INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

PRIVACY PRESERVING CHATTING IN VEHICULAR PEER-TO-PEER NETWORKS

P. SURESH[1], R. H. ASWATHY[2], P. KUMARAN[1],

M. EZHILVENDAN[3]

IJPRET-QR CODE *PAPER-QR CODE*

1. Assistant Professor, Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai.

2. Assistant Professor, RMK Engineering College, Chennai.

3. Assistant Professor, Jawahar Engineering College, Chennai.

Accepted Date:

04/08/2013

Publish Date:

01/09/2013

Keywords

Vehicular Ad Hoc Networks; Cooperative Authentication, Free-Riding Attacks; Selfishness.

Corresponding Author

Mr. Suresh P.

Abstract

Vehicular Ad-Hoc Networks (VANETs) have emerged as a promising approach to increase road safety and efficiency, as well as improve driving experience. however, if we do not take security and privacy issues into consideration, the attractive features of VANETs will inevitably result in higher risks for abuse, even before the wide deployment of such networks. While message authentication is a common tool to ensure information reliability, namely data integrity and authenticity, it faces a challenge in VANETs. In this paper, we propose an efficient cooperative authentication scheme for VANETs. In order to reduce the authentication overhead on individual vehicles, and shorten authentication delay, this scheme maximally eliminates redundant authentication efforts on the same message by different vehicles. To further resist various attacks, including free-riding attacks launched by selfish vehicles, and encourage cooperation, the scheme uses an evidence-token approach to control authentication workload, without the direct involvement of a trusted authority (TA). When a vehicle passes a Road-Side Unit (RSU), the vehicle obtains an evidence token from the TA, via the RSU. This token reflects the contribution that the vehicle has made to cooperative authentication in the past, which enables the vehicle to proportionally benefit from other vehicles' authentication efforts in the future, and thus, reduce its own workload.

INTRODUCTION

With the rapid development of wireless technologies, people are starting to enjoy wireless access everywhere, from cafes, to hotels, to airports; wireless access is even being seen in vehicles on the move. Recently, car manufactories and telecommunications industries have teamed up to equip every car with wireless technologies; these technologies can not only bring various information technology services to vehicles on the move, but also improve road safety and traffic efficiency. Cars equipped with wireless communication devices and roadside infrastructure can form a huge, self-organized communication network called a Vehicular Ad-Hoc Network (VANET). Specifically, a VANET is a dynamic collection of networked vehicles that communicate with each other, or nearby Road-Side Units (RSUs), using the Dedicated Short Range Communications (DSRC) technique [1]. These vehicles are equipped with wireless On-Board Units (OBUs), which perform this communication.

The VANET provides a ubiquitous computing environment to drivers and passengers, and enables numerous services through a variety of vehicle applications. Such applications, such as emergency braking warning, are made possible by communication between vehicles. By using VANETs, travelers can achieve improved driving safety and comfort. One fundamental security problem in VANETs is message authentication.

Achieving message authentication consists of two essential security checks: an integrity check, and an identification check. Message authentication must be implemented to allow vehicle users to differentiate reliable information from bogus information, and to resist modification attacks and impersonation attacks. An appealing solution to this problem in VANETs is to digitally sign messages before sending them; not only does this allow the receiver to identify the sender, but the signature also prevents the message contents from being modified in transit. Several schemes have been proposed in literature, and can mainly be divided into the following two categories. One is traditional Public Key Infrastructure (PKI)-based digital signature schemes [5], [7], and the other is group signature based security schemes [2]. In both categories, each message needs to be signed by the sender using an asymmetric algorithm, and its receiver needs to verify the message received. Both of these schemes can effectively ensure secure communication while simultaneously protecting user privacy, but traditional PKI-based schemes may fail to satisfy the stringent time requirements of vehicular communication applications. Especially as traffic density increases, a vehicle may become unable to verify the authenticity of the messages sent by its neighbors in a timely manner, which results in message loss, and in turn, an increased risk to public safety.

In this paper, we propose an efficient cooperative message authentication scheme that does not directly involve a trusted authority (TA). This scheme is carried out by a set of neighboring vehicle users; with minimal inter-vehicle coordination, the scheme minimizes redundant authentication efforts of different vehicles working on the same message. It also encourages cooperation and resists free-riding attacks.

