COOPERATIVE MESSAGE AUTHENTICATION AND RESISTING FREE RIDING ATTACKS IN VANETs

P.Shilpa[1], Rajkumar B Patil[2]

[1]M.Tech Scholar (CSE) BKIT, Bhalki
[2]Professor of CSE Dept, BKIT, Bhalki

Abstract

A Vehicular Ad-Hoc Network (VANET) achieving its excellence when road safety, its efficiency and also enhancement in driving experience come into consideration. The road safety and efficiency can be accomplished by using the applications that communicate from one vehicle to another i.e., intercommunicating vehicles, emergency brake warning; however, if privacy and security issues are not considered, the captivating features of VANETs causes unpreventable risks for abuse. Information reliability, namely data integrity and authenticity can be achieved by a common tool known as message authentication, which faces a challenge in VANETs. If large number of messages are received by a vehicle, it becomes exhaustive (per-message) authentication may cause some extravagant computational overhead on the vehicle, and hence applications that are time critical suffers from unacceptable delay, such as accident warning and therefore in this concept introducing a cooperative authentication scheme for VANETs. This scheme eliminates unnecessary authentication attempts on the same message by different vehicles at a maximum which reduces the overhead caused by authentication on an individual vehicle, and shortening the authentication delay. This concept uses a token evidence approach that control authentication workload but without a trusted authority's(TA) direct involvement which further resist numerous attacks, including freeriding attacks set by selfish vehicles, and promote cooperation. Vehicle passing a Road-Side Unit (RSU) obtains an evidence token via the RSU from the Trusted Authority. This token represents the contribution that the vehicle has made to cooperative authentication in the past, and thus enabling a vehicle to get convenience from other vehicles' authentication attempts in the future, and hence its workload is reduced. Through this substantial simulation, the main goal is of saving workload, and resisting free-riding attacks.

Keywords- *Vehicular ad hoc networks; cooperative authentication; free-riding attacks; selfishness*

---***---

1. INTRODUCTION

As there is a rapid development of wireless technologies, people are enjoying wireless access everywhere, such as cafes, hotels, airports and wireless access is even being used in vehicles on the move. For this to happen telecommunications industries and car manufactories have lined up to equip every car with wireless technologies; these technologies bring various information technology services to vehicles on the move, and also advance road safety and traffic efficiency. Cars built with roadside infrastructure and wireless communication devices can form a selforganized communication network called a VANET. Using the Dedicated Short Range Communications (DSRC) technique, the networked vehicles communicate with each other, or nearby Road-Side Units (RSUs). Such vehicles are built with wireless On-Board Units (OBUs), which perform communication.

There are three efforts of this work: first, proposing a cooperative authentication scheme where no intervehicle interaction is involved, under different parameter setting, deriving an optimal strategy for vehicle user using extensive simulations. Second, no fraudulent authentication attempts (hereinafter "inactive free-riding attacks") in order to avoid free-riding attacks which use fake authentication. Evidence token mechanism is introduced. This mechanism manageably controls the co-operational ability of vehicles using TA in accordance of their cooperative history. Further an authentication proof is needed to be outputted by cooperative vehicles to avoid free-riding attacks where fake-authentication attempts are involved. There should be a free access to one's selfish behavior. Third, performance in this scheme is evaluated in a simulated VANET environment. Hereinafter, keywords such as 'vehicle user', 'driver', 'vehicle' and 'user' will be used.

2. RELATED WORK

There are basically two security mechanism and protocols that ensures privacy-preserving and secure vehicle are communications namely, Public Key Cryptography(PKC) and Secret Key Cryptography(SKC)- based solutions. Protocol using PKC approach is classified into two subcategories: Traditional Public Key Infrastructure (PKI) and group signature techniques. In the group signature technique, Lin et al. found a fact that an important cryptographic primitive is the unique characteristics of group signature that exactly match the privacy and security requirements in VANETs. Different privacy and security requirements are considered based on two types of VANET communication, namely vehicle-to-vehicle and vehicle to infrastructure communications, and based on a combination of group identity and signature(ID)- based techniques, they proposed privacy-preserving and novel secure protocol for vehicular communication.

