International Journal of Security and Its Applications
Vol.8, No.5 (2014), pp.185-194
http://dx.doi.org/10.14257/ijsia.2014.8.5.17

A Network Coding Based Privacy-Preservation Scheme for Online Service Access in VANET

Jizhao Liu and Quan Wang

School of Computer Science and Technology, Xidian University
liujizhao2009@163.com, qwang@xidian.edu.cn

Abstract

Privacy threat is one of crucial issues for the wide deployment of Vehicular Ad-hoc Networks. Due to the open nature of the wireless communications, many kinds of attacks such as eavesdropping and traffic analysis can be launched by various malicious adversaries. Network coding allows intermediate nodes to encode/mix incoming message, thus it can provide a feasible way to thwart effectively eavesdropping and traffic analysis attacks. Inspired by newly developed secure network coding solution, we propose a privacy preservation scheme for online service access in VANET. The proposed scheme can achieve data confidentiality and flow untraceability, and protect the identity and location privacy of vehicles. Moreover, because lightweight coding operation is performed on message content instead of computation-expensive public key encryption, the proposed scheme is much more efficient than traditional privacy preservation scheme, such as Mix-net and Onion Routing based scheme. Finally, security analysis and simulation demonstrate the validity and efficiency of the proposed scheme.

Keywords: *Vehicular Ad-hoc Network, privacy preservation, network coding, anonymity*

1. Introduction

Vehicular ad-hoc networks (VANET) are receiving increasing attentions from academia and industry, due to various applications and potential benefits they offer for improving driving experience and road safety. VANETs generally consist of on-board unit (OBU), road side unit (RSU) and a central trusted authority (TA). Vehicles may communicate with each other (Vehicle-to-Vehicle: V2V), as well as with a nearby RSU (Vehicle-to-Infrastructure: V2I).

In VANET, vehicles access online services using V2I communication through RSU deployed along the road (Figure 1), in which both uplink (Vehicle-to-RSU) and downlink (RSU-to-Vehicle) can be multiple hops. Due to the open nature of the wireless communication, it is particularly easy for an adversary to eavesdrop the V2I communication. Particularly, some advanced attacks, such as traffic and flow analysis attack [1], can be launched to compromise user's security and privacy. For example, an eavesdropper can incept messages, analyze the correlation of the incoming and outgoing messages at each intermediate vehicle, and evenly disclose the forwarding path and trace back the source vehicle in a V2I communication session. Moreover, due to advances in localization technologies enable accurate location estimation based on received radio signal strength [2], the source vehicle's location can be estimated with high resolution. Even if a pseudonym changing mechanism [3] is used to break link between the vehicle and its identifiers in the long run, the eavesdropper can still easily link two consequent pseudonyms because the traffic flow usually exhibits particular pattern in terms of packet size, time interval and

ISSN: 1738-9976 IJSIA

sending ratio. For example, when a vehicle is uploading a bulk of data to a SP through a nearby RSU, an eavesdropper can easily discriminate the vehicle from its neighbors because its sending ratio is higher significantly than its neighbors. Furthermore, when this uploading process spans several RSUs due to vehicular movement, the eavesdropper is able to trace the vehicle's whereabouts for a long distance even a pseudonym updating has been performed.

