Enhanced Threshold Anonymous Announcement in VANETs

Chun-Ta Li[1], Yan-Ming Lai[2], and Cheng-Chi Lee[2,]

[1] *Department of Information Management, Tainan University of Technology*

529 Zhongzheng Road, Tainan City 71002, TAIWAN (R.O.C.) th0040@mail.tut.edu.tw

[2] *Department of Library and Information Science, Fu Jen Catholic University*

510 Jhongjheng Road, New Taipei City 24205, TAIWAN (R.O.C.) Corresponding author: cclee@mail.fju.edu.tw

Abstract :

Vehicular ad hoc network (VANET) allows the vehicles can share traffic information or communicate with each other. However, some shared information maybe come from a malicious user who wants to mislead others. For this reason, in 2011, Chen et al. proposed a threshold anonymous announcement scheme to ensure the reliability of the shared information. Unfortunately, we found that the description of their scheme about the generating process of an important parameter is not enough to be feasible. In order to solve the problem of the Chen et al.'s scheme, in this paper, we propose some simple modifications on the Chen et al.'s scheme.

Keywords : *Vehicular ad hoc networks; Threshold verification; Reliability; Conditional privacy.*

1. Introduction

Due to development of wireless communication technologies, wireless communication between vehicles has been attracted great attention in recent years [3,5,8, 10,13,15]. Vehicular ad hoc network (VANET) is an ad hoc network's extended application [16]. By in-stalling an on-board unit (OBUs), the vehicles can communicate with other vehicular (V2V) or a roadside unit (RSU) (V2R), which is an Internet connecting infrastructure, based on the Dedicated Short Range Communications (DSRC) protocol [1]. Through the VANET, drivers can share traffic information or communicate with others to improve the traffic experience substantially, such as heavy traffic flow information, lo-cation information, or traffic accident [4,17].

However, anyone can share his or her information on VANET. If a sender of the information is a malicious user, he/she can mislead the others by sharing false information. For ensuring the reliability of shared information on the VANET, a solution is a threshold scheme [6]. In general, there is weak trust relation between two strange vehicles. For strengthening the reliability of shared information, such as traffic accident information, a certain number of witnesses and endorses is needed [4,6,11]. The type of threshold scheme includes fixed system-wide and user-controlled. Because a high threshold value maybe let the protocol difficult to reach; a low threshold value will let malicious user can disseminate false information easy, the threshold value must be selected carefully [6,11]. Another issue in threshold scheme is distinguishability of origin [7,14]. If the system cannot find out two or more endorses from the same source, a malicious user can dilate his/her influence by sending the same information repeatedly. On the other hand, an adaptive scheme also should protect user privacy, such as hiding personal information and anonymity.

On the other hand, a scheme achieving anonymity is always difficulty in allowing distinguishing of sources without online user manager. For this reason, designing a scheme can distinguish the source of information become more difficult. User anonymity also brought another problem, anonymous criminal. User anonymity not only protects the information of legal user, but also provides malicious users for a hiding space. To avoid the inside user using the user privacy preserving to broadcast malicious message which maybe mislead other legitimate user, the designed system should have a mechanism for retrieving the real identity of a malicious user and the mechanism is well known as conditional privacy [4,9]. Some proposed schemes setts a receiver to check the information origin [6,11,14]. However, the method perhaps compromises user privacy and discloses user activities. The other schemes use credentials to solve this problem, but updating credentials becomes a new issue [2,11,12,14]. If the credential has long validity, the user may be traced during the validity of credential; if the credential only has short validity, the certification authority will hard to find the malicious user. Using pseudonyms provides the other way to achieve user anonymity. The pseudonyms can comprise some information from vehicles and some private data of system manager, i.e. certification authority (CA) or trust Authority (TA), and the manager can trace the malicious user by analyzing the pseudonyms [2,12]. However, there are delay between the malicious behavior is reported and the man-ager catching the malicious user and stopping his/her usufruct, and the malicious user can continually broadcast the malicious information before caught [4].

