Research Paper

Volume : 3 | Issue : 5 | May 2014 • ISSN No 2277 - 8179

Survey on Various Approaches to Message Authentication System for VANETS

Engineering

KEYWORDS : Wireless Technology, Vehicular Ad hoc Networks, Message Authentication.

Ranjitha P — Final Year M.Tech CSE, Vedavyasa Institute of Technology,Calicut

Dr. Sangheethaa S — Professor, Department of CSE, Vedavyasa Institute of Technology, Calicut

ABSTRACT

The number of automobiles has been increased on the road in the past few years. Due to high density of vehicles, the potential threats and road accident is increasing. Wireless technology is aiming to equip technology in vehicles to reduce these factors by sending messages to each other. VANETs have emerged as a promising approach to increasing road safety and efficiency. This can be accomplished in a variety of applications that involve communication between vehicles, such as warning other vehicles about emergency braking etc. Message authentication is a common tool for ensuring information reliability, namely, data integrity and authenticity. When the number of messages that are received by a vehicle becomes large, traditional authentication may generate unaffordable computational overhead on the vehicle and therefore bring unacceptable delay to time-critical applications.

I. INTRODUCTION

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). However, 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 (DSRC). These vehicles are equipped with wireless On-Board Units (OBUs), which perform the communication. The VANET enables numerous services through a variety of vehicle applications, such as emergency-braking warning, etc. One fundamental security problem in VANET 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. A 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.VANET is still a virgin research area. Most of the road vehicles will receive messages, and they won't be considering all of these messages, as not all vehicles have a good intention and some of them are evil-minded. And so it is critical for VANET to guard against those activities that poses different threats.

An efficient cooperative message authentication scheme is adopted that does not directly involve a Trusted Authority (TA). This scheme is carried out by a set of neighbouring vehicle users; with minimal intervehicle coordination, the scheme minimizes redundant authentication efforts of different vehicles working on the same message. It also encourages cooperation and resists free-riding attacks. Various Message authentication approaches are described in this paper.

VANET Technology

This section depicts the VANET technology and various security concerns in VANET. The purpose of the study and the scope is discussed along with recent applications. Taking into account message authentication as one of the fundamental security issue in VANET, it is well explained with the needed data.

VANETs are subgroup of Mobile Ad hoc Networks (MANETs) with the distinguishing property that the nodes are vehicles like cars, trucks, buses and motorcycles. The primary goal of VANETs is to increase road safety. To achieve this, the vehicles act as sensors and exchange warnings**.** A VANET uses moving cars as nodes in a network to create a transportation network. A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. In VANET, rather than moving at random, vehicles tend to move in an organized fashion.

Security Issues in VANET

Security is more crucial in VANETs due to involvement of critical life threatening situations. Some of the security issues are in handling malicious/misbehaving as well as faulty nodes. The attackers may be insider, outsider, malicious or rational. Handling message attacks include bogus information, false positioning, privacy (disclosure of ID), denial of service and masquerading. Communication is mainly performed based on exchange of messages. Security largely depends on trust worthiness of messages that are exchanged between the nodes. On the other hand, security in VANET can be established by valid communication between trusted vehicles/nodes. Taking into account the message authentication as a security concern, the following section presents a brief idea regarding message authentication in VANETs.

The remainder of this paper is structured as follows. Section II provides a description of related research studies performed. An overview of the message authentication scheme is presented in Section III along with the comparative table. Finally, section IV concludes the paper

II. RELATED WORK

This section presents some of the most popular research works related to the message authentication scheme.

The concept of AEMA [3] was described by Haojin Zhu in the year 2008. The concept of AEMA was to achieve efficient authentication on emergency events in VANETs. This mainly incurs to validate an emergency event. For reducing the transmission cost, the author made use of syntactic aggregation and cryptographic aggregation technique. According to Haojin Zhu, "During the emergency messages opportunistic data forwarding process, a vehicle can hold multiple message which can be aggregated into a single one before the vehicle launches aggregated message in the air". This paper adopts a batch verification technique for efficient emergency message verification to reduce the computation cost. The fast propagation of emergency and local warning messages to the approaching vehicles will be helpful for preventing secondary accidents. In most cases, a VANET carries out such emergency message propagation in a multihop transmission manner, particularly in the suburban areas where less RSU are installed. In particular, there launched a voting mechanism in which crosschecking the emergency event by collecting the feedback of witnesses was defined which was originally used to detect the misbehaving nodes in a distributed ad hoc network without any centralized security authority. The mechanism can be migrated to VANETs to enhance the overall security of emergency events authentication. A voting scheme was implemented on location based groups, where vehicles are grouped according to their location. According to the author, the

voting mechanism effectively improves the security of VANET at the expense of increased computation and transmission overhead.