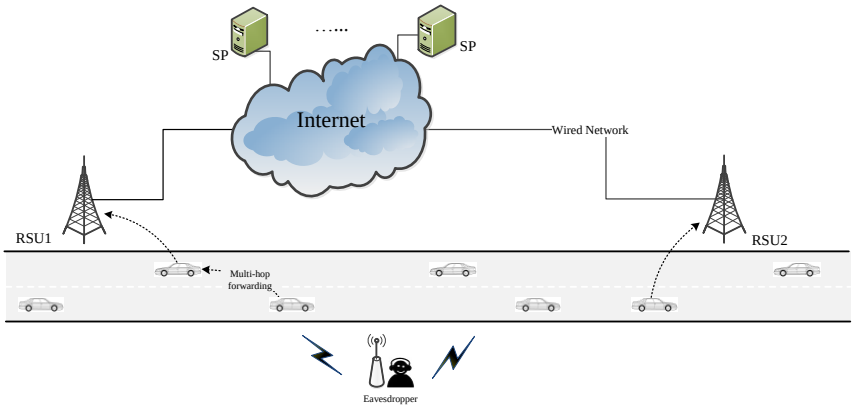


Figure 1. VANET Online Service Access Scenario

Although several privacy-preserving schemes, *i.e.*, Crowds [4], Onion Routing [5] and Mix-net [6], have been proposed to achieve sender/receiver anonymity and session unlink ability for Internet. They may either require pre-established multi-hop forwarding path or result in severe performance degradation. Due to the unique nature of VANETs, *i.e.,* vehicular mobility, huge network scale and limited computation resource, make it infeasible to re-use them directly in VANETs. Network Coding [7-9] offers an elegant solution to achieve data confidentiality and flow untraceability against eavesdropping and traffic analysis attacks. Recent researches prove that network coding not only brings performance benefits, but also provide a feasible way to achieve security and privacy preservation [10-15]. The coding/mixing mechanism provided by network coding can effectively resist traffic analysis attack: each message is trimmed into equal size, intermediate nodes buffer received incoming messages instead of forwarding instantly, and each outgoing message is the result of linear combine on multiple incoming messages. It make more difficult for an adversary to track the upstream/downstream nodes by correlating incoming and outgoing messages in terms of message size, content and transmitting time. In this paper, we propose a network coding based privacy preservation scheme for V2I communication scenario. The proposed scheme combines network coding and group signature techniques, achieves source anonymity, flow untraced ability and session unlink ability.

The rest of this paper is organized as follows: We discuss the related work in Section 2. Section 3 gives system model. In Section 4, the proposed privacy preservation scheme is presented in detail. Security analysis and performance analysis are given in section 5 and 6 respectively. Finally, we draw the concluding remarks in Section 7.

2. Related work

ASRPAKE [16] integrates a ring signature based authenticated key exchange mechanism and achieve anonymity for source nodes, relay nodes and destination nodes. Z. Wan, *et al.*, proposed a privacy protection routing scheme [17] based on group signature and onion

routing for wireless mesh networks. Anonymous mesh router registration and anonymous user-user communication are implemented in the proposed scheme. Up to now, little research has focused on privacy preservation for online service access in VANET. In AMOEBA [18], vehicles are organized into groups and the group leader acts as the proxy to forward packets between group members and RSU. Thus, identity and location privacy can be preserved against the semi-trusted RSU. Based on mix-net, P. Cencioni, *et al.,* proposed VIPER [19] to resist traffic analysis attack in V2I communication scenarios.

Unlike traditional store-and-forward routing, network coding allows intermediate nodes to encode received messages into a single coded message before forwarding them. Random Linear Network Coding (RLNC) [9] makes network coding more practical, in which participating nodes linearly combine receiving messages using randomly chosen coefficients. RLNC has been verified to be both sufficient and efficient for network coding paradigms. Several secure network coding schemes are proposed achieve data confidentiality and source anonymity against eavesdropping and traffic analysis attacks. Y. F. Fan, *et al.,* [10-11] proposed a network coding based privacy preserving scheme against traffic analysis and flow tracing attacks, in which the GEV is protected by homomorphism encryption function. In P-Coding proposed by P. Zhang, *et al.,* [12], the lightweight permutation encryption is performed on message content and coding coefficient vector. P-Coding can efficiently thwart eavesdropping attack and provide scalability and robustness. J. Wang, *et al.,* proposed a privacy preservation scheme [13, 14] to achieve flow untraceability without using encrypted GEVs. They consider a communication network with multiple unicast flows, in which multiple flows are mixed at their intersection nodes, downstream GEVs are generated from the common basis of upstream GEVs of multiple flows to hide the correlation between upstream and downstream GEVs.