For the above reasons, Chen et al. proposed a Threshold Anonymous Announcement (TAA) scheme in 2011 [4]. The design of TAA not only adopts threshold to en-sure the reliability of the shared information, but also adds distinguishable signature and conditioned traceability by other users. In TAA, VANETs' users can collect the shared information form VANET system, and trust the information if the shared in-formation's sources exceeds the threshold; VANETs' user can not only distinguish the information's source, but also catch the malicious user who wants to broadcast the same information repeatedly by himself/herself in this scheme. However, there is an indefinite point in TAA, and the point lets the TAA become infeasible. In this paper, we will describe the indefinite point and propose a simple improved suggestion. The organization of this paper is as follows: we review the TAA scheme briefly in Section 2; in Section 3, we will describe the indefinite point in TAA and propose our simple suggestion. Finally, we conclude the paper in Section 4.

2. Review of TAA Scheme

The TAA [4] is composed of Setup algorithm, Join protocol, Signing algorithm, Verification algorithm, Threshold checking algorithm, Disavowing algorithm, and Revocation, and the scheme is based on bilinear paring [4]. Chen et al. proposed two versions in their paper, and only the version 2 of their scheme can help user to catch the malicious user. For brevity, the detail of bilinear paring we don't describe here and we only review the first three subsections of the version 2 and review how to trace the malicious user in TAA briefly in this section. Anyone who is interested in bilinear paring or the TAA scheme can refer to the original literature.

In TAA scheme, each vehicle is equipped with a tamper-resistant box (TRB), which is considered to be trusted, and secret parameters of the system, functions, and algorithms are preloaded in the TRB. In addition, each TRB will generate an internal unique TAAseed by itself, and the TAAseed is kept secretly. There are three partici-

pators in TAA system: an issuer I, the third authorities; signers $S\hat{}$, the system users who broadcast the information and they must to sign the information before sending; and verifiers V , the system users who receive the information, and they will verifies the signature of the information.

2.1. Setup Algorithm

First, the issuer I generates the bilinear map $\hat{}e : G_1 \times G_2 \rightarrow G_t$, where $\{G_1,G_2,G_t\}$ are cyclic groups, choose a sufficiently large prime order q, and let $P_1 \in G_1$, $P_2 \in G_2$. Bilinear map $\hat{}e$ satisfies $\hat{}e(aP_1,bP_2) = e\hat{}(P_1,P_2)^{ab}$, where $\{a,b\} \in Z_q$, and there is a polynomial time algorithm for computing $\hat{}e(P,Q)$, where $\{P,Q\} \in$ cyclic groups. Then, I chooses two random numbers $\{x,y\} \in Z_q$ as his/her privacy key i_{sk} and computes his/her public key $i_{pk} = \{X = xP_2,Y = yP_2\}$. After that, I selects six hash functions: $H_1,H_2,H_4,H_6 : \{0,1\}^* \rightarrow Z_q$;$H_3,H_5 : \{0,1\}^* \rightarrow G_1$. Finally, I publishes $\{G_1,G_2,G_T,q,H_{1\,6},i_{pk},KI\}$, where KI is a public information.

2.2. Join Protocol

Users $U\hat{}$ must to join this system by registering at the issuer I before sharing and accessing the information. When the join protocol is started, the user side asks to I a value $n_I \in \{0,1\}^*$, which is randomly selected by I. Upon to receiving n_I, $U\hat{}$ generates a secret value f from the unique value TAAseed which is stored in the TRB. Then $U\hat{}$ computers $str = (X||Y\,||n_I),f = H_1(\text{TAAseed}||cnt||KI)$, where cnt is a count number. After that, $U\hat{}$ chooses a random number $u \in Z_q$, and computes $\{U = uP_1,F = fP_1,v = H_2(str||F||U),w = u + vf(\text{mod}q),\gamma = sig_{SK}(F||v||w)\}$, where sig_{SK} is a private key of a user $U\hat{}$. Finally, $U\hat{}$ submits $\{n_I,F,v,w,\gamma\}$ to I.

After receiving $\{n_I,F,v,w,\gamma\}$, I verifies the integrity of the received information by checking n_I and γ. Then, I verifies the validity of $U\hat{}$ as follows: I computes $U^0 = wP_1 - vF$ and checks $F = f_iP_1$ for any f_i on the rogue list, which is a malicious user list maintained by I. If there is no matched F on the rogue list, I computes $str = (X||Y\,||n_I)$ and verifies that $v \stackrel{?}{=} H_2(str||F||U^0)$. If the equation is correctly, I assures the validity of U and chooses a random number $r \in Z_q$, and computes $\{A = rP_1,B = yA,C = (xA + rxyF),cre = (A,B,C)\}$. Finally, I returns the cre to $U\hat{}$.