III. MESSAGE AUTHENTICATION SCHEME

A. Research Objectives

The objective of this research is to

- Present a survey on various Message Authentication approaches in VANET.
- Study the security issues in VANET.
- Compare different approaches in Message authentication.

B. Message Authentication

Message authentication is a security measure in which the sender of the message is verified for every message sent. Message authentication is considered as one of the major security problem in VANET. Message authentication allows one party say the sender to send a message to another party say the receiver in such a way that if the message is modified in route, then the receiver will almost certainly detect this. Message authentication is also called data-origin authentication. Message authentication is said to protect the integrity of a message, ensuring that each message that it is received and deemed acceptable is arriving in the same condition that it was sent out with no bits inserted, missing, or modified. 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. A 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.

The considered threats can be summarized as follows:

Linkability attack: Authentication linkability helps the TA to identify misbehaving users. In the 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 to avoid being punished.

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

Free-riding attack with fake authentication efforts (or active free-riding attack): Active free-riding attack is launched by an active malicious user who participates in the cooperative authentication protocol by generating fake authentication efforts. In a cooperative authentication environment, 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 authenticate any original message but provide valid verification efforts because these signatures have been checked by others. The active attack is more intelligent than the passive attack. It can be hardly detected by nearby users or the TA.

Message Authentication Approaches

Researches in secure authentication and privacy protection have been quite active in recent years. Numbers of schemes have been proposed. According to the pattern in which messages are verified, these existing authentication schemes can be classified into two categories, i.e., one-by-one message verification [2], [7], [11] and batch verification [4], [12] schemes.

GSIS: GSIS [2] is a Secure and Privacy-Preserving Protocol for Vehicular Communications that eliminates the public key certificates. A secure and privacy preserving protocol for VANETs by integrating the techniques of Group Signature and Identity (ID)-based Signature, called (GSIS).

Security problems are divided into the following two aspects: security and privacy preservation between OBUs and OBUs, as well as that between the OBUs and the RSUs, in light of their different design requirements. In the first aspect, group signature is used to secure the communication between OBUs and OBUs, where messages can securely and anonymously be signed by the senders, while the identities of the senders can be recovered by the authorities. In the second aspect, a signature scheme using ID-based cryptography (IBC) is adopted in the RSUs to digitally sign each message launched by the RSUs to ensure its authenticity, where the signature overhead can greatly be reduced.

By adopting any publicly known ID of an RSU or an emergency vehicle, such as the location of the RSU or the emergency vehicle's license plate number, as the public key, the certificate management in the VANETs can greatly be simplified as compared with that in the traditional public key infrastructure.

STAP: Social-Tier-Assisted Packet forwarding protocol [8] assist in achieving receiver-location privacy preservation in VANETs, where the social tier is a virtual tier formed by social spots, such as well-traversed shopping malls and busy intersections in a city environment. The STAP protocol is characterized by disseminating packets to social tier in order to not only improve the packet delivery performance but also protect receiver-location privacy against an active global adversary.

Vehicles often visit some social spots, such as well-traversed shopping malls and busy intersections in a city environment, deploy storage-rich Road Side Units (RSUs) at social spots and form a virtual social tier with them. Then, without knowing the receiver's exact location information, a packet can be first forwarded and disseminated in the social tier. Later, once the receiver visits one of social spots, it can successfully receive the packet.

CMAP: cooperative message authentication protocol (CMAP) [7] describes with an assumption that each safety message carries the location information of the sender vehicle (which can be generated by a global positioning system (GPS) device). Verifiers of each message are defined according to their locations in relation to the sender. Only the selected verifiers check the validity of the message while other vehicles rely on verification results from these verifiers. RSU authenticated message one by one and broadcasted 128B hash value for each valid message, which brought heavy communication burden. CMAP [12] embraced cooperation verification idea to improve efficiency. Verifiers were chosen based on location, and non-verifiers waited for the verifier's results. Due to the uncertainty of the vehicle speed and road conditions, the scalability and practicality of CMAP are facing questioning.

