operation cost becomes larger, according to this figure, after the signature verification latency reaches to a certain value (4 ms) the message loss ratio is increased significantly. In addition, the performances under two scenarios are close.

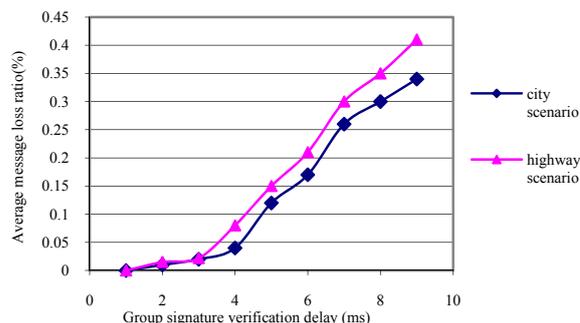


Figure 5. Impact due to signature verification delay on the average message loss ratio under NTRUsign

V. CONCLUSION

In this paper, it have been tried to establish security and privacy as two critical features of VANETs at the same time. In order to achieve trustworthiness in VANETs, we believe security must focus on prevention of attacks rather than detection and recovery thus relying on a priori measures against internal attackers has been proposed. In fact, this scheme have been proposed to achieve unlinkability without losing trustworthiness and outperform similar proposals in signature generation and verification times hence computational cost to enhance performance. In terms of future work, we intend to further develop this proposal for sparse VAVETs as a tradeoff between unlinkability and availability in addition this proposal assumes an governmental exists which coordinates share distribution thus research into an optimal method of key distribution is needed when no governmental authority is available.

REFERENCES

- [1] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications", *IEEE Wireless Communications Magazine*, vol. 13, no. 5, pp. 8–15, 2006.
- [2] 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.
- [3] 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.
- [4] 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.
- [5] J.-P. Hubaux, S. Capkun, and J. Luo. The security and privacy of smart vehicles. *IEEE Security and Privacy Magazine*, 2(3):49–55, May-June 2004.
- [6] Parno and A. Perrig. Challenges in securing vehicular networks. In *Proceedings of HotNets-IV*, 2005.
- [7] M. Raya and J.-P. Hubaux. The security of vehicular ad hoc networks. In *Proceedings of SASN'05*, 2005.

- [8] M. El Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian. Security issues in a future vehicular network. In Proceedings of European Wireless, 2002.
- [9] 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.
- [10] Kargl, Z. Ma, and E. Schoch, "Security Engineering for Vanets," Proc. 4th Wksp. Embedded Sec. in Cars, Berlin, Germany, Nov. 2006, pp. 15–22.
- [11] B. Ostermaier, F. D'otzer 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.
- [12] 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.
- [13] 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.
- [14] V. Daza, J. Domingo-Ferrer, F. Seb'e and A. Viejo, "Trustworthy Privacy-Preserving Car-Generated Announcements in Vehicular Ad Hoc Networks", IEEE Transactions on Vehicular Technology, to appear.
- [15] Q. Xu, T. Mak, J. Ko, and R. Sengupta. Vehicle-to-vehicle safety messaging in DSRC. In Proceedings of the first ACM workshop on Vehicular ad hoc networks, pages 19– 28. ACM Press, 2004.
- [16] M. Brown, D. Hankerson, J. L'opez and A. Menezes. Software implementation of the NIST elliptic curves over prime fields. Lecture Notes in Computer Science, 2020:250–265, 2001.
- [17] <http://www.rsasecurity.com>
- [18] Personal communication from NTRU, Inc.
- [19] NS2: <http://www.isi.edu/nsnam/ns/ns-build.html#allinone>
- [20] MOVE: <http://lens1.csie.ncku.edu.tw>
- [21] SUMO: <http://sumo.sourceforge.net/wiki/index.php/LinuxBuild>