



A Lightweight Conditional Privacy-Preservation Protocol for Vehicular Traffic-Monitoring Systems

Rongxing Lu, *Nanyang Technological University*

Xiaodong Lin, *University of Ontario Institute of Technology*

Zhiguo Shi, *Zhejiang University*

Xuemin (Sherman) Shen, *University of Waterloo*

The Vehicular Ad Hoc Network (Vanet), as a special mobile ad hoc network, has received considerable attention in recent years. In Vanet, each vehicle comes equipped with an on-board unit (OBU) device, which enables a vehicle to not only communicate with other vehicles on the road using vehicle-to-vehicle (V2V) communications, but also to roadside unit (RSU) devices—that is, vehicle-to-RSU (V2R) communications. When RSUs serve as the gateways, vehicles can also access to the remote servers, such as a traffic-monitoring server, on the road. Because of its hybrid architecture, Vanet can provide safety- and entertainment-related applications on the road.¹ Vehicular traffic monitoring (VTM) is an important application of Vanet,² where vehicles moving on the road can use V2V and V2R communications to report the traffic congestion, accidents, and road-surface conditions to the traffic-monitoring server and other vehicles (see Figure 1). With a VTM system, drivers can avoid traffic jams and take less-congested roads, and the government can take effective action to control traffic and quickly detect road-surface problems.

Although VTM is a promising cyber-physical system, it faces many security and privacy preservation challenges, especially for location privacy. If the vehicles' location privacy can't be preserved, drivers won't participate in the VTM system. To encourage drivers' participation, the VTM should employ extensive and trusted privacy-preservation techniques that protect vehicles' identity and location privacy. However, because a malicious

vehicle can't be tracked using a *complete* privacy-preservation technique,³ then most users would expect to have a *conditional* privacy-preservation technique to secure VTM systems, where a trusted authority (TA) has the ability to track a malicious vehicle's real identity. Group signatures can build conditional privacy preservation; however, the computation costs are relatively high.^{3,4} Unlinkable pseudo-ID techniques can also build conditional privacy preservation, but the revocation list will get very long when revoking a malicious vehicle.⁵ Although an efficient certificate-revocation mechanism is proposed,⁶ it doesn't support *forward unlinkability*. Forward unlinkability is actually an important requirement in VTM systems—if a vehicle is compromised and becomes malicious, the compromised vehicle definitely should be revoked; yet the vehicle's past messages and locations (from before the time when it was compromised) should still be protected and unlinkable.

In this article, to address these challenges, we introduce a lightweight conditional privacy-preservation (LCPP) protocol, which uses simple hash-chain techniques to not only support real identity tracking by a TA, but also to achieve efficient local revocation verification on the road. This would include the requirements of location privacy, conditional privacy preservation, and forward unlinkability in secure VTS systems.

LCPP

Here, we propose our efficient LCPP protocol for securing VTM systems, which is comprised of two