Our contributions are threefold: first, we propose a cooperative authentication scheme that doesn't involve inter-vehicle interaction, using extensive simulations to derive the optimal strategy for vehicle users under different parameter settings. Second, in order to resist the free-riding attacks that do not use fake authentication efforts (hereinafter referred to as "passive free-riding attack"), an evidence-token mechanism is added. This mechanism enables the TA to flexibly control the co operational capability of vehicles, according to their cooperation history. An authentication proof is further required to be output

by cooperative vehicles to resist the free-riding attacks where fake authentication efforts are involved (hereinafter referred to as "active free-riding attack"). Without having free access to others' cooperation efforts, one's selfish behavior is effectively discouraged. Third, we evaluate the performance of the proposed scheme in a simulated VANET environment. From this point forward, we use 'vehicle', 'vehicle user', 'driver' and 'user' interchangeably

II. PROBLEM FORMULATION

A. Network Model:

We consider a VANET consisting of a large number of vehicles *V* = *fv*1*; v*2*; _ _ _; v_g*. The OBUs equipped on the vehicles enable them to communicate with neighboring vehicles in range *trv*. A central TA provides registration to vehicle users during which vehicles' pseudonyms and corresponding secrets are updated and stored in the vehicles' OBUs. A limited

number of RSUs are deployed in the VANET. The TA can talk to vehicle users via RSUs through wireless communication when the vehicles are close to the RSUs. The RSUs have both wireless connections and wired connections. The wireless connections with communication range *trr* (> *trv*) can be used for contacting with nearby OBUs. The wired connections

allow RSUs to communicate with each other in a secure and reliable way.

B. Security Model:

In our security model, we assume that the TA is fully trusted by all vehicles and it is infeasible for any attacker to compromise. We do not consider attacks by compromised vehicles or outside adversaries, and only focus on user selfish behavior in cooperative authentication. Since cooperative authentication is conducted in an unattended and autonomous environment, vehicles may behave selfishly to take advantages from others' authentication contributions and rarely make their own. Such selfish behavior, referred to as free-riding attack, poses a serious threat to cooperative message authentication.

We consider the security threats of the following three types:

1) Linkability attack: Authentication linkability is necessary for the TA to identify misbehaving users. In linkability attack, a malicious user falsely claims that it has verified multiple message-signature pairs, and it also disables the TA to trace its unique identifier so as to avoid being punished.

2) Free-riding attack without authentication efforts (or passive free-riding attack): Such attack is launched by a malicious user who aims to enjoy the authentication efforts of other users at no cost, for example, by passively listening to the information sent from nearby users. It reduces the attacker's authentication overhead and breaks the fairness among users.

3) Free-riding attack with fake authentication efforts (or active free-riding attack): Such attack is launched by an active malicious user who participates in the cooperative authentication protocol by generating fake authentication efforts. Considering the synchronism in a cooperative authentication process, the attacker checks the authentication efforts of other users and combines them to forge an authentication effort for itself. By doing so, it does not actually authenticate any original message but provide valid verification efforts because these signatures have been checked by others. This attack is more intelligent than the second one. It can hardly be detected by nearby users or the TA.

III. BASIC COOPERATIVE AUTHENTICATION SCHEME

We consider *x* vehicles that gather in a small area and are able to directly communicate with each other. There are *y* messages available to these vehicles, and each message contains a unique index and is attached with a signature. The *x* vehicles need to authenticate the *y* messages by verifying their attached signatures. Let *Cv* denote the cost of authenticating one signature, and *Cs* the cost of generating one signature. In the following, we analyze the non-cooperative authentication case and the cooperative authentication case, respectively.

Non-cooperation case: Vehicles do not cooperate on message authentications. Each of them has to authenticate the *y* signatures alone. Per vehicle authentication cost is $Cnc\ 1 = y\ \_\ Cv$, and the total cost of the *x* vehicles is $x\ \_\ y\ \_\ Cv$.

Cooperation case: The *x* vehicles cooperatively authenticate the *y* signatures.

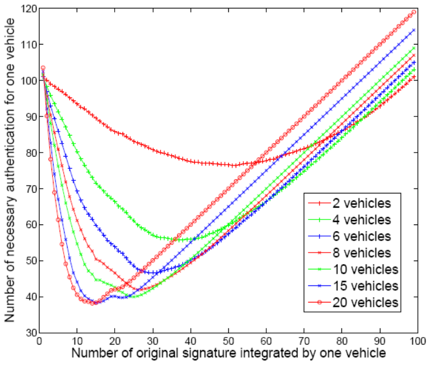


Fig. 1. Cooperative gain

Figure 1 shows the cooperation gain in message authentication, where *x* = 10 users have *y* = 100 common message-signature pairs.