When $U\hat{}$ receives the cre, $U\hat{}$ verifies the validity of I by checking $\hat{}e(A,Y) \stackrel{?}{=} e\hat{}(B,P_2)$ and $\hat{}e(A+fB,X) \stackrel{?}{=} e\hat{}(C,P_2)$. If both of the two equations are correctly, $U\hat{}$ assures the validity of I, and stores cre in TRB secretly. The join protocol is shown as Figure 1.

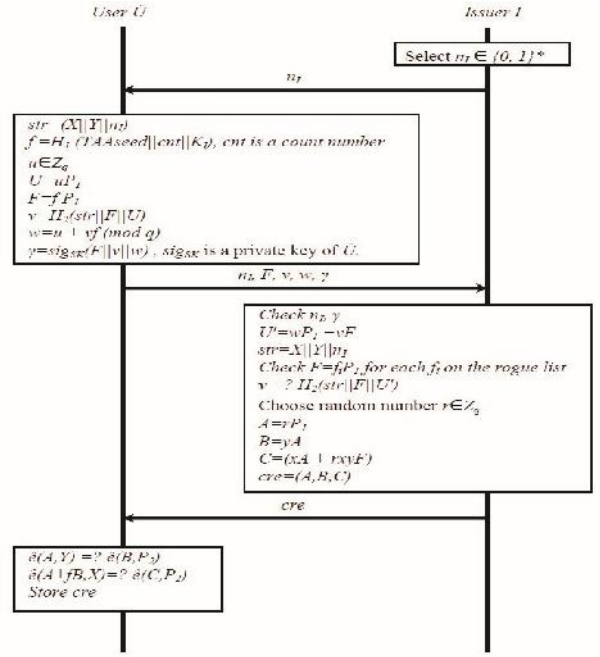

Fig.1. *Join protocol of TAA*

2.3. Sign Algorithm

When a user Uˆ wants to share some information, he/she must to sign the information before sending, and he/she is also a singer Sˆ when sharing information. Sˆ has to choose a variable $n_T \in \{0,1\}$, such as timestamp or random number, and generate the $msg = (msgt, msgb)$, $msgt \in \{0,1\}^*$,that means the predefined title of information; $msgb \in \{0,1\}^*$, that denotes the main body of information, and it is arbitrary. After that, Sˆ chooses two numbers $\{a,z\} \in Z_q$, and computes $\{J,K,L,R,S,T,M,N,O,c,s,\sigma\}$ as following.

$$J = H_3(msgt) \in G_1, K = fJ, L = zJ$$

$$R = aA, S = aB, T = aC, \tau = e\hat{}(S,X)^z$$

$$M = H_5(msgt) + H_6(n_T||msgb||L||R||S||T)P_1, N = fM, O = zM\ c = H_4(\tau||J||K||M||N||O||n_T||msgb), s = z + cf (\mathrm{mod} q)$$

$$\sigma = (R,S,T,J,K,M,N,c,s,n_T).$$

Finally, Sˆ broadcasts $\{\sigma, msg\}$ to other users.

2.4. Verification Algorithm

If a user Uˆ accesses the shared information in VANET, he/she has to verify the integrity and validity of the information to ensure the reliability of the accessed information, and he/she is also a verifier V when accessing information.

Upon receives $\{\sigma, msg\}$, V checks $K = f_i J$, for each f_i in the kept in rogue list. If there is no matched f_i in the rogue list, the information comes from a non-malicious user; if there is a matched f_i, V rejects the information. After that, V