3. System Model

3.1. Network Coding

We employ the random linear network coding model with multiple generations introduced in [9]. Source s firstly splits the message stream into generations, each of h messages. A message is viewed as symbols in a finite field, the encoding operation is performed only among the messages in the same generation. We define $x_i (i = 1,2, \dots h)$ as the i^{th} message, s chooses h coding coefficients $\tilde{c}_1, \tilde{c}_2, \dots \tilde{c}_h \in GF(q)$ randomly and independently, and generates a coded message y_i as:

$$y_i = \sum_{i=1}^{h} \tilde{c}_i x_i \quad (1)$$

The coefficient vector $\tilde{c} = (\tilde{c}_1, \tilde{c}_2, \dots \tilde{c}_h)$ is called Local Encoding Vector (LEV). Source s generates k coded messages $y_1, y_2, \dots y_k$ and broadcast them to its neighbors. Intermediate nodes store received coded messages into its buffer. Whenever there is a transmitting opportunity, it starts a recoding process to generate outgoing messages. We define $y_i^{[v]} = (y_{i,1}^{[v]}, y_{i,2}^{[v]}, \dots y_{i,L}^{[v]}) (i = 1,2, \dots M^{[v]})$ as the i^{th} message received at intermediate node v, where $M^{[v]} \geq 2$, intermediate node v chooses its LEV and constructs a coded message $y_{out}^{[v]}$ as

$$y_{out}^{[v]} = \sum_{i=1}^{M^{[v]}} \tilde{c}_i y_i^{[v]} \quad (2)$$

Because received messages $y_i^{[v]}$ themselves can be regarded as the linear combine of the source messages $x_1, x_2, \ldots x_i$. Thus, $y_{out}^{[v]}$ can be represented in terms of *source message* $x_i (i = 1,2, \ldots h)$:

$$y_{out}^{[v]} = \sum_{i=1}^{h} c_i x_i \quad (3)$$

Where c_i can be computed recursively using equation (1), is termed as the Global Encoding Vector (GEV). Coded messages received at receiver node r yield a system of linear equations that should be solved so as to retrieve native messages $x_i (i = 1,2, \ldots h)$. We now define X, Y and C as *source messages*, *coded messages* received at r, and g*lobal encoding matrix* consisting of GEV of each received message, respectively.

$$Y = [y_1, y_2, \ldots y_{M^{[r]}}]^T = [c_1, c_2, \ldots c_{M^{[r]}}]^T X = CX \quad (4)$$

If C is invertible, receiver r can recover source messages x by applying Gauss elimination. In practice, GEV should is carried in each coded message for the receiver to decode. The source node prefixes each source message x_i with a i^{th} unit vector u_i.

$$[u_i, x_i] = [\underbrace{0, \ldots 0}_{i-1}, 1, \underbrace{0, \ldots 0}_{h-i}, x_{i,1}, x_{1,2}, \ldots x_{i,L}] \quad (5)$$

Where, the u_i is termed as a tag. The source and intermediate nodes perform coding operation on both tag and coded message, thus each message automatically contains GEV which can record calculation on it.

4. Network Coding based Communication Protocol

The proposed scheme consists of three phases: 1) Neighbor authentication and key agreement phase. 2) Vehicle registration phase. 3) Message delivery phase.