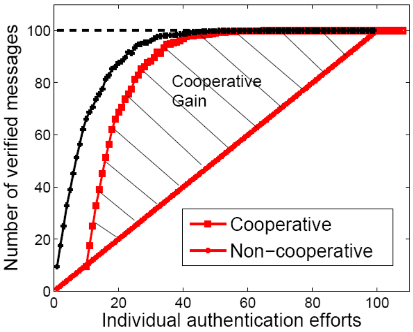


Fig. 2. Optimal number of original signatures

The number of messages that have been verified by a vehicle is shown in terms of the number of authentications that have been performed by the vehicle. The red lines represent the performance of cooperative/noncooperative authentications. The shadow area is the gain that can be achieved by cooperative authentication. We take an example as follows: if a vehicle authenticates 39 signatures in a non-cooperative way, it obtains 39 authenticated messages; if a vehicle authenticates 30 + 9 signatures by cooperative authentication introduced above, it will receive 87 authenticated messages. It can be seen that vehicles can receive larger benefits by authenticating 9 integrated signatures. The black line represents the number of original signatures that have been covered by integrated signatures in terms of *vx; y*.

IV.SECURE COOPERATIVE AUTHENTICATION SCHEME

In this section, we improve the basic scheme to deal with selfish behavior. It is observed that if a vehicle does not generate integrated signatures, it can always consume less for message authentication than those who do. Since VANETs are highly dynamic environments and the privacy of vehicles needs to be guaranteed by pseudonyms, the cooperation among

vehicles can be regarded as a non-repeated game where defection is always the optimal strategy for individual vehicles.

A. Evidence and token for fairness:

The basic principal of the evidence-token mechanism is to balance the effort that vehicles make over time with the advantages that vehicles take from others.

The mechanism requires time to be slotted. The TA will be responsible to maintain the balance according to the time slots. It receives the evidences from vehicles via RSUs when vehicles pass by the RSUs, and sends the tokens back to vehicles based on the evaluation of their authentication efforts in the past time slots. The evidences will not be repeatedly used to count their effort. The TA generates and distributes tokens to vehicles in order to enable them to verify other vehicles' integrated signatures. The tokens must be of timeliness; otherwise vehicles may disconnect from RSUs after obtaining enough tokens.

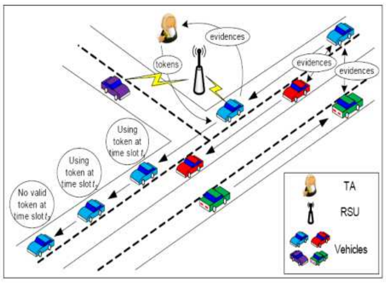

evidences
tokens
evidences
evidences
Using token at time slot t_1
Using token at time slot t_2
No valid token at time slot t_3
TA
RSU
Vehicles

Fig. 3. Evidence-token mechanism

Evidence collection by vehicles: in step 1) of the basic

Scheme, a vehicle authenticates some of the original signatures received and generates an integrated signature at a time slot. It then creates an evidence for its authentication effort, which includes the time slot, the number of cooperative vehicles *x*, the number of original signatures *y* and the number of original signatures *vx;y* that have been included into the integrated signature. It transmits the integrated signature and the evidence to others. Note that the evidence cannot be forged and will be publicly verified by the receiver vehicles.

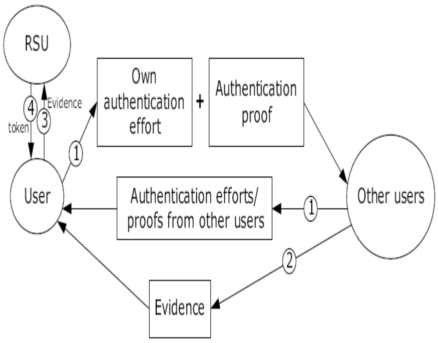
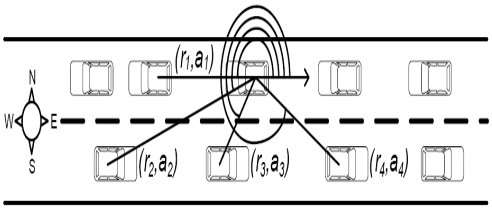