verifies that $J \stackrel{?}{=} H_3(msgt)$ and $\hat{e}(R,Y) \stackrel{?}{=} e\hat{}(S,P_2)$. If both of two equations are correctly, V computes $\rho_a^\dagger = \hat{e}(R,X)$, $\rho_b^\dagger = \hat{e}(S,X)$, $\rho_c^\dagger = \hat{e}(T,P_2)$, $\tau^\dagger = (\rho_b^\dagger)^s \cdot (\rho_c^\dagger/\rho_a^\dagger)^{-c}$ and $L^\dagger = sJ - cK$ and verifies $M \stackrel{?}{=} H_5(msgt) + H_6(n_T||msgb||L^\dagger||R||S||T)P_1$. If the equation is also correctly, V computes $O^\dagger = sM - cN$ and $c \stackrel{?}{=} H_4(\tau^\dagger||J||K||M||N||O^\dagger||n_T||msgb)$. Finally, V assures the integrity of the information the validity of the information's source if c equals to $H_4(\tau^\dagger||J||K||M||N||O^\dagger||n_T||msgb)$.

2.5. Tracing Algorithm

When V receives two or more $\{\sigma,msg\}$, V must catch the malicious user who sends the same information repeatedly. We assume that V receives two $\{\sigma,msg\}$, that is denoted (σ_b,msg_b),$msg_b = (msgt_b,msgb_b)$, and $b = 0$ or 1, and $\sigma_b = (R_b,S_b,T_b,J_b,K_b,M_b,N_b,c_b,s_b,(n_T)b)$. V must to check the link between $\{\sigma_0,msg_0\}$ and $\{\sigma_1,msg_1\}$. The protocol is shown in Figure 2.

If there is link between $\{\sigma_0,msg_0\}$ and $\{\sigma_1,msg_1\}$, the two different $\{\sigma,msg\}$ perhaps come from the same user who is malicious. For further confirming, V computes $\{L^\dagger_b = s_bJ_b - c_bK_b, h_b = H_6((n_T)_b||msgb_b||L^\dagger_b||R_b||S_b||T_b)\}$, and checks that $h_0 \stackrel{?}{=} h_1$, $L^\dagger_0 \stackrel{?}{=} L^\dagger_1$ and $s_0 \stackrel{?}{=} s_1$. If h_0 is not equate to h_1 and s_0 is not equate to s_1 either, V assures that the two $\{\sigma,msg\}$ are broadcasted at different time. In this case, if $L_0^\dagger$ and $L_1^\dagger$ are the same, V assures that the two $\{\sigma,msg\}$ share the same information. For above reason, V can infer that the source of $\{\sigma_0,msg_0\}$

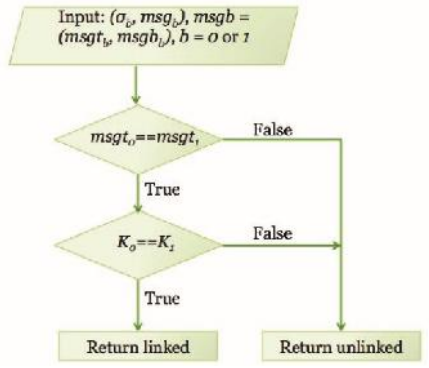

Fig.2. *The link protocol of TAA*

and $\{\sigma_1,msg_1\}$ shares the same information at different time, and the source perhaps wants to affect the reliability of TAA. And then, V can obtain the unique value f and F of the caught source by computing as follows:

$f = (s_0 - s_1)/(c_0 - c_1)$

$F = (N_0 - N_1)/(h_0 - h_1)$.

Finally, V reports $\{f,F\}$ to issuer I, and I updates the rogue list when receives the enough reports from different sources.

3. Analysis of TAA

3.1. The Infeasible Point in TAA

In TAA scheme, the authors set the value $s = z + cf(\mathrm{mod}q)$ (refer to Section 2.3) and use the equation $f = (s_0 - s_1)/(c_0 - c_1)$ (refer to Section 2.5) to catch the malicious user's unique value f. However, the value $z \in Z_q$ of the original literature is a random number in common sense and it lets the TAA scheme be infeasible. If z is a random number, and $\{s_0,s_1\}$ come from $\{\sigma_0,msg_0\}$ and $\{\sigma_1,msg_1\}$, respectively. Let $s_0 = z_0 + c_0f(\mathrm{mod}q)$,$s_1 = z_1 + c_1f(\mathrm{mod}q)$, and $z_0 6= z_1$.