4.1. Anonymous Neighbor Authentication and Key Agreement Phase

In this phase, vehicles must perform an anonymous mutual authentication process with each of its neighbors to exclude the outside adversaries. The authentication and key agreement procedure between vehicle S and X is demonstrated as follows:

Step 1: $S \rightarrow * : g, g^{r_S}, Sig_g(g^{r_S})$

Step 2: $X \rightarrow S : g^{r_X}, E_{k_{SX}}(k_{X*}), Sig_g(g^{r_S} \mid g^{r_X})$

Step 3: $S \rightarrow X : E_{k_{SX}}(k_{S*} \mid k_{X*})$

Where g is a random generator of multiplicative cyclic group G, $r_S \in Z_p^*$ denotes a random nonce. S generates a group signature Sig_g over g^{r_S} using its group private key. Upon receiving the broadcast message, a neighbor X firstly verifies Sig_g by the group public key. If the verification passed, X generates and sends a reply: X chooses randomly $r_X \in Z_p^*$ and calculates g^{r_X}. X also generates a group signature Sig_g over $g^{r_S} \mid g^{r_X}$ using its own group private key. X generates a session key $k_{SX} = H(g^{r_S r_X})$,

and a local broadcast key k_{X*} . Then X replies to S with $< g^{r_X}, E_{k_{SX}}(k_{X*}), Sig_g(g^{r_S} \mid g^{r_X}) >$. S receives the replies from X and verify the group signature $Sig_g(g^{r_S} \mid g^{r_X})$. If the verification is successful, it computes same session key $k_{SX} = H(g^{r_S r_X})$ and decrypt $E_{k_{SX}}(k_{X*})$ to obtain the broadcast key of k_{X*}. It stores these elements into its neighbor list. S generates the local broadcast key k_{S*} and send $E_{k_{SX}}(k_{S*} \mid k_{X*})$ to X. In the end, X decrypts the message to obtain k_{S*}, and stores it into its neighbor list. The authentication procedure completes.

4.2. Vehicle Registration Phase

RSUs periodically broadcast the message $< g, g^{r_R}, ts, l, Sig_r(g^{r_R}), Cert_R, URL_R >$ to declare the service existence. Where, $r_R \in Z_p^*$ is a random nonce, and l indicates the uniform size of coded message. Sig_r Is a regular signature over g^{r_R}. $Cert_R$ and URL_R are the certification of the RSU and user revocation list published by GM. After receiving RSU's broadcasted message, the source vehicle S checks validity of the RSU by check $Cert_R$. If verification passed, S calculates $k_{SR} = H(g^{r_S r_R})$ as the vehicle-RSU pairwise session key, and generates a registration request $req =< g^{r_S}, Sig_g(g^{r_R} \mid g^{r_S}) >$ to RSU. Finally, S starts an encoding procedure to deliver the registration request to the RSU.

Source Vehicle: the source vehicle S fill request req to $h \cdot L$ bytes with a random padding. The filled request is split into h blocks $x_1, x_2, \ldots x_h$ and tags these blocks with a unit vector u_i. An encoding operation is performed as follows.

$$y = \sum_{i=1}^{h} \alpha_i \cdot [u_i, x_i] = \alpha_i \cdot u_i \mid \alpha_i \cdot x_i \qquad (6)$$

Where $\alpha_i \cdot u_i$ is the GEV. Since anyone can recover the source messages by Gauss elimination after collecting enough number of coded messages，Thus we employee the *m*-partial permutation encryption [12] based secure coding scheme to encrypt the GEV. The *permutation encryption function* can be defined as a permuting operation on the input symbols $x_1, x_2, \ldots x_L$ with a secret key k as follows:

$$E_k(x) = E_k([x_1, x_2, \ldots x_L]) = [x_{k(1)}, x_{k(2)}, \ldots x_{k(L)}] \qquad (7)$$

The *permutation decryption function* on cipher text c with secret key k can be defined as:

$$D_k(c) = D_k([c_1, c_2, \ldots c_L]) = [c_{k^{-1}(1)}, c_{k^{-1}(2)}, \ldots c_{k^{-1}(L)}] \qquad (8)$$

For reducing the computer overhead and the length of the secret key, we only permute part of input symbols. A *s,m* permutation refers to only *m* elements whose position is within $[s, s + m - 1] \subseteq [1, L]$ is permuting in a symbol sequence with length *L*, other elements still in their original position. s is the starting position, and m is the length of the permuted portion. In this paper, the GEV is insert a random chosen

position s in the coded message, and symbols in $[s, s + m - 1]$ are performed the permutation encryption.

