INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

EVIDENCE TOKEN APPROACH TO ACHIEVE MESSAGE AUTHENTICATION AND RESIST ATTACKS IN VANETS

N.Navaneeth
PG scholar
Electronics and Communication Engineering
PSNA College of Engineering and Technology
navanu901@gmail.com

Dr.C.Chitra
Professor
Electronics and Communication Engineering
PSNA college of Engineering and Technology
chitrasrivi@gmail.com

ABSTRACT
Vehicular ad hoc networks (VANETs) have emerged as a promising approach to increasing road safety and efficiency, as well as improving the driving experience. This can be accomplished in a variety of applications that involve communication between vehicles, such as warning other vehicles about emergency braking; 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. When the number of messages that are received by a vehicle becomes large, traditional exhaustive authentication may generate unaffordable computational overhead on the vehicle and therefore bring unacceptable delay to time-critical applications, such as accident warning. Hence we propose an efficient cooperative authentication scheme for VANETs. Through extensive simulation we evaluate the proposed cooperative authentication scheme in terms of workload savings and the ability to resist free-riding attacks.

Keywords: VANETs, RSU, Token Mechanism.

I. 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 manufacturers 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 that are 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 roadside units (RSUs), using a dedicated short-range communications technique. 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. Applications, such as emergency-braking warning, are made possible by communication between vehicles. By using VANETs, travellers can achieve improved driving safety and comfort. For example, each vehicle user may periodically broadcast its proximal traffic information to others, enabling them to take early action to avoid car accidents. Moreover, nearby vehicle users can share specific information with each other, such as road conditions, tourism information, music, movie files, or hotel information, making themselves more comfortable and knowledgeable during their journeys. Indeed, due to their enormous potential and social impact, VANETs have drawn considerable research attention from both academia and industry, and many prototype applications have already been developed; however, before implementing these promising applications, particularly safety-related ones, VANET-related security problems must be addressed and resolved.

One fundamental security problem in VANETs is message authentication. Achieving message authentication consists of two essential security checks, i.e., an integrity check and 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 the literature and can be mainly divided into the following two categories: traditional public-key-infrastructure (PKI)-based digital signature schemes and group signature-based security schemes. In both categories, each message needs to be signed by the sender using an asymmetric algorithm, and its receiver needs to verify the message that is 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. Particularly as the 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.

II. RELATED WORK

Trusted security mechanisms and protocols have been recently developed to ensure secure privacy-preserving vehicular communications they can be classified as public-key-cryptography based or secret-key cryptography based solutions. Protocols using a PKC approach can be further classified into two subcategories: traditional PKI-based digital signature techniques and group-signature techniques. In the first subcategory, the anonymous public-key certificate of Raya and Hubaux is the first noteworthy attempt to ensure security and privacy in vehicular communications, while also preserving the ability to trace messages back to their senders. Raya and Hubaux proposed a protocol for secure vehicular communication. Each vehicle is preloaded with a large number of private keys, as well as their corresponding anonymous certificates. The sending vehicle then randomly selects one of the anonymous certificates, using its corresponding private key to digitally sign messages to be sent.

To verify the integrity of the message received, other vehicles use the sender's public key associated with this signature. Each anonymous certificate has only a short lifespan to meet the driver's privacy requirements. Unlike traditional public-key certificates, anonymous certificates are generated using the pseudo identities of the vehicles, instead of identifying information from the driver. Each driver's entire list of anonymous certificates, which is mapped to the driver's real identity, is kept by the authority, allowing messages to be traced back to the driver in the event of a dispute. In the latter subcategory, Lin *et al.* discovered the fact that the unique characteristics of group signature, which is an important cryptographic primitive, perfectly match the security and privacy requirements in VANETs. By taking different security and privacy requirements of two types of VANET communications into account, namely, vehicle-to-infrastructure and vehicle-to-vehicle communications, they propose a novel secure and privacy-preserving protocol for vehicular communication, based on a combination of group signature and identity (ID)-based signature techniques. Zhang *et al.* proposed an efficient authentication protocol for vehicular communication, using an efficient cryptographic primitive, which is called a batch signature. It allows an RSU to simultaneously verify multiple signatures, significantly reducing the message verification overhead of the RSU as a result. Unfortunately, the inherent weakness of batch verification (verifying multiple digital signatures in a batch mode) makes it vulnerable to DoS attacks caused by the injection of false data.

Recently, a cooperative approach, known as cooperative message authentication, has been explored to deal with this challenging situation. Lin proposes a cooperative message validation protocol, where each vehicle probabilistically validates a certain percentage of its received messages, in accordance with its own computing capacity, and reports

any invalid messages that are detected. The protocol relies on the assumption that each individual vehicle is willing to contribute its computing resources and participate in a cooperative effort for message authentication. In reality, there will always be some selfish vehicles that do not want to make such contribution and only want to take advantage of others' efforts. Hao *et al.* proposed a distributed cooperative message authentication scheme, aimed at reducing the number of verifiers for a single message.

III.PROPOSED SYSTEM

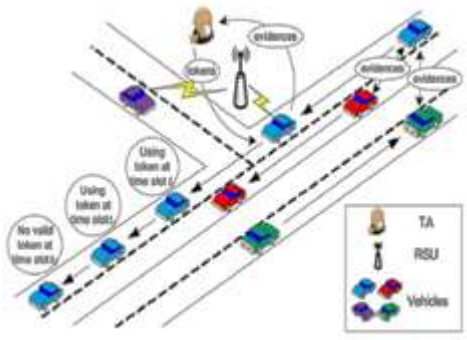


Figure 1 Evidence Token Mechanism

Evidence token mechanism

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 (trusted Authority) will be responsible for maintaining the balance according to the time slots. It receives the evidences from vehicles via RSUs when vehicles pass by the RSUs, and it sends the tokens back to the 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 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.