In both the above two cases the sender signs and broadcasts each message, the receivers using corresponding public key verifies the receive message. An asymmetric algorithm becomes unscalable when a high traffic load is encountered where the protocols creates heavy overhead in signature verification. As a result, message authentication of all the received messages becomes unable to verify. In metropolitan-area transportation, a vehicle may not quickly verify the authenticity of all the received messages and this may cause message loss and also putting public safety at risk. Zhang at al. proposed an enhancement for PKC-based mechanisms using a cryptographic primitive called batch signature providing an efficient authentication protocol for vehicular communication. It reduces the message verification overhead of RSU by allowing RSU to verify multiple signatures at a time. But the disadvantage of this batch verification is when a false data is injected, it makes vulnerable to DoS attack.

Zhang et al. proposed a novel RSU-aided message authentication scheme named RAISE, where RSUs verifies authenticity of messages sent from vehicles, and the result will be notified to the vehicles. Message Authentication Codes(MACs) are used with the aid of RSUs for message authentication in inter-vehicle communication. However, RSUs are highly required for message authentication phase, but when RSUs are not widely available, For example, early development stages of VANETs, it becomes ineffective.

Lin et al. developed a TSVC (Time Efficient and Secure Vehicular Communication) scheme which is based on Timed Efficient Stream Loss-tolerant Authentication (TESLA). In TSVC, in advance, a number of hash chains are generated. At random, a vehicle selects one chain and broadcasts to it neighbours about the commitment of the chain, which is protected by PKI-based digital signature. MACs are generated by the vehicle which uses elements of the chain originating from it. Now, its neighbors based on these MACs are able to authenticate the message. However, TSVCs effectiveness of message authentication will be reduced because of dynamic topological structure for vehicular network.

Lin proposes a cooperative message validation protocol, where vehicle reports any invalid messages detected by validating some percentage of its received messages, in accordance with its own computing capacity. However, some selfish vehicles may not contribute for cooperative efforts for message authentication. Hao et al. proposed a distributed cooperative message authentication scheme, which aims to reduce the number of verification for a single message where verifiers are selected using geographical locations relative to the message sender. The disadvantage of this scheme is it requires direct involvement of RSUs and allows redundant authentications on the same message.

3. PROBLEM FORMULATION

3.1 Network Model

Let us consider VANET with large number of vehicles V={v_1, v_2,…,v_μ}. trv be the range that the OBUs equipped on the vehicles allow them to communicate with neighboring vehicles. A centered Trusted Authenticity allows vehicle users to register so that the vehicles pseudonyms and its corresponding secrets are stored and updated in the vehicles OBUs. There will be less number of RSUs are in the VANET. Trusted Authority communicates with the vehicle users via RSUs either by wireless or wired connection, both type of communication are available in RSUs. To contact with nearby OBUs, the wireless connection with communication range of $tr_r(>tr_v)$.. The wired connection supports secure and reliable way of communication. Vehicles are assigned with a set of asymmetric key pairs, and the public keys are alternatively used. Vehicles keeps on changing their public keys and thus their location privacy preservation can be achieved due to the unlinkability of new and old public keys. Trusted Authority assigns new public key when a vehicle uses its public key. Public key can be linked to a specific vehicle by the Trusted Authority so that the Trusted Authority is able to trace and regulate the vehicle's behavior.

4. SECURE COOPERATIVE MESSAGE

4.1 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. In order to overcome the incentive to defect, we introduce an evidence-token mechanism and an identity-based signcryption scheme. We then propose a secure cooperative authentication scheme which provides an efficient and secure cooperation platform for vehicles. In the last part, we additionally require vehicles output cooperation proofs so that they can verify the originality of authentication efforts made by each other. The generation of such proofs is to prevent the free-riding attacks with fake authentication efforts (or active freeriding attack) at a reasonable cooperation cost.