For RSU to recover the source messages, some necessary parameters must be carried in each outgoing message. Firstly, the source vehicle encrypts permuting parameters s, m as well as permuting key pk with the RSU's public key and obtains $E_r^p(pk \mid s \mid m)$. Then, a random identifier GID is assigned for each message generation. Finally, the source vehicle encrypts h, GID and $E_r^p(pk \mid s \mid m)$ with its broadcast key and cipher text $E_{S*}^p(E_r^p(pk \mid s \mid m) \mid h \mid GID)$ is attached to coded message to generate an outgoing message. The source vehicle generates k outgoing message and enqueue them into the sending queue. In the end of each time slot, a batch of n messages are dequeued and broadcasted to downstream vehicles (which are closer to the RSU).

Intermediate Vehicles: Intermediate vehicles buffer received incoming message. At the end of each time slots, it triggers a recoding operation using buffered messages to generating h outgoing messages for each received message generation.

$$\sum_{i=1}^{k} \alpha_i \cdot [E_{pk}^{pe}(y_i)] = E_{pk}^{pe}(\sum_{i=1}^{k} \alpha_i \cdot y_i) \quad (9)$$

Where $E_{pk}^{pe}(\circ)$ refers to the permutation encryption operation with permuting key pk. Note that the permutation encryption only reorders the coded message and corresponding GEV in term of symbols, the linear combine can be transparently performed on them as equation (9).

RSU: After more than *h* linearly independent coded messages are received, RSU decodes messages according to equation (4) and obtain vehicle's registration request $req =< g^{r_S}, Sig_g(g^{r_R} \mid g^{r_S}) >$. If the signature $Sig_g(g^{r_R} \mid g^{r_S})$ is valid and the source vehicle not is included in user revocation list URL_R, the RSU stores k_{SR} and the registration is completed successfully.

4.3. Message Delivery Phase

The uplink messages delivery is similar to that in registration request phase. Firstly, the source vehicle performs the encoding and the permutation encryption operation on the source messages. Since a shared session key k_{SR} has been established between the source vehicle and the RSU, the symmetric encryption is performed on pk, s and h instead of asymmetric encryption.

For protecting the anonymity of the source vehicle, downlink messages cannot contain the address of the source vehicle in clear text. We solve this problem by using a special message identifier. We denote GID_{SR} by generation number of an uplink message generation, the RSU uses its hash value $H(GID_{SR})$ as the identifier in downlink messages. After receiving a downlink message, an intermediate vehicle firstly calculates the hash value of all GID_{SR} it stored and tries to find a matched item. If the intermediate vehicle has participated corresponding uplink message forwarding, it will forward the downlink messages. Otherwise it simply drops the message. By this way, the downlink messages will eventually reach the source vehicle. Note that no any

identity and location information are compromised in this process because no intermediate vehicles need to know the identity of the source vehicle.

5. Security/privacy Analysis

In proposed protocol, data confidentiality can be achieved by network coding mechanism. Since each messages received by intermediate vehicles is a result of linear combination on multiple pieces of source messages. Thus, it is computationally difficult for both outside and inside adversaries to recover any meaningful information without the permuting key even enough number of coded messages are collected.

Proposed scheme can resist effectively traffic analysis attack. Since the length of all coded messages is fixed, and each coded message is a result of random linear combination, thus adversaries cannot correlation the size and content of incoming and outgoing messages at intermediate vehicles. At the same time, intermediate vehicles buffer received messages and send outgoing messages only at the end of each time slot. Note that between two transmissions of a vehicle, all its neighbors perform exactly one transmitting operation. Thus, adversaries cannot trace back upstream vehicles by transmission time correlation. Moreover, since coding parameters and permuting parameters are encrypted by vehicular broadcast key and RSU's public key, it is computationally difficult for an adversary to obtain GEV and launch a linear analysis on incoming and outgoing messages to trace back upstream vehicles.

