# Authenticating and tracing biological anonym of VANET based on KMC decentralization and two-factor

**Conference Paper** · June 2013

DOI: 10.1145/2462456.2465712

CITATIONS
2

READS
35

**5 authors**, including:

Fei Wang
Chinese Academy of Sciences
**67** PUBLICATIONS **2,355** CITATIONS
SEE PROFILE

Yong-Jun Xu
Chinese Academy of Sciences
**243** PUBLICATIONS **4,188** CITATIONS
SEE PROFILE

Lin Wu
Chinese Academy of Sciences
**27** PUBLICATIONS **498** CITATIONS
SEE PROFILE

Dan Liu
Beijing University of Technology
**6** PUBLICATIONS **153** CITATIONS
SEE PROFILE

# Poster: Authenticating and Tracing Biological Anonym of VANET Based on KMC Decentralization and Two-Factor

Fei Wang[1, 2], Yongjun Xu[1], Lin Wu[1, 2], Dan Liu[3] and Liehuang Zhu[3]

[1]Institute of Computing Technology, Chinese Academy of Sciences, P. R. China
[2]University of Chinese Academy of Sciences, P. R. China
[3]School of Computer Science, Beijing Institute of Technology, P. R. China
E-mail: {wangfei, xyj, wulin}@ict.ac.cn, {liudanking, liehuangz}@bit.edu.cn

## Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General——*Security and Protection*;
C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design——*Wireless communications*

## Keywords

VANET; Privacy Preservation; Authentication; Two-Factor; Decentralization; Conditional Traceability

## 1. Motivation

Some previous privacy preserving authentication (PPA) schemes for vehicular ad-hoc network (VANET) are able to secure vehicle-to-vehicle (V2V) communication, and trace a vehicle conditionally. However due to centralized key management center (KMC), few could jump out scope of asymmetric key mechanism, thus corresponding cost is too high to suit broadcasting scenarios especially with high vehicle density. Plus, the tracing can't reach a single one of many biological drivers of one vehicle. So we consider an improved solution based on two ideas: 1) Decentralizing KMC by giving its duties to tamper-proof device (TPD); 2) Utilizing two-factor authentication (2FA) to integrate biological identifiers of drivers into messages. Overview is shown in Figure 1. The objective is to both authenticate anonymous drivers faster and provide enough evidences to trace any biological anonym driver.

## 2. Decentralizing KMC to improve efficiency

Cryptographic values and code are stored in TPD and can't be extracted in any circumstance. Thus vehicles can only do limited operations indirectly with system key. A vehicle registers itself to KMC to configure its TPD (system key and an initial pseudo identity (PID) written to TPD) and applies for access token of TPD. Before sending a message, a vehicle logs on TPD with access token and signs the message with PID generated by TPD based on initial PID. A receiver verifies received messages with matching PIDs. This benefits VANET PPA in 4 aspects compared with GSIS [1] and STAP [2]: 1) V2V authentication is $10^2$~$10^5$ times quicker based on symmetric key mechanism or 2FA; 2) Bandwidth consumption decreases by 41.33% ~77.60%; 3) Cost of KMC's certificate revocation list is removed; 4) Mitigated role of roadside units (RSUs) makes it hard to reveal real identities even with all RSUs compromised.



*MobiSys'13*, June 25–28, 2013, Taipei, Taiwan.

ACM 978-1-4503-1672-9/13/06.

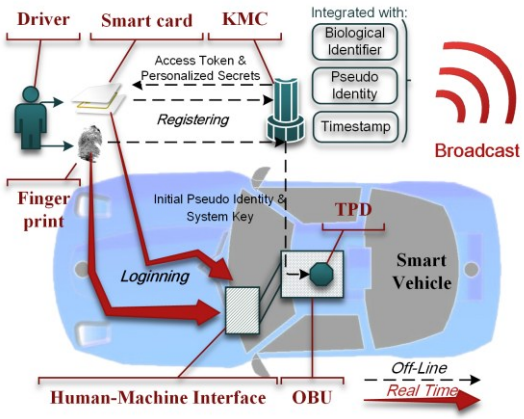


**Figure 1. Overview of Proposed Solution.**

## 3. Tracing Biological Anonym Utilizing 2FA

Multiple drivers of a vehicle might cause confusions when authorities need to reveal the real identities in case of accident investigation and other disputes. Moreover, smart vehicle is hot with advanced human-machine interface (e.g., tablet with fingerprint or iris scanner). Thus we uses 2FA which employs "something you have" (smart card) and "something you are" (biological identifier) to trace a single biological anonym driver conditionally. KMC utilizes submitted biological identifiers to generate personalized secret values and write them into a smart card. A driver needs to plug smart card and input biological identifier to pass the verification of human-machine interface. Then he is free to log on TPD and participate in VANET application. In V2V communication, PIDs are generated with initial PIDs by TPD, biological information and timestamps. Thus, any V2V message could be used by KMC to trace its biological author with privacy preserving. Moreover, 2FA is much faster than existing PPA schemes.

This poster shows an opportunity of using decentralized KMC to improve efficiency of PPA in VANET and using 2FA to trace any biological anonym.

## 4. REFERENCES

[1] X. Lin, X. Sun, P. Ho, X. Shen. GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications. IEEE T VEH TECHNOL, 56, 6 (2007), 3442-3456.

[2] 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 *INFOCOM*, 2011.