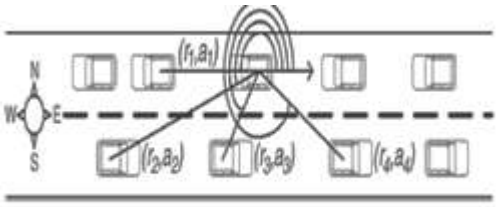


Figure 2 Secure Cooperative Authentication Scheme

Secure Cooperative Authentication Scheme

Vehicle authenticates some of the original signatures that are 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 in 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. Since evidence generation and transmission consume energy, the number of evidences that are generated per vehicle should be limited. 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 via with multiple tokens according to the provided evidences.

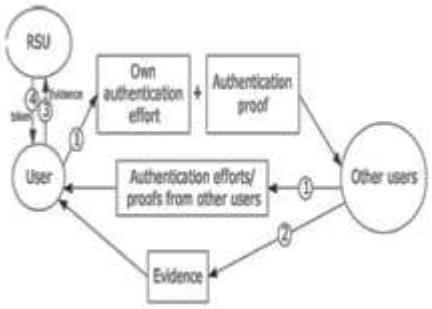
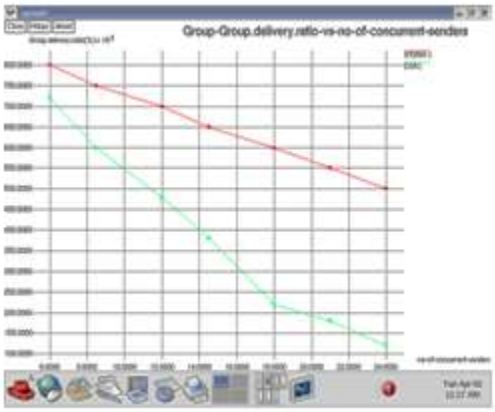


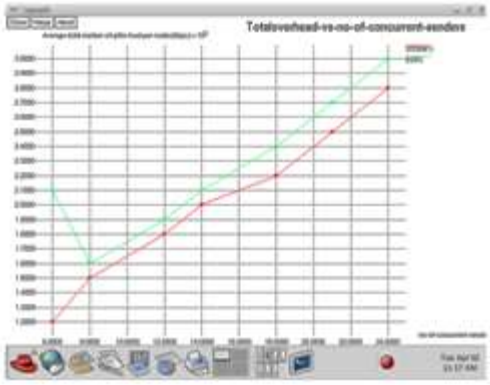
Figure 3 Polar Coordinates of Vehicles

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.

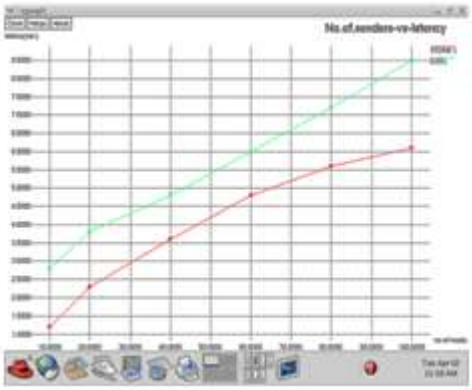
IV.SIMULATION RESULTS



Group Delivery Ratio



Overhead Analysis



Latency Analysis

Parameters	DSR PROTOCOL	Proposed Method
Group Delivery Ratio	0.725	0.8
Total Overhead	3642841	2891643
Latency	85 sec	54sec

Performance Comparison

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. 27th IEEE INFOCOM*, Phoenix, AZ, USA, 2008, pp. 246–250.
[2] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.
[3] X. Liang, R. Lu, X. Lin, and X. Shen, "PPC: Privacy-preserving chatting in vehicular peer-to-peer networks," in *Proc. 72nd IEEE VTC*, Ottawa, ON, Canada, 2010, pp. 1–5.

[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. 30th IEEE INFOCOM*, Shanghai, China, 2011, pp. 2147–2155.
[5] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, Jan. 2007.
[6] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 616–629, Mar. 2011.
[7] "Veh. safety commun. project final report. Appendix H: WAVE/DSRC security," Nat. Highway Traffic Safety Admin., Washington, DC, USA, Apr. 2006.
IEEE Trans. Wireless Commun., vol. 7, no. 12, pp. 4987–4998, Dec. 2008.
Summer/Fall 2002.

AUTHOR's PROFILE

Mr N. Navaneeth was born at Nilgiris, India in 1990. He graduated in Electronics and Communication Engineering from Anna University Coimbatore, India in the year 2011 and pursuing his post-graduation in Applied Electronics from Anna University Chennai, India in the year 2014 respectively. His fields of interest include Computer Networks and Network Security.

Ms C. Chitra was born at Dindigul, India in 1974. She graduated in Electronics and Communication Engineering and post graduated in Digital Communication and Network Engineering from Madurai Kamaraj University, India in the year 1996 and 2002 respectively. She obtained her PhD degree in the year 2012 from Anna University, Chennai, India. She has a teaching experience of thirteen years. Her fields of interest include Computer Networks, Satellite Communication and Network Security.