A Practical and Extendible VANETs Privacy-Preserving System

Yang Tao, Hu Jian-Bin, and Chen Zhong
MoE Key Lab of High Confidence Software Technologies, Peking University, Beijing, 100871, China
MoE Key Lab of Computer Networks and Information Security, Peking University, Beijing, 100871, China
School of Electronics Engineering and Computer Science, Peking University, Beijing, 100871, China
{ytao, hujb,chen}@infosec.pku.edu.cn

***Abstract*—VANETs are the academic and industry research priorities in recent years. Security and privacy-preserving have become a bottleneck for VANETs' future developing. There are few literatures about the architecture of VANETs privacy-protecting system. In this paper, we introduce a practical VANETs Privacy-Preserving System which aims to the prior location and identity privacy protecting. We propose the architecture and do some close analysis about that. The proposed system is based on the key technologies such as TP4RS protocol, and achieves some good features: the system not only can provide good identity and location privacy protecting for the vehicles, but also can be implemented and deployed well because of its practical design and expandability. To the best of our knowledge, our scheme is the first architecture design scheme for the practical VANETs privacy protecting system.**

***Index Terms*—vehicular ad-hoc networks, privacy-preserving, message authentication, traceability**

I. Introduction

Vehicular ad hoc networks (VANETs) are instances of mobile ad hoc networks with the aim to enhance the safety and efficiency of road traffic. And more, VANETs can provide various value-added infotainment services (such as location based service) on the road. Typically, in a VANET, Equipped with communication devices, alias On-Board Unit (OBU), vehicles can communicate with each other (V-2-V communication mode) or with the RoadSide Units (RSUs) located at critical points of the road (V-2-I communication mode), such as intersections or construction sites. The Transportation Regulation Center (TRC) is in charge of the registration of all RSUs and OBUs each vehicle is equipped with. The TRC can reveal the real identity of a safety message sender by incorporating with its subordinate RSUs.

According to the Dedicated Short Range Communications (DSRC), each vehicle equipped with OBU will broadcast routine traffic messages, such as the position, current time, direction, speed, acceleration/deceleration, and traffic events, etc. In this way, drivers can get better awareness of the driving environment and take early actions to the abnormal situation to improve the safety of both vehicle drivers and passengers.

However, before the above attractive applications come into reality, the security and privacy issues should be addressed. Otherwise, a VANET could be subject to many security threats, which will lead to increasing malicious attacks and service abuses. More precisely, an adversary can either forge bogus messages to mislead other drivers or track the locations of the intended vehicles. Therefore, the security and privacy is the key to the VANETs, and has been well-studied in recent years.

Since the vehicle is extremely personal device, its communication data should be secured and the driver's privacy should be unrevealed. Generally, privacy means "Right of an individual to decide when and on what terms his or her attributes should be revealed" [1]. Driver's attributes such as 5W1H (who, when, where, what, why, and how) can be revealed and utilized by adversaries without privacy-protecting. In the context of VANETs, privacy can be categorized into three parts [2]: 1) Data Privacy: prevent others from obtaining communication data. 2) Identity Privacy: prevent others from identifying subject of communication. 3) Location Privacy: prevent others from learning one's current or past location. Usually, data privacy easily achieved through encryption method in an application layer. So identity and location privacy are usually mentioned as the privacy issues on VANETs.

To address these issues, this paper proposes a practical and extendible privacy preserving system for VANETs. Our scheme has the following unparalleled features:

Achieving practical goal: The system has been designed as a practical-first system. According to the real vehicle environment, especially to the real transportation management status, the system can be implemented smoothly because of its practical-oriented.

Achieving secure goal: The system exploit many secure protocols and secure attack-protecting mechanism to get this target. And more, for preventing the right abusing or misusing, some decentralized mechanism has been adopted.

Achieving extendible goal: The system can efficiently deal with a growing secure protocols and applications, and does not rely on a large modification.

II. Related Work

doi: 10.12720/joace.1.2.166-169

Security and privacy in VANETs raise many challenging research issues that have been studied in the literature. Raya et al. introduced the landmark HAB [3], [4] protocol, and the key idea is to install on each OBU a large number of private keys and their corresponding anonymous certificates. To sign each launched message, a vehicle randomly selects one of its anonymous certificates and uses its corresponding private key. The other vehicles use the public key of the sender enclosed with the anonymous certificate to authenticate the source of the message. These anonymous certificates are generated by employing the pseudo-identity of the vehicles, instead of taking any real identity information of the drivers. Each certificate has a short life time to meet the drivers' privacy requirement. Although HAB protocol can effectively meet the conditional privacy requirement, it is inefficient and may become a scalability bottleneck.