IBV: IBV [4] devised identity based (ID-based) signature to realize batch verification. To avoid any possible malicious attack and resource abuse, employing a digital signature scheme is widely recognized as the most effective approach for VSNs to achieve authentication, integrity, and validity. However, when the number of signatures received by a Roadside Unit (RSU) becomes large, a scalability problem emerges immediately, where the RSU could be difficult to sequentially verify each received signature within 300 ms interval according to the current Dedicated Short Range Communications (DSRC) broadcast protocol. An efficient batch signature verification scheme for communications between vehicles and RSUs (or termed vehicle- to-Infrastructure (V2I) communications), in which an RSU can verify multiple received signatures at the same time such that the total verification time can be dramatically reduced.

RAISE: RAISE is a RSU-assisted verification scheme [5]. Secret key shared between vehicle and RSU was used to generate message authentication code (MAC). With RAISE, roadside units (RSUs) are responsible for verifying the authenticity of the messages sent from vehicles and for notifying the results back to vehicles. In addition, this scheme adopts the k-anonymity approach to protect user identity privacy, where an adversary cannot associate a message with a particular vehicle.

CPAS: CPAS adopted pseudonyms to protect privacy and realize batch verification [12] between the vehicle and the RSU. But

the Private Key Generator (PKG) is essential to generate user private key, i.e. key escrow. In addition, signature verification is based on bilinear pairing operation which is of large computational overhead.

The comparison of the aforementioned programs is shown as Table 1, from which we can see they are all not applicable to emergency communication, as roadside infrastructures are assumed to cover the entire network in all the schemes.

Table I. Comparison of message authentication approaches

Message Authentication Approaches	Communication patterns	Cryptographic style	Batch Verification	Emergency Communication	
				No RSU	Vehicle Group Communication
GSIS	V2V & V2R	Group & ID-based Signature	No	No	No
STAP	V2R	Group Signature	No	No	No
CMAP	V2V	Group Signature	No	No	No
IBV	V2R	ID-based Signature	No	No	No
RAISE	RSU based V2V	PKI Signature & MAC Code	Yes	No	No
CPAS	V2R	ID-based Signature with PKG	Yes	No	No

IV CONCLUSION

The major contribution of this paper is the study and comparison of related papers. Various privacy preserving, security, batch verification and message authentication schemes are introduced. In addition, Different message authentication approaches has been compared with several parameters.

REFERENCE

[1] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," in Proceedings of VANET' 07, Montreal, Quebec, Canada, pp. 19–28, September 2007. | [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] H. Zhu, X. Lin, R. Lu, Pin-Han Ho, X. Shen "AEMA: An Aggregated Emergency Message Authentication Scheme for Enhancing the Security of Vehicular Ad Hoc Networks", IEEE Trans, pp. 1436-1440, May 2008. | [4] 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, pp. 246–250, 2008. | [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. IEEE ICC, Beijing, China, pp. 1451–1457, May 2008. | [6] C. Zhang, X. Lin, R. Lu, P.-H. Ho and X. Shen, "An efficient message authentication scheme for vehicular communications," IEEE Trans. Veh. Technol., vol. 57, no. 6, pp. 3357-3368, 2008. | [7] 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. | [8] 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, pp. 2147–2155, 2011. | [9] A. Perrig, R. Canneti, D. Song, and J. D. Tygar, "The TESLA broadcast authentication protocol," RSA Crypto., vol. 5, no. 2, pp. 2–13, 2002. | [10] X Jia, X. Yuan, L. Meng, L. Wang, "EPAS: Efficient Privacy-preserving Authentication Scheme for VANETs-based Emergency Communication", journal of software, vol. 8, no. 8, august 2013. | [11] C Zhang, X Lin, R Lu, P-H Ho, X. Shen, "An efficient message authentication scheme for vehicular communications", IEEE Transaction Vehicular Technology, vol. 57, no. 6, pp. 3357-3368, Nov. 2008. | [12] K-A Shim, "CPAS: An Efficient Conditional Privacy- Preserving Authentication Scheme for Vehicular Sensor Networks". IEEE Transactions on Vehicular Technology, vol.61, no.4, pp.1874-1883, May 2012. |