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 enables them to verify other vehicles' integrated signatures. The tokens must be of timeliness; otherwise vehicles may disconnect from RSUs after obtaining enough tokens. Specifically, we describe the evidence-token mechanism as shown in Figure 1.

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 $v_{x,y}$ that have been included into the integrated signature. It transmits the integrated signature and the evidence to others. Since evidence generation and transmission consume energy, the number of evidences generated per vehicle should be limited.2) we devise a distributed approach based on geographical information in order for vehicles to be locally aware of their responsibilities of evidence generation. The approach randomly and fairly distributes the workload of evidence generation and minimizes the number of evidences. It also enables good vehicles to monitor the potential malicious behavior. We consider that vehicle users $\{v_1,\ldots,v_x\}$ are all aware of the geographical information $(L_1,\ldots,L_x)$, where Li is a (latitude, longitude)- tuple representing the location of user v_i. User v_i builds a polar coordinate system with itself as the origin and the east direction as axis, as shown in Figure 2. Another user v_j has its unique polar coordinates (r_j , a_j) in this coordinate system, where r_j is the distance between v_i and v_j and a_j is the angle.

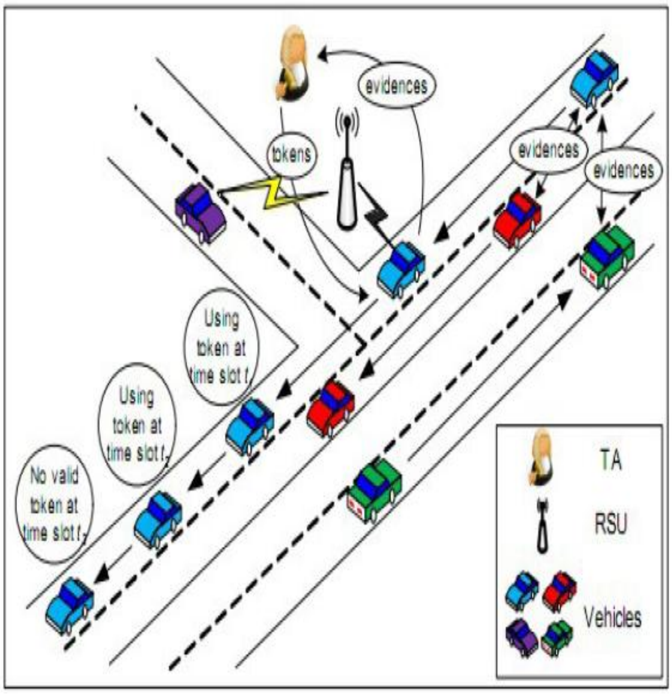
evidences
tokens
evidences
evidences
Using token at time slot t
Using token at time slot t
No valid token at time slot t
TA
RSU
Vehicles

Fig 1: Evidence-token mechanism

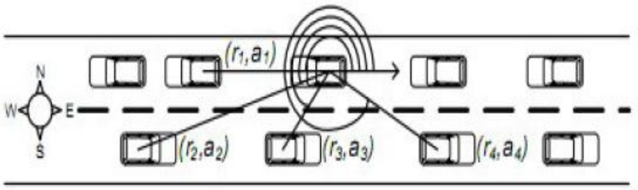

Fig 2: Polar coordinates of vehicles

All the other vehicles can be sorted in an increasing order odi = $\{v_{i,1},\ldots,v_{i,x-1}\}$ 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 for user vi is started by $v_{i,1}$.