RSU
4
token
3
Evidence
1
Own authentication effort
+
Authentication proof
User
Authentication efforts/ proofs from other users
1
Other users
2
Evidence

Fig. 4. Polar coordinates of vehicles

We consider that vehicle users *fv*1*; _ _ _; vxg* are all aware of the geographical information (*L*1*; _ _ _; Lx*), where *Li* is a (latitude, longitude) - tuple representing the location of user *vi*. User *vi* builds a polar coordinate system with itself as the origin and the east direction as axis, as shown in Fig. 4. Another user *vj* has its unique polar coordinates (*rj ; aj*) in this coordinate system, where *rj* is the distance between *vi* and *vj* and *aj* is the angle. All the other vehicles can be sorted in an increasing order *odi* = *fvi;* 1*; _ _ _; vi; x*−1*g* based on their polar coordinates. *odi* can be obtained by all *x* users. We set a time upper bound for evidence generation. The evidence generation foruser *vi* is started by *vi;* 1.



B. Authentication proof:

In the previous subsection, we introduced an approach to enable the off-line TA to coordinate the cooperations among users via RSUs. The TA balances the contributions from and rewards toward individual users so that cooperation is largely stimulated and users are fairly treated. However, the approach cannot resist the free-riding attacks. Users are unable to distinguish a fake authentication effort from a real one, and the TA still rewards the attackers with valid tokens. In this subsection, we consider the free-riding attacks with fake authentication efforts (or active free-riding attack). The attackers make use of other users' authentication efforts and refuse to contribute in the cooperation.

Specifically, consider a selfish user *ui* receives the cooperative authentication efforts *ej*1; *ej*2; _ _ _; *ejk* from multiple users *uj*1; *uj*2; _ _ _; *ujk,* where *ejx* corresponds to a group of indexes *Sjx* that from *ujx.* By using IBSC scheme, if *ejx* contains any incorrect information, user *uj;x* can be easily tracked. Based on

this observation, user *ui* assumes that the cooperation efforts from other users are valid, and thus select a subset group of indexes *Si* _ ∪*k* *x*=1 *Sjx* , and generates a signature on the index set of *Si* as its cooperative authentication effort *ei*. In case that all the signatures in *Si* are good, such selfish behavior cannot be detected by other users. As such, the attack succeeds

since user *ui* does not check any original signature in *Si* but obtain the maximum profits. We regard this attack as free riding attack with fake authentication efforts (or active free riding attack).

C. Flows of proposed scheme:

Consider some geographically-close users with a common set of message-signature pairs. We summarize the secure cooperative authentication scheme as follows. As shown in Fig. 5, each user randomly picks and verifies *vx; y* original signatures, and generates an integrated signature as its own authentication effort. The value of *vx; y* can be calculated according to Section IV. In addition, the user also generates an authentication proof, which proves that it indeed verified the original signatures. After that, it shares its authentication proof with the public. Whenever a user is able to communicate with

an RSU, it sends the authentication proof as evidence of others to the RSU. The RSU then checks the validity of the evidence and rewards the user with new tokens that can be used to verify the cooperative authentication efforts in the subsequent time slots.

V. SECURITY ANALYSIS

In this section, we analyze the security properties of our proposed scheme following the pre-defined security model. We will show how the scheme can effectively resist linkability and free-riding attacks.

A. Linkability attack:

In this attack, the attackers generate integrated signatures and disable the TA to trace the signatures to its identity. Because generating an integrated signature requires the attacker to input a pseudonym secret key *pski*, the generated signature is linked to the corresponding pseudonym. The TA records the mapping from pseudonyms to identities and is therefore able to recover the identity of the attacker. Hence, linkability attack is successfully prevented.

B. Free-riding attack without authentication efforts:

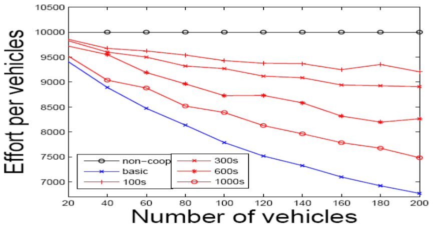
In this attack, the attacker does not verify any original signature but obtains the authentication efforts from other cooperative users. In the basic cooperative authentication scheme (Section IV), we do not adopt any security mechanism to overcome this attack. An evidence-token mechanism was then devised in Section V-A to deal with it. After sharing its authentication effort with nearby users, a user obtains unforgeable evidence from a random neighbor. It then trades the evidence with the TA for new tokens. Only with the new tokens, it may enjoy the authentication efforts from nearby users in the following time slots. If the user does not cooperate at all, it will obtain no tokens and be unable to benefit from other users' authentication efforts. Hence, free-riding attack without authentication efforts (or passive free-riding attack) is resisted. We will demonstrate the effectiveness of the evidence token mechanism through simulations in the next section.