$$\textit{Compute } (s_0 - s_1)/(c_0 - c_1) = z_0 + c_0f(\mathrm{mod}q) - [z_1 + c_1f(\mathrm{mod}q)]/(c_0 - c_1)$$

$$= [z_0 - z_1 + f(c_0 - c_1)(\mathrm{mod}q)]/(c_0 - c_1)$$

$$= (z_0 - z_1)/(c_0 - c_1) + f$$

$$6= f,\textit{because } z_0 - z_1 6= 0.$$

In the original literature, the verifier V has to check $K = f_iJ$, for each f_i in the kept in rogue list and determine to accept it or not. However, the way provided by the original literature cannot help the verifier V to recover the malicious user's unique value f. Although the original literature said the verifier

V can obtain F by computing $F = (N_0 - N_1)/(h_0 - h_1)$ and report F to the issuer I, the original literature did not describe how the value F can help I to obtain the secure value f and put it in the rogue list. We infer that TAA scheme is infeasible if z is a random number.

3.2. Our Simple Improvements

To improve the TAA scheme, we propose a suggestion focus on sign algorithm. In our improved TAA scheme, $S\hat{}$ also has to choose a variable $n_T \in \{0,1\}$, and generate the $msg = (msgt,msgb)$,$msgt \in \{0,1\}^*$.

After that, $S\hat{}$ chooses a numbers $a \in Z_q$, and generates $z = H_1(msgt||(t \cdot f))$, where t is a timestamp, t=(the total minutes)/d, d is a pre-configured value, such as 5 or 10, and it can avoid the user broadcasts the same information repeatedly at a short time. After that, $S\hat{}$ continues the original protocol of TAA. $S\hat{}$ computes $\{J,K,L,R,S,T,M,N,O,c,s,\sigma\}$ as following.

$$J = H_3(msgt) \in G_1,K = fJ,L = zJ$$

$$R = aA,S = aB,T = aC,\tau = e\hat{}(S,X)^z$$

$$M = H_5(msgt) + H_6(n_T||msgb||L||R||S||T)P_1,N = fM,O = zM\ c = H_4(\tau||J||K||M||N||O||n_T||msgb),s = z + cf(\mathrm{mod}q)$$

$$\sigma = (R,S,T,J,K,M,N,c,s,n_T).$$

Finally, $S\hat{}$ broadcasts $\{\sigma,msg\}$ to other users. In our improved TAA scheme, we adopt $z = H_1(msgt||(t \cdot f))$. Because of that, z will be the same value if the user wants to broadcasts the same information repeatedly at a short time; and z will be changed if the shared information or sharing time is different with others. And then, the malicious user's unique value catching equation $f = (s_0 \cdot s_1)/(c_0 \cdot c_1)$ can be feasible. The proof is shown as follows:

Proof: Assume $\{s_0,s_1\}$ come from $\{\sigma_0,msg_0\}$ and $\{\sigma_1,msg_1\}$, respectively.

(1) If both of $\{\sigma_0, msg_0\}$ and $\{\sigma_1, msg_1\}$ came from the same source, shared the same information at a short time:

Let $s_1 = z_0 + c_0 f (\mathrm{mod} q)$, $s_1 = z_1 + c_1 f (\mathrm{mod} q)$, and $z_0 = H_1(msgt_0 || (t_0 \cdot f))$, $z_1 = H_1(msgt_1 || (t_1 \cdot f))$.

Compute $(s_0 - s_1)/(c_0 - c_1) = z_0 + c_0 f (\mathrm{mod} q) - [z_1 + c_1 f (\mathrm{mod} q)]/(c_0 - c_1) = [z_0 - z_1 + f(c_0 - c_1)(\mathrm{mod} q)]/(c_0 - c_1)$.

$\because msgt_0 = msgt_0$ and $t_0 = t_1 \therefore z_0 = z_1$, and $z_0 - z_1 = 0, [z_0 - z_1 + f(c_0 - c_1)(\mathrm{mod} q)]/(c_0 = c_1) = f$.

(2) If both of $\{\sigma_0, msg_0\}$ and $\{\sigma_1, msg_1\}$ came from the same source, but shared information or sharing time are different:

Let $s_1 = z_0 + c_0 f (\mathrm{mod} q)$, $s_1 = z_1 + c_1 f (\mathrm{mod} q)$, and $z_0 = H_1(msgt_0 || (t_0 \cdot f))$, $z_1 = H_1(msgt_1 || (t_1 Pf))$.