6. Performance Evaluation

6.1. Simulation Setup

In this section, we turn the proposed scheme into simulation to evaluate its performance. Our scheme is implemented on NS-2 simulator. We employ the traffic simulation software SUMO [20] to generating the vehicle traces. The size of geographic area is $2 \times 2km$ which corresponds to a part of Xi'an, Shanxi province, China. We compare performance of the proposed scheme with the Vehicle-to-Infrastructure communication Privacy Enforcement pRotocol (VIPER) [19] which is based on mix-net scheme.

6.2. Computation Overhead Evaluation

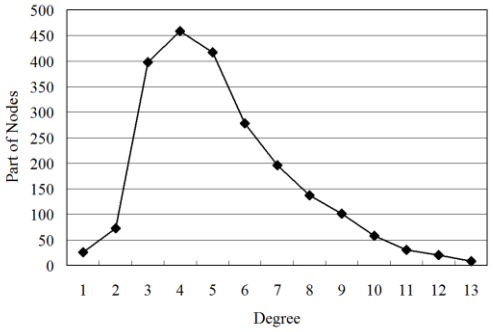
The computation time induced by encoding/decoding operation is given in Table 1. In the proposed scheme, encoding and permutation encryption are performed on message content instead of public key crypto operation in VIPER. A linear combine operation on 64 incoming messages (each of them 1K Bytes) for generating an outgoing message only needs $0.37ms$. The decoding operation takes $2.49ms$ to decode 64 incoming message and recover all of source messages in a single generation. VIPER needs perform an ElGamal encryption operation on message content at the source node. It takes 53.4ms for a 1K Bytes message. At intermediate vehicles, the re-encryption operation consumes 0.09ms, and at the RSU, the decryption operation needs 27.5 *ms*. From above analysis, we can conclude that the proposed scheme can reduce significantly the computational overhead compare to existing VIPER protocol.

Table 1. Computation Time for Coding Operations in the Proposed Scheme (in ms)

OPERATION	*h*=4	*h*=8	*h*=16	*h*=32	*h*=64
Encoding/Recoding	0.02	0.04	0.08	0.18	0.37
Decoding	0.56	0.6	0.68	0.88	2.49

6.3. Routing Performance

The network connectivity is shown in Figure 2. We count the average node degree which represents how many neighbors one node can get. In generated traffic scenario, the average node degree is 5.22.



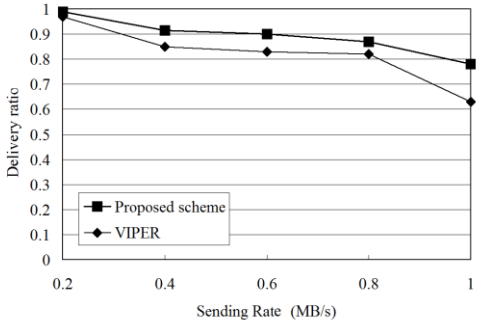
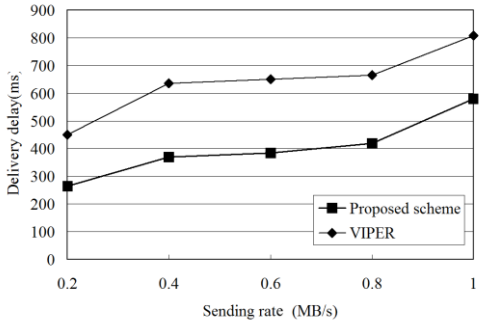