- If user $v_{i,1}$ generates an evidence in the given time bound, user $v_{i;2}$ will check the validity of the evidence based on user v_i's effort. If the evidence is incorrect, user $v_{i,2}$ will continue to wait.
- If user $v_{i,2}$ does not receive a valid evidence from user $v_{i,1}$ in the given time bound, users $v_{i,2}$ records this irresponsible behavior together with the current pseudonym of user vi,1. It then takes over the evidence generation responsibility of vi in the following time period. User $v_{i,3}$ will be invoked in turn if $v_{i,2}$ fails to do so. Since every user knows its order in odi and the time upper bound is fixed, user v_j will be responsible for checking v_i's evidence if v_{j-1} outputs the evidence. If the check fails, user v_j then generates the evidence. Since the geographical information of vehicles is totally random and unpredictable, vehicle users will fairly share the evidence generation load. The number of evidences is minimum, i.e., it is equal to the number of vehicles. If any vehicle does not generate evidence as required, another vehicle will record its malicious behavior and report it to the TA. Such behavior will also be considered selfish. Note that, an exceptional case is that all the x-1 vehicles are irresponsible, which exists with a very small probability.

Token generation by TA: The TA balances the workload of vehicles and the advantages the vehicles take from each other. Based on the evidences, it checks the number of integrated signatures si,c that are generated by user vi in previous time periods. Then, it assigns user vi with multiple tokens according to the provided evidences. Each token is only valid for a specific time slot. If user vi provides enough evidences to confirm its proper behavior, the TA will assign a large number of tokens to user vi so that vi can benefit from other vehicles in a long time period. On the other hand, if vi does not provide the expected number of evidences, the TA will assign less tokens to vi so that vi does not have enough tokens before contacting the next encountered RSU. Now, we adopt an identity-based signcryption (IBSC) technique into the secure cooperative authentication. An IBSC scheme can be used to control the capability of verification. For example, after verifying a group of original signatures, a user could encrypt an integrated signature such that others know which signatures it has verified after the corresponding decryption. Specifically, the IBSC scheme consists of the following five algorithms,

5. PERFORMANCE EVALUATION

In order to give insight into the performance of the proposed secure cooperative authentication scheme, we call the Matlab methods from java for better interfacing and to present the simulation results.

Simulation Settings

We consider a relatively small and typical VANET, where μ= 20 vehicle users equipped with RSUs. The wireless range considered is 100m. A set of 20 social spots indexed from 1 to 20, are randomly deployed into the area. At each of the four randomly-selected social spots, four storage-rich RSU devices is deployed, which helps users to contact with the TA. We Higher Authority(HA) to be the TA. A HA distributes the PKC to a Moving Vehicle(MV). As soon as the key is distributed from HA to MV, the RSUs share the MVs information. After every move, the information such as MV's id, location and the key is shared among the RSUs such that the other vehicles may get to know nearby traffic information. If a particular vehicle is unauthorized or if any emergency breaking then a MV will come to know that the path is busy so that it can change its route. By the proposed scheme, vehicle users can cooperatively authenticate a bunch of messagesignature pairs without direct involvement of a TA. The simulation parameters include the number of users (20), the number of RSUs (4) . We plot the results in Figure 3.The red line implies the performance of the cooperative authentication scheme with selfish concerns. In order to pre-vent selfish users from launching freeriding attacks, the TA adopts the proposed evidencetoken mechanism to control the cooperation capability of users. Thus, the proposed scheme overcomes the users' incentive to defect and effectively resists freeriding attack. Required authentication effort in the 4-RSU setting is much larger than that in the 10-RSU setting. The main reason is that users have less probability to contact with RSUs in the former case. This indicates that users with 100-second lifetime tokens may have less cooperation on authentication since they cannot update their tokens in time. Therefore, the determination of token lifetime should depend on not only the selfish behavior of users but also the number of users and the number of RSUs. The scheme must ensure that reducing of token lifetime as punishment lead to the reduction of gain in cooperative authentication.