Compute $(s_0 - s_1)/(c_0 - c_1) = z_0 + c_0 f (\mathrm{mod} q) - [z_1 + c_1 f (\mathrm{mod} q)]/(c_0 - c_1) = [z_0 - z_1 + f(c_0 - c_1)(\mathrm{mod} q)]/(c_0 - c_1)$.

$\because msgt_0 = 6\ msgt_0$ or $t_0 = 6\ t_1 \therefore z_0\ 6 = z_1$, and $z_0 - z_1 = 0, [z_0 - z_1 + f(c_0 - c_1)(\mathrm{mod} q)]/(c_0 = c_1)\ 6 = f$.

The unique value *f* can be caught when shares the same information at a short time, and be protected in other case. And then, the improved scheme achieve to the real conditional privacy.

4. Conclusions

The TAA scheme not only provides reliability and privacy protected, but also allows user catch the malicious user's unique value *f*. However, the TAA scheme is not comprehensive. There is a lack that can let the TAA scheme become unfeasible. In this paper, we pointed out the lack of the TAA scheme, and proposed a simple suggestion to improve it. The TAA scheme can be batter and more feasible after adopting our simple suggestion.

References

1. ASTM E2213-03, "Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems 8212; 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *ASTM org.*, http://www.astm.org/Standards/E2213.htm, 2011.
2. G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and Robust Pseudonymous Authentication in VANET," In *Proceedings of the fourth ACM International Workshop on Vehicular Ad Hoc Networks (VANET 2007)*, pp. 19-28, 2007.
3. C. C. Chang and C. Y. Lee, "A smart card-based authentication scheme uing user identify cryptography," *International Journal of Network Security*, 15(2):139-147, 2013.
4. L. Chen, S. L. Ng, and G. Wang, "Threshold Anonymous Announcement in VANETs," *IEEE Journal on Selected Areas in Communications*, 29(3):605-615, 2011.

5. A. K. Das, "Improving identity-based random key establishment scheme for largescale hierarchical wireless sensor networks," *International Journal of Network Security*, 14(1):1-21, 2012.

6. V. Daza, J. Domingo-Ferrer, F. Seb´*e* and A. Viejo, "Trustworthy Privacypreserving Car-generated Announcements in Vehicular Ad Hoc Networks," *IEEE Transactions on Vehicular Technology*, 58(4):1876-1886, 2009.

7. J. R. Douceur, "The Sybil Attack," *Peer to Peer Systems*, 2429(2002):251-260, 2002.

8. D. He, W. Zhao, and S. Wu, "Security analysis of a dynamic ID-based authentication scheme for multi-server environment using smart cards," *International Journal of Network Security*, 15(5):350-356, 2013.

9. D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, 12(6):736-746, 2011.

10. J. Kar, "ID-based deniable authentication protocol based on Diffie-Hellman problem on elliptic curve," *International Journal of Network Security*, 15(5):357-364, 2013.

11. G. Kounga, T. Walter, and S. Lachmund, "Proving Reliability of Anonymous Information in VANETs," *IEEE Transactions on Vehicular Technology*, 58(6):29772989, 2009.

12. X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: Secure Vehicular Communications with Privacy Preserving," *IEEE Transactions on Vehicular Technology*, 56(6):34423456, 2007.

13. M. Naveed, W. Habib, U. Masud, U. Ullah, and G. Ahmad, "Reliable and low cost RFID based authentication system for large scale deployment," *International Journal of Network Security*, 14(3):173-179, 2012.

14. P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J. P. Hubaux, "Secure Vehicular Communication Systems: Design and Architecture," *IEEE Communications Magazine*, 46(11):100109, 2008.

15. R. Ramasamy and A. P. Muniyandi, "An efficient password authentication scheme for smart card," *International Journal of Network Security*, 14(3):180-186, 2012.

16. Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle Ad Hoc Networks: Applications and Related Technical Issues," *IEEE Communications Surveys & Tutorials*, 10(3):74-87, 2008.

17. C. Zhang, P. H. Ho, and J. Tapolcai, "On Batch Verification with Group Testing for Vehicular Communications," *Wireless Networks*, 17(8):1851-1865, 2011.