Figure 2. Node Degree Distribution **Figure 3. Delivery Ratio**

We analyze the performance of VIPER and the proposed scheme under various traffic loads by adjusting the message generating rate of the source vehicle from 0.2-1.0MB/s, the message delivery ratio are shown in Figure 3. Both two schemes exhibit good performance under light traffic loads. More than 90% messages can be successfully delivered when sending rate is 0.2 MB/s. The delivery ratio decreases when network traffic loads get heavy. The VIPER and proposed scheme only deliver 63% and 78% messages respectively when sending rate reach 1MB/s. The proposed scheme achieves higher delivery ratio than VIPER. The delivery delay is given in figure 4. Proposed scheme can achieves 260 *ms* average delivery delay when sending rate is 0.2 MB/s, while VIPER is 427 *ms*. When sending rate is 1MB/s, the average delivery delay of the proposed scheme and VIPER is 575 *ms* and 810 *ms* respectively. The proposed scheme can reduce the average delivery latency by 38%.

In Figure 5, the effect of vehicular velocity on the delivery ratio is given. Both VIPER and the proposed scheme can achieve high delivery ratio at low average velocity. The delivery ratio decreases significantly as increased average velocity in VIPER. Only 79% messages can be received successfully by the RSU when average velocity reaches 100km/h. The delivery ratio only decreases slightly: 95.2% messages can be delivered successfully. The main cause is that the VIPER protocol sends messages only at the end of each time slot. Because the movement of vehicles leads to frequent link break, messages vehicle carried will be lost. In the proposed scheme, source/intermediate vehicles broadcast outgoing messages to all its neighbors. Even if

parts of links are broken as vehicular movement, messages still can reach the RSU along others paths.



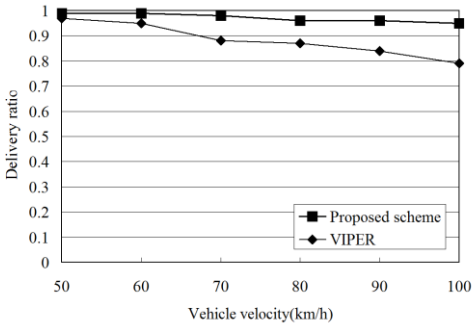


Figure 4. Delivery Delay **Figure 5. Delivery Ratio with Velocity Change**

7. Conclusion

In this paper, we proposed a network coding based privacy preservation scheme to provide anonymity, flow untraceability and session unlinkability for online service access scenario in VANET. Proposed scheme consists of three phases: neighbor authentication phase, vehicular registration phase and message delivery phase. In first phase vehicular identity information are well protected relying on a group signature based mutual authentication process. Since network coding offers inherent coding/recoding mechanism, proposed scheme offers flow untraceability in the second and third phases. Thus the traffic flow analysis attack can be thwarted effectively. The quantitative analysis and simulative evaluation on privacy preservation and system overhead demonstrate the effectiveness and efficiency of the proposed scheme. In our further work, we will extend our research to achieve flow untraceability under a semi-trusted RSU and improve privacy preservation of proposed scheme.

References

[1] M. Shao, Y. Yang, S. Zhu and C. Guohong, "Towards statistically strong source anonymity for sensor networks", Proceedings of the 27th Conference on Computer Communications, **(2008)**, April, 13-18, Phoenix, AZ, USA.
[2] O. Abumansoor and A. Boukerche, "A secure cooperative approach for nonline-of-sight location verification in VANET", IEEE Transactions on Vehicular Technology, vol. 61, no. 1, **(2012)**, pp. 275-285.
[3] R. Lu, X. Li, T. H. Luan, L. Xiaohui and S. Xuemin, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets", IEEE Transactions on Vehicular Technology, vol. 61, no. 1, **(2012)**, pp. 86-96.
[4] M. K. Reiter and A. D. Rubin, "Crowds: Anonymity for web transactions", ACM Transactions on Information and System Security, vol. 1, no. 1, **(1998)**, pp. 66-92.
[5] D. Goldschlag, M. Reed and P. Syverson, "Onion routing", Communications of the ACM, vol. 42, no. 2, **(1999)**, pp. 39-41.
[6] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms", Communications of the ACM, vol. 24, no. 2, **(1981)**, pp. 84-90.
[7] R. Ahlswede, N. Cai, S. Y. R. Li and R. W. Yeung, "Network information flow", IEEE Transactions on Information Theory, vol. 46, no. 4, **(2000)**, pp. 1204-1216.
[8] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard and J. Crowcroft, "XORs in the air: practical wireless network coding", IEEE/ACM Transactions on Networking, vol. 16, no. 3, **(2008)**, pp. 497-510.
[9] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, S. Jun and B. Leong, "A random linear network coding approach to multicast", IEEE Transactions on Information Theory, vol. 52, no. 10, **(2006)**, pp. 4413-4430.