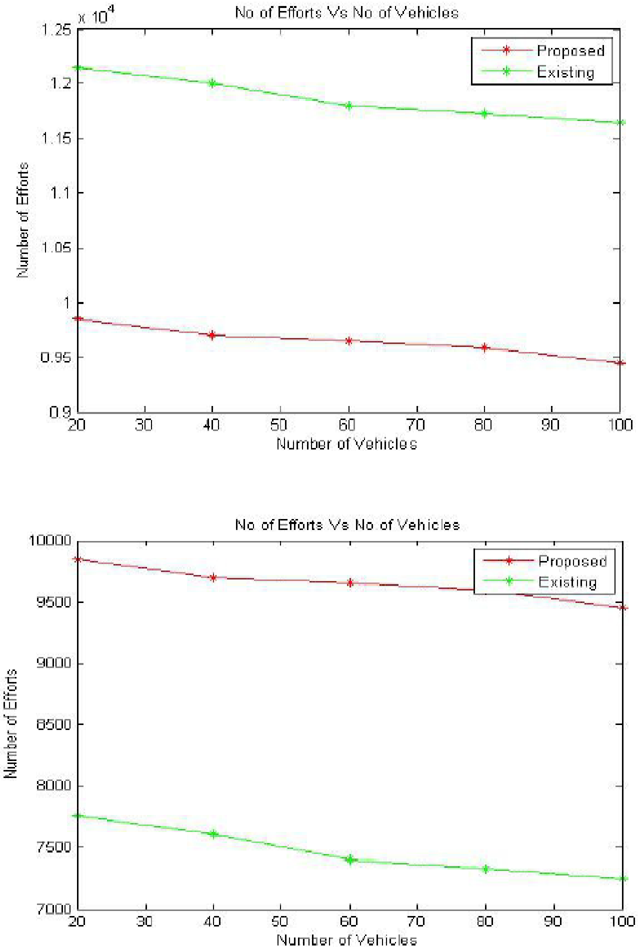

Fig 3: Simulation results

6. CONCLUSION

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). 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. The TA strategically adjusts the valid period (lifetime) of tokens for each vehicle user based on the collected evidence, thereby controlling vehicle users' cooperation capabilities periodically. For the proposed scheme, the adopted evidencetoken mechanism requires the TA to track selfish vehicle users and minimize their gain. It is desired to have a completely distributed cooperative authentication scheme for VANETs with a small number of RSUs. In future, removing the indirect involvement of the TA and exploit game theory to discuss the best strategy for vehicle users.

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. 246?50, Phoenix, Arizona, USA,2008.

[2]. X. Liang, R. Lu, X. Lin and X. Shen, “PPC: Privacy-preserving chatting in vehicular peer-topeer networks,” In Proc. of the 72nd IEEE Vehicular Technology Conference(VTC2010-Fall), pp. 1-5, Ottawa, Cannada, 2007.

[3]. X. Lin, “Secure and Privacy Preserving Vehicular Communication” PhD Thesis, University of Waterloo, Canada, 2008.

[4]. U.S. Department of Transportation. “National highway traffic safety administration,” In Veh. Safety Commune. Project, Final Report. Appendix H: WAVE/DSRC Security, Apr.2006.

[5]. C. Zhang, X. Lin, R. Lu, and P-H. Ho, “RAISE: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks,” In Proc. of IEEE International Conference on Communications (ICC), Beijing, China, May 2008.

[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, pp616?29,2011.

[7]. M. Raya and J. P. Hubaux, “Securing Vehicular Ad-Hoc networks,” Journal of Computer Security, Vol. 15, No. 1, pp. 39-68, 2007.

[8]. A. Perrig, R. Canneti, D. Song, and J.D. Tygar,”” The TELSA broadcast authentication protocol,” RSA Cryptobytes, vol.5,no. 2, pp. 2-13,2002.

[9]. C.-P. Schnorr,”Efficient identification and signature for smart cards,” in Proc. of the 9th Annual International Cryptology Conference (Advances in Cryptology- CRYTO), Santa Barbara, California, USA, pp. 239-252, 1989.

[10]. X. Lin, X.Sun, X. Wang, C. Zhang, P-H. Ho, and X. Shen, “TSVC: Time efficient and secure vehicular communications with privacy preserving,” IEEE Transaction on Wireless Communications, vol. 7, no. 12, DECEMBER 2008.