Lin *et al.* proposed the GSB [5], [6] protocol. With GSB, each vehicle stores only a private key and a group public key. Messages are signed using the group signature scheme without revealing any identity information to the public. Thus privacy is preserved while TRC is able to track the identity of a sender. However, the time for safety message verification grows linearly with the number of revoked vehicles in the revocation list in the entire network. Hence, each vehicle has to spend additional time on safety message verification. Furthermore, when the number of revoked vehicles in the revocation list is larger than some threshold, it requires every remaining vehicle to calculate a new private key and group public key based on the exhaustive list of revoked vehicles whenever a vehicle is revoked.

Guo *et al.* proposed GBW [7] scheme， which included a VANETs Secure and Privacy-Preserving Communication Framework based on group signature, as shown in the Fig. 1.

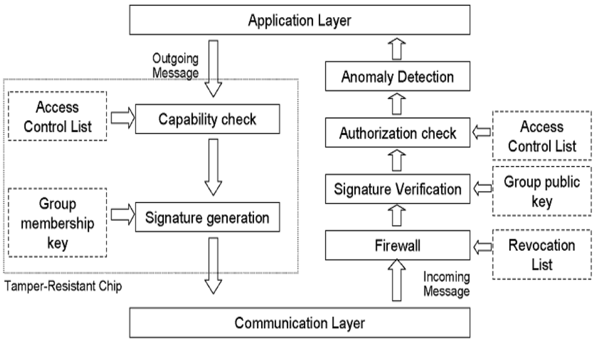

Figure 1. Secure and privacy-preserving communication framework

There are six fundamental components of the security layer of our framework. These six components are formalized as follows: capability check, signature generation, firewall, signature verification, authorization check, and anomaly detection.

Lu *et al.* [8] introduced an efficient conditional privacy preservation protocol (ECPP) based on generating on-the-fly short-lived anonymous keys for the communication between vehicles and RSUs. ECPP used RSUs as the source of certificates. In such an approach, RSUs (as opposed to OBUs) check the group signature to verify if the sender has been revoked and record values to allow tracing. OBUs then use a RSU provided certificate to achieve authenticity and short-term linkability. However, ECPP is vulnerable to Sybil attacks and requires an unreasonable amount of computation for RSUs (i.e., linear in the size of the revocation information for every certificate request).

Lu *et al.* [9] proposed SPRING based on ECPP and first introduced social network into VANETs. The scheme deployed limited RSU in the high-social intersection to improve the performance of the VDTN. Lu et al. proposed SPF [10] based on the Social Spot (the place which vehicle often visit, such as shopping mall, cinema, etc.). RSUs were deployed in the Social Spots and act as Mix Server to protect OBUs' privacy.

III. THE SYSTEM

Fig. 2 describes the system architecture.

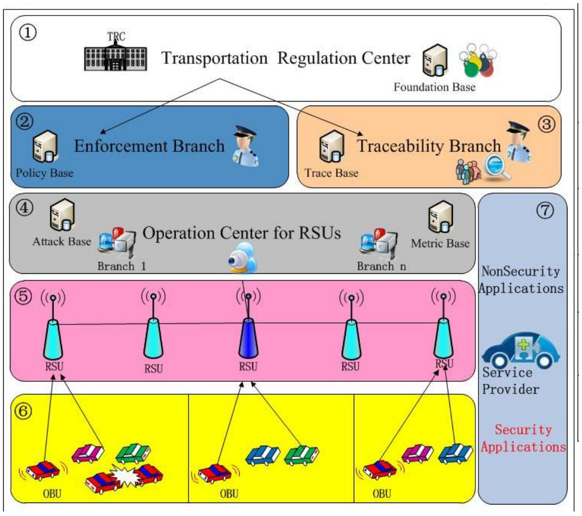

Figure 2. System architecture

As shown in the Fig. 2, the most important seven subsystems include:

Management Center Subsystem: in charge of the whole management of the system. It includes the parameter configuration base and the Foundation Base. It comprises the key modules as following: grant modules (such as authentication grant, and trace grant, etc.), key management module, cryptographic engine module, policy management module, log audit module, visual presentation module, etc.

Management Branch Center Subsystem: in charge of the part management of the system granted by TRC. It provides the vehicle (in the area) identity request and cancel request, formulates the secure policies in the area, and supervises the execution of the policies. The subsystem includes the policy base. The subsystem comprises the key modules as following: policy management module, key management module, cryptographic engine module, log audit module, visual presentation module, etc.

Trace & Audit Branch Center Subsystem: in charge of the event trace lifecycle. It should provide accurate vehicle ID locate service. The service has been strictly controlled to prevent the abusing or misusing. It includes the trace base in the area. The subsystem comprises the key modules as following: the trace entity management module, the trace algorithm module, log audit module, visual presentation module, etc.

Operation Center for RSUs Subsystem: in charge of the operation of RSUs. The subsystem guarantees the RSUs continuous, secure and efficient. It includes the attack base and metric base, and monitors the RSUs network real-time. It aims to dynamically blockage the attack, periodically reinforce and periodically measure. The center could be divided into some branches according to the scale and the area for the more accurate operation. It comprises the key modules as following: the real-time monitor module, the emergency response module, the intrusion detecting module, patrol and examine module, policy management module, log audit module, visual presentation module, etc.