[10] Y. Fan, Y. Jiang, H. Zhu and X. Shen, "An efficient privacy-preserving scheme against traffic analysis attacks in network coding", Proceeding of the 28th Conference on Computer Communications, **(2009)** April 20-25, Rio de Janeiro, Brazil.
[11] Y. Fan, Y. Jiang, H. Zhu, J. Chen and X. Shen, "Network coding based privacy preservation against traffic analysis in multi-hop wireless networks", IEEE Trans. On Wireless Communications, vol. 10, no. 3, **(2011)**, pp. 834-843.
[12] P. Zhang, Y. Jiang, C. Lin, Y. Fan and X. Shen, "P-coding: secure network coding against eavesdropping attacks", Proceeding of the 29th Conference on Computer Communications, **(2010)** March 15-19, San Diego CA, USA.
[13] J. Wang, C. Wu, K. Lu and N. Gu, "Anonymous communication with network coding against traffic analysis attack", Proceeding of the 29th Conference on Computer Communications, **(2011)** April 10-15, Shanghai, China.
[14] J. Wang, K. Lu and C. Qiao, "Untraceability of Mobile Devices in Wireless Mesh Networks using Linear Network Coding", Proceeding of the 32nd IEEE International Conference on Computer Communications, **(2013)** April 14-19, Turin, Italy.
[15] Z. Wan, K. Xing and Y. Liu, "Priv-Code: Preserving privacy against traffic analysis through network coding for multi hop wireless networks", Proceeding of the 31nd IEEE International Conference on Computer Communications, **(2012)** March 25-30, Orlando, Florida, USA.
[16] X. Lin, R. Lu, H. Zhu, P.-H. Ho, X. Shen and Z. Cao, "ASRPAKE: an anonymous secure routing protocol with authenticated key exchange for wireless ad hoc networks", Proceeding of the IEEE International Conference on Communications, **(2007)** June 24-28, Glasgow, England.
[17] Z. Wan, K. Ren and B. Zhu, "Anonymous user communication for privacy protection in wireless metropolitan mesh networks", IEEE Transactions on Vehicular Technology, vol. 59, no. 2, **(2010)**, pp. 519-532.
[18] K. Sampigethaya, M. Li, L. Huang and R. Poovendran, "Amoeba: Robust location privacy scheme for vanet", IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, **(2007)**, pp. 1569-1589.
[19] P. Cencioni and R. D. Pietro, "A mechanism to enforce privacy in vehicle-to-infrastructure communication", Computer communications, vol. 31, no. 12, **(2008)**, pp. 2790-2802.
[20] K. Daniel, E. Jakob, B. Michael and B. Laura, "Recent Development and Applications of SUMO Simulation of Urban Mobility", International Journal on Advances in Systems and Measurements, vol. 5, no. 3, **(2012)**, pp. 128-138.

Authors

Jizhao Liu, he was born in 1981. He received the M.Sc. degree in computer science and technology from Henan University of Technology, Zhengzhou, China. He is currently working toward the Ph. D. degree in computer science and technology with Xidian University. His current research interests include Ad-hoc networks and information security.

Quan Wang, he was born in 1970. He received the B.Sc., M.Sc., and Ph.D. degrees in computer Science and technology from Xidian University, Xi'an and China. His current research interests include input and output technologies and systems, image processing and image understanding.