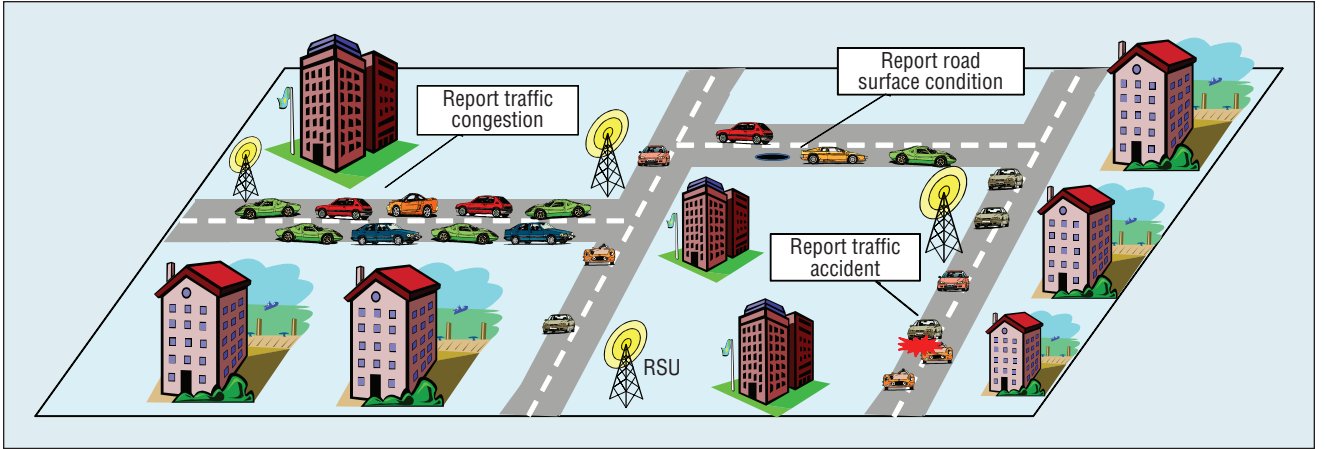


Figure 1. Vehicular traffic monitoring (VTM)—an important Vehicular Ad Hoc Network (Vanet) application. This system lets vehicles report traffic congestion, accidents, and road-surface conditions to the traffic-monitoring server and other vehicles. If used effectively, this could help drivers avoid traffic jams and reroute traffic to less-congested roads.

parts: system settings and conditional tracking.

System Settings

We consider a secure VTM system, which includes a set of vehicles $V = \{V_1, V_2, \dots\}$ moving on the road, a set of RSUs deployed roadside, and a TA. The TA is a highly trusted entity, whose duties include initializing the whole system, assigning key materials to vehicles, and helping track and revoke malicious vehicles. RSUs are connected with the TA through some reliable wired/wireless communications, and the functions of RSUs include relaying the messages exchanged between vehicles and the TA and disseminating the revocation list (RList) to passing vehicles. Each vehicle $V_j \in V$ is moving on the road, periodically reporting the road conditions, traffic congestions, and accidents through V2V and V2R communications. To establish a secure VTM system, the TA first sets up the system parameters as follows: given a security parameter κ , the TA generates the bilinear parameters (q, P, G, G_T, e) , where q is a κ -bit prime number, G, G_T are two groups with order q , $P \in G$ is a generator, and $e: G \times G \rightarrow G_T$ is a nondegenerated and efficiently computable bilinear map.⁷ Then the TA chooses two random numbers $k, s \in \mathbb{Z}_q^*$

as the master key, and computes $P_{\text{pub}} = sP$. In addition, the TA selects a secure symmetric encryption algorithm Enc —for example, the Advanced Encryption Standard (AES)—and three cryptographic hash functions H_0, H_1, H , where $H_i: \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$ with $i \in \{0, 1\}$ and $H: \{0, 1\}^* \rightarrow G$. Finally, the TA keeps the master key secretly, and publishes the public parameters $(G, G_T, q, e, P, P_{\text{pub}}, H_0, H_1, H, Enc)$.

To achieve the conditional privacy-preservation for the vehicles on the road, the TA first divides a long time range into some small, continuous time periods $V_1, V_2, \dots, T_n$, and then assigns a large number of pseudo-IDs to each vehicle $V_j \in V$ (see Figure 2). Concretely, for each vehicle $V_j \in V$, the TA first chooses a random number $R_j \in \mathbb{Z}_q^*$ and stores (V_j, R_j) in a tracking list (TList). Then, the TA generates auxiliary key materials (k_i^j, l_i^j) at each time period for T_i for V_j , where $k_i^j = R_j$, $k_i^j = H_0(k_{i-1}^j)$ with $i = 2, \dots, n$, and $l_i^j = H_1(k_i^j)$ with $i = 1, \dots, n$. At each time period T_i , the TA can generate a number of pseudo-IDs for V_j so that V_j can periodically change its pseudo-ID for location unlinkability. To generate a specific pseudo-ID PID_x^j for V_j at time period T_i , the TA first chooses two random numbers R_{jix1}, R_{jix2} , uses the master key k and l_i^j to compute the pseudo-ID

$PID_x^j = Enc_k(V_j \| R_{jix1}) \| Enc_{l_i^j}(T_i \| R_{jix2}) \| T_i$, and then uses the master key s to compute the corresponding private key $sk_x^j = sH(PID_x^j)$. With the key pair (PID_x^j, sk_x^j) , vehicle V_j can generate an ID-based signature⁸ for anonymous message/entity authentication during the V2V and V2R communications.

Conditional Tracking

Within the secure VTM system, once a message M signed by PID_x^j is in dispute, the real identity V_j of the message source should be tracked and disclosed by the TA, and if V_j has been revoked before, other vehicles on the road can perform the local revocation verification on PID_x^j .