VI. PERFORMANCE EVALUATION

In order to give insights into the performance of the proposed secure cooperative authentication scheme, we have conducted a set of custom simulations using a Java simulator. In the following, we detail our simulation settings and present the simulation results.

A. Simulation settings:

We consider a relatively small and typical VANET, where _ = (20*;* 40*;* _ _ _*;* 200) vehicle users equipped with OBUs are uniformly deployed in a 10*;* 000m _ 10*;* 000m area. The wireless transmission range of each OBU is 300m. A set of 10 social spots indexed from 1 to 10, denoted as *Su*, are randomly deployed into the area. At each of the four randomly-selected social spots 4*;* 6*;* 8*;* 10, a storage-rich RSU devices with transmission radius of 1*;* 000m is deployed, which helps users to contact with the TA. Each vehicle user has a fixed social spot set *Si* _ *Su*, where 6 _ *jSij* _ 10. It randomly chooses a social spot from this set, and arrives there along the shortest path at the average velocity 10m/sec. After arriving at the social spot, it stays at most 5 minutes and then moves to another randomly chose spot from its social spot set.



(a) 4 RSUs

Fig. 5. Flow chart of the secure cooperative authentication scheme

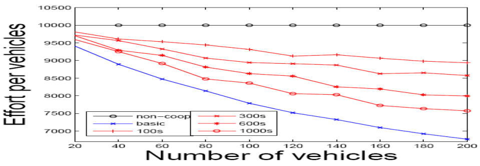
B. Simulation Results:

Figure 6(a) shows the simulation results for three settings. The black line indicates the performance of the no cooperative authentication scheme. It can be seen that the average total efforts of the users over 10; 000 seconds is 10; 000. This is because each user has to do 100 message authentications every 100 seconds and 100 _ (10000=100) = 10000 message authentications in total. The blue line shows the performance of the cooperative authentication scheme

without selfish behavior. The users can obtain maximum cooperative gain since all of them behave according to the optimal approaches. The authentication effort made by users significantly decreases as the number of users increases.

VII. CONCLUSIONS

In this paper, we have presented a novel cooperative message authentication scheme for VANETs. By the proposed scheme, vehicle users can cooperatively authenticate a bunch of message-signature pairs without direct involvement of a trusted authority (TA).



(b) 6 RSUs

Fig. 6. (a) Passive free-riding, (b) active free-riding

In addition, the free-riding attacks without authentication efforts (or passive free-riding attack) launched by selfish vehicle users can also be effectively resisted through an evidence-token approach; the free-riding attacks with fake authentication efforts (or active free-riding attack) can be prevented by enforcing vehicle users to output their authentication proofs.

REFERENCES

1. C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity based batch verification scheme for vehicular sensor networks," In *Proc. of the 27th IEEE International Conference on Computer*

Communications (INFOCOM), pp. 24650, Phoenix, Arizona, USA, 2008.

2. 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. 3442456, NOVEMBER 2007.

3. X. Liang, R. Lu, X. Lin, and X. Shen, "PPC: Privacy-preserving chatting in vehicular peer-to-peer networks," In *Proc. of the 72nd IEEE Vehicular Technology Conference (VTC2010-Fall)*, pp. 1-5, Ottawa, Canada, 2010.

4. X. Lin, R. Lu, X. Liang, and X. Shen, "STAP: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in VANETs," In *Proc. of the 30th IEEE International Conference on Computer Communications (INFOCOM)*, pp. 2147-2155, Shanghai, China, 2011.

5. M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, Vol. 15, No. 1, pp. 39-68, 2007.

6. Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 61629, 2011.

7. U.S. Department of Transportation, "National highway traffic safety administration," In *Veh. Safety Commun. Project, Final Report. Appendix H: WAVE/DSRC Security*, Apr. 2006.

8. X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: Timed efficient and secure vehicular communications with privacy preserving," *IEEE Transaction on Wireless Communications*, vol. 7, no. 12, DECEMBER 2008.