RSU Subsystem: in charge of the RSUs' secure configuration, protocol management and cooperation with each other. It comprises the key modules as following: key management module, cryptographic engine module, policy enforcement module, configuration protecting module, secure protocol module (include the identity-privacy protecting protocol and the location-privacy protecting protocol), log audit module, local-storage management module, information dump module, time synchronous module, communication management module, etc. The secure protocol module should have high expandability to constantly support the new protocol.

OBU Subsystem: in charge of the OBUs' secure configuration, protocol management and cooperation with each other. The subsystem comprises the key modules as following: key management module, cryptographic engine module, policy enforcement module, configuration protecting module, secure protocol module (include the identity-privacy protecting protocol and the location-privacy protecting protocol), log audit module, local-storage management module, information dump module, time synchronous module, communication management module, power management module, etc. The secure protocol module should have high expandability to constantly support the new protocol.

Application Cluster: in charge of the applications (include security application and non-security application) based on VANETs. Because of the capriciousness of the applications, it must have high expandability to adapt to the new-adding applications and the patch for the old applications. It comprises the key modules as following: standardized application access module, application audit module, account management module, access control module, billing management module.

IV. Key Technology Analysis

A. TP4RS Protocol

We exploit the TP4RS [11] protocol to implement a security and identity-privacy protecting application. TP4RS is a traceable privacy-preserving communication protocol for VANETs based on a single hop proxy re-signature in the standard model, The protocol has some appealing features: The TRC designates the RSUs translating signatures computed by the OBUs into one that is valid as for TRC's public key. The potential danger that vehicles could be traced by the signatures on messages can be deleted, and attacks are thwarted by using an endorsement based on signatures.

B. RSU Host Protecting

RSU host compromise is one of the most serious security problems in our system. However, most existing integrity protection models for operating systems are difficult to use; on the other hand, available integrity protection models only provide limited security protection. We will use a novel security and practical integrity protection model (SecGuard [12]) for RSU host protecting.

V. Conclusion

This paper proposes architecture of the privacy-preserving system, and then do some close analysis about that. The proposed system is based on the key technologies such as TP4RS protocol, and achieves some good features: the system not only can provide good identity and location privacy protecting for the vehicles, but also can be implemented and deployed well because of its practice-based design and expandability. We break down it to multiple subsystems, such as management subsystem, sub-management subsystem, trace-event audit subsystem, RSU maintenance subsystem, RSU subsystem, OBU subsystem, application subsystem.

References

[1] S. T. Kent and L. I. Millett, *IDs--not that easy: questions about nationwide identity systems*, National Academy Press, 2002.

[2] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *Pervasive Computing, IEEE*, vol. 2, no. 1, pp. 46-55, 2003.

[3] M. Raya, A. Aziz, and J. P. Hubaux, "Efficient secure aggregation in VANETs," in *Proc. 3rd international workshop on Vehicular Ad-hoc Networks*, 2006, pp. 67-75.

[4] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39-68, 2007.

[5] X. Lin, X. Sun, and P. H. Ho, et al., "GSIS: a secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3443-3456, 2007.

[6] X. Lin, R. Lu, C. Zhang, *et al.*, "Security in vehicular ad hoc networks," *Communications Magazine, IEEE*, vol. 46, no. 4, pp. 88-95, 2008.

[7] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *Proc. Mobile Networking for Vehicular Environments*, 2007, pp. 103-108.

[8] R. Lu, X. Lin, H. Zhu, *et al.*, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. The 27th IEEE Conference on Computer Communications, 2008*, pp. 1229-1237.

[9] R. Lu, X. Lin, and X. Shen, "Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *INFOCOM*, 2010, pp. 1-9.

[10] R. Lu, X. Lin, X. Liang, *et al.*, "Sacrificing the Plum Tree for the Peach Tree: A Socialspot Tactic for Protecting Receiver-location Privacy in VANET," in *Proc. Global Telecommunications Conference*, 2010, pp. 1-5.

[11] T. Yang, H. Xiong, *et al.*, "A traceable privacy preserving authentication protocol for vanets based on proxy re-signature," in *Proc. Eighth International Conference on Fuzzy Systems and Knowledge Discovery*, 2011, pp. 2270-2274.

[12] E. N. Zhai, Q. N. Shen, *et al.* "Secguard: Secure and practical integrity protection model for operating systems," in Proc. *13th Asia-Pacific Web Conference*, 2011, pp. 370-375.

Tao Yang, born in 1976, Ph. D. candidate. His major research interests are wireless sensor networks security, Cloud security, IoT security, VANETs security and privacy protecting, proxy signatures, and security operation system.