Tracking real identity by the TA. Once the TA receives a disputed message M , together with its signature with respect to the pseudo-ID $PID_x^j = Enc_k(V_j \| R_{jix1}) \| Enc_{l_i^j}(T_i \| R_{jix2}) \| T_i$, the TA first parses and extracts $Enc_k(V_j \| R_{jix1})$, and uses the master key k to recover $V_j \| R_{jix1}$. In such a way, the TA can track and disclose the real identity V_j . To support local revocation verification on the road, the TA first uses the identity V_j to search the TList to retrieve the entry (V_j, R_j) , then computes the key material k_i^j at time period T_i from the retrieved R_j —that

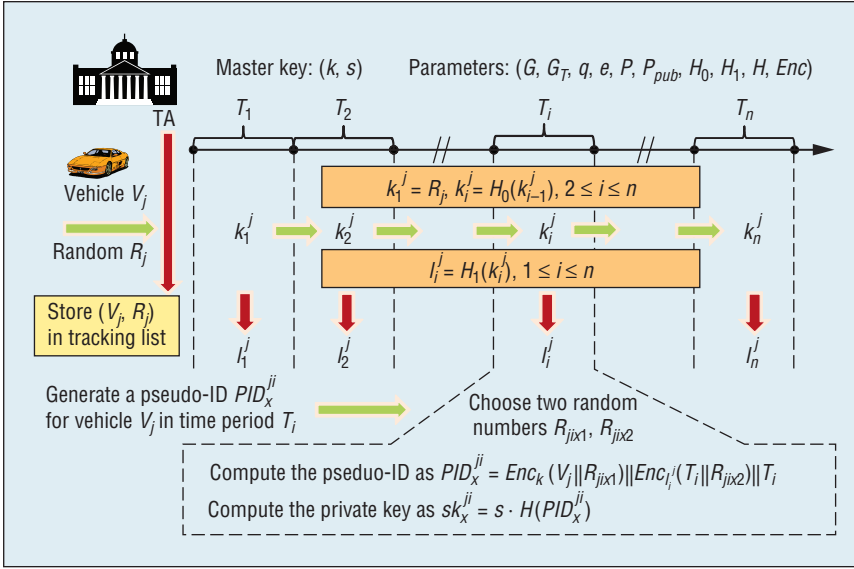


Figure 2. Pseudo-ID generation in the lightweight conditional privacy-preservation (LCPP) protocol. The pseudo-ID generation in the protocol is highly efficient, and only requires several hash operations and one symmetric encryption.

is, $k_i^j = H_0(H_0(\dots H_0(R_j)))$, and finally updates k_i^j in the RList and disseminates the latest RList to vehicles on the road through RSUs.

Local revocation verification (LRV) on the road. If V_j hasn't been revoked before, even though the message M signed by PID_x^{ji} is in dispute, other vehicles on the road can't perform LRV. However, if V_j was revoked in a past time period T_x where $x < i$, other vehicles can perform LRV through the material k_i^j in the RList. For example, once k_i^j in the RList is chosen by a vehicle V_1 , V_1 first computes k_i^j at time period T_i from k_x^j —that is, $k_i^j = H_0(H_0(\dots H_0(k_x^j)))$, computes $l_i^j = H_1(k_i^j)$, and then uses l_i^j to decrypt $Enc_{l_i^j}(T_i || R_{jix2})$. If the recovered T_i is correct, the message M sent by PID_x^{ji} can be locally revoked.

Privacy-Preservation Verification

In the following, we verify the privacy preservation of LCPP in terms of location privacy, conditional privacy preservation, and forward unlinkability.

Location Privacy

To achieve location privacy in the VTM system, each vehicle $V_j \in V$ should hold a large number of unlinkable pseudo-IDs. In LCPP, any pseudo-ID $PID_x^{ji} = Enc_k(V_j || R_{jix1}) || Enc_{l_i^j}(T_i || R_{jix2}) || T_i$ is calculated from two random numbers R_{jix1}, R_{jix2} . Because of the randomness, all pseudo-IDs of V_j are unlinkable. As a result, location privacy can be preserved only if V_j changes its pseudo-IDs at the proper time and occasion.⁹

Conditional Privacy Preservation

To achieve conditional privacy preservation, no other vehicles except a TA should be able to identify the real identity V_j from any pseudo-ID $PID_x^{ji} = Enc_k(V_j || R_{jix1}) || Enc_{l_i^j}(T_i || R_{jix2}) || T_i$. Based on PID_x^{ji} , we can see that only the TA is able to use the master key k to recover V_j from $Enc_k(V_j || R_{jix1})$. Hence, LCPP preserves conditional privacy. In addition, LCPP also supports the LRV on the road. If V_j was revoked with the inclusion of k_x^j in the RList in time period T_x , then even though other vehicles don't know the real identity of V_j , they can use k_x^j to locally detect any future message sent by V_j .

Forward Unlinkability

To achieve forward unlinkability, even though V_j was revoked in time period T_x , any messages sent by V_j in previous time periods ($< T_x$) still shouldn't be linked. In LCPP, k_x^j is calculated by $H_0(k_{x-1}^j)$. Because the hash function H_0 only works in one direction, k_{x-1}^j can't be recovered from k_x^j . As a result, LCPP achieves forward unlinkability.

Efficiency Analyses

To support LRV, the size of RList in LCPP is only proportional to the number of revoked vehicles, not proportional to the huge number of revoked pseudo-IDs corresponding to the revoked vehicles. Therefore, compared with other schemes,⁵ the storage of RList in LCPP is significantly reduced. Additionally, to check whether a received message is sent from a revoked vehicle, LRV in LCPP just requires several hash operations and one symmetric decryption for each element in RList. Thus, LCPP is lightweight and efficient.

In this article, to secure VTM systems, we introduced a lightweight privacy-preservation protocol, called LCPP. In future work, we plan to design more efficient and fine-grained revocation mechanisms for VTM systems by considering bidirectional hash chains.□

References

1. X. Lin et al., "Security in Vehicular Ad Hoc Networks," *IEEE Comm.*, vol. 46, no. 4, 2008, pp. 88–95.
2. A. Skordylis and N. Trigoni, "Efficient Data Propagation in Traffic Monitoring Vehicular Networks," *IEEE Trans. Intelligent Transportation Systems*, vol. 12, no. 3, 2011, pp. 680–694.
3. R. Lu et al., "ECCP: Efficient Conditional Privacy Preservation Protocol for Secure

- Vehicular Communications,” *Proc. 27th Conf. Computer Comm.*, IEEE, 2008, pp. 1229–1237.
4. X. Lin et al., “GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications,” *IEEE Trans. Vehicular Technology*, vol. 56, no. 6, 2007, pp. 3442–3456.
 5. M. Raya and J.-P. Hubaux, “Securing Vehicular Ad Hoc Networks,” *J. Computer Security*, vol. 15, no. 1, 2007, pp. 39–68.
 6. J.J. Haas, Y.-C. Hu, and K.P. Laberteaux, “Design and Analysis of a Lightweight Certificate Revocation Mechanism for Vanet,” *Proc. Vehicular Ad Hoc Networks*, ACM, 2009, pp. 89–98.
 7. D. Boneh and M.K. Franklin, “Identity-Based Encryption from the Weil Pairing,” *Advances in Cryptology*, LNCS 2139, Springer, 2001, pp. 213–229.
 8. P.S.L.M. Barreto et al., “Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps,” *Advances in Cryptology*, LNCS 3788, Springer, 2005, pp. 515–532.
 9. R. Lu et al., “Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in Vanets,” *IEEE Trans. Vehicular Technology*, vol. 61, no. 1, 2012, pp. 86–96.

Rongxing Lu is a faculty member at the School of Electrical and Electronics Engineering at Nanyang Technological University, Singapore. Contact him at rxlu@ntu.edu.sg.

Xiaodong Lin is a faculty member of the Faculty of Business and Information Technology at the University of Ontario Institute of Technology, Canada. Contact him at xiaodong.lin@uoit.ca.

Zhiguo Shi is a faculty member at the Department of Information and Electronic Engineering at Zhejiang University, China. Contact him at shizg@zju.edu.cn.

Xuemin (Sherman) Shen is a faculty member at the Department of Electrical and Computer Engineering at the University of Waterloo, Canada. Contact him at xshen@bcr.uwaterloo.ca.

cn Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.

IEEE computer society NEWSLETTERS

Stay Informed on Hot Topics

COMPUTING NOW
TRAINING SPOTLIGHT
 TRANSACTIONS CONNECTION
 WHAT'S NEW BUILD YOUR
 IN COMPUTER CAREER COMPUTING
 MEMBER CONNECTION
CSCONNECTION NEWS
 DIGITAL LIBRARY NEWS FLASH
 CONFERENCE CONNECTION
WHAT'S
 NEW IN COMPUTER
 BUILD YOUR CAREER
 MEMBER CONNECTION
 TRANSACTIONS CONNECTION
 COMPUTING NOW
 TRAINING SPOTLIGHT
 CS MEMBER CONNECTION



computer.org/newsletters

