An Efficient and Practical Authenticated Communication Scheme for Vehicular Ad Hoc Networks

Chin-Chen Chang[1], Jen-Ho Yang[2], and Yu-Ching Wu[3]

(Corresponding author: Jen-Ho Yang)

Department of Information Engineering and Computer Science, Feng Chia University[1]

100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan, R.O.C.

Department of Information and Electronic Commerce, Kainan University[2]

No. 1, Kannan Rd., Luzhu, Taoyuan County, 33857, Taiwan, R.O.C.

(Email: jenhoyang@mail.knu.edu.tw)

Department of Computer Science and Information Engineering, National Chung Cheng University[3]

160 San-Hsing, Ming-Hsiung, Chiayi 621, Taiwan, R.O.C.

(Received Mar. 4, 2013; revised and accepted May 16 & Aug. 13, 2013)

Abstract

In the vehicular ad hoc networks (VANET), various authentication schemes have been proposed for secure communications. However, the previous schemes are inefficient because each vehicle needs to share and keep a large number of session keys for communicating with the other vehicles on the VANET. To overcome the above drawback, we propose a new authenticated communication scheme for the VANET. In the proposed scheme, each vehicle communicates with the other vehicles through the roadside unit (RSU). Based upon this environment, each vehicle only has to share a session key with the RSU to communicate with different vehicles. Thus, the proposed communication model can be simplified on the VANET.

Keywords: Authentication, elliptic curve cryptography, mobile ad hoc networks, vehicular ad hoc networks, wireless communication

1 Introduction

Mobile ad hoc networks (MANET) [1, 3, 14, 17, 19, 21] is a network architecture which combines ad hoc and wireless networks. The MANET does not require a fixed network infrastructure to keep the network connection and it is self-organized. In the MANET applications, a vehicular ad hoc network (VANET) is the most popular one because it provides a secure environment for vehicular communications. However, some characteristics of the VANET are different from those of the MANET. For example, the vehicle speed on the VANET is faster than the mobile node in the MANET, and the network topology of the VANET is deployed according to the direction of roadway. The main goal of the VANET is to provide the driving safety and comfortable to users. The applications of the VANET can be divided into two parts: the Intelligent Transportation system (ITS) application and the comfortable application [5, 11, 13, 16].

Generally, the ITS is used to provide the transmission safety of vehicle communications and increase the driving efficiency. The ITS applications include the control of traffic flows, preventing the car collisions, analyzing the traffic jams, evaluating the traffic situations, and deciding the driving routes and so on. For example, a vehicle can broadcast the accident message to caution the other incoming vehicles while a vehicle accident happens. Then, the incoming vehicles can select other driving routes to prevent this traffic jam so the possibility of the traffic accident can be reduced.

Besides, the comfortable application on the VANET is to provide the network connections for vehicles so the passengers in vehicles can derive some electronic services. For example, the passenger can easily download the electronic music, games, and E-mails in a vehicle.

From the business or commercial point of view, the VANET has the commercial potential for many applications so it becomes a popular research in recent years. For the communication security, many secure communication schemes for the VANET have been proposed [5, 12, 13, 16]. For traffic control on the VANET, Li et al. [11] proposed a secure model with three communication schemes based on ID-based cryptography [10, 15, 20] and the blind digital signature schemes [2, 4, 18]. In addition, they also proposed an entertainment service scheme with privacy preservation for the VANET.

However, we found that Li et al.'s communication model for traffic control is too complicated and inefficient. This is because that each vehicle needs to share and keep a large number of session keys for communicating with the other vehicles in their scheme. Moreover, Li et al.'s communication model is impractical because a vehicle needs to perform different communication schemes to communicate with different roles on the VANET. Besides, their entertainment service scheme is also inefficient and impractical because it has unnecessary communications between the vehicle and the service provider.

To overcome the above-mentioned drawbacks, we propose an efficient authenticated communication scheme for the VANET. In the proposed scheme, a vehicle communicates with the other vehicles through the roadside unit (RSU), which is set on the roadside to broadcast and receive messages for vehicles. Based upon this environment, a vehicle only needs to share a session key with the RSU to communicate with a large number of vehicles. Besides, the proposed scheme integrates Li et al.'s three communication schemes so the infrastructure of the proposed scheme is more practical and simpler for the VANET.

Besides, we also propose an entertainment service scheme for the VANET without involving the service provider. In the proposed service scheme, the function of the service provider is integrated into the RSU. Therefore, the communication and computation costs can be drastically reduced when the passenger requires the entertainment services in a vehicle. According to the above-mentioned advantages, the proposed scheme is more efficient and practical than the previously proposed schemes for the VANET.

2 The Related Work

In this section, we briefly describe Li et al.'s scheme [11] and its drawbacks.

2.1 Li et al.'s Scheme

There are three roles in Li et al.'s scheme: the vehicle, the roadside unit (RSU), and the service provider. In this system, each vehicle is equipped with a mobile device to communicate with the other vehicles and the RSU. The RSU is responsible for broadcasting traffic information or entertainment applications to the vehicles. And, the service provider is responsible for providing some entertainment services to passengers in a vehicle. In [11], Li et al. proposed three communication models for the VANET: the vehicle-to-vehicle communication, the vehicle-to-RSU communication, and the RSU-to-vehicle communication models. Besides, Li et al. also proposed a secure and efficient communication scheme with privacy preservation (SECSPP) for entertainment applications on the VANET. The notations used in Li et al.'s schemes are shown in Table 1. Now, we describe Li et al.'s schemes as follows.

2.1.1 The Vehicle-to-Vehicle Communication Scheme

Assume that a vehicle V_i wants to communication with another vehicle V_j, the detailed steps are shown as follows.

1) V_i selects a random number a and $tag\#$. Next, V_i computes $M = C \oplus (tag\#||ID_{V_i}||ID_{V_j}||T_{V_i}||a)$ and $C = (ID^2_{V_i})^{H(T_{V_i}||r)K_{V_i}}$, where T_{V_i} is a timestamp, r is the roadway section, and K_{V_i} is the secret key of V_i.

2) V_i broadcasts $H'(SK) \oplus (tag\#,\ ID_{V_i},\ ID_{V_j},\ hop,\ r,\ T_{V_j},\ M)$ to the vehicles within V_i's transmission range, where $H'(SK)$ is the shared secret key in the network.

3) After receiving $H'(SK) \oplus (tag\#, ID_{V_i}, ID_{V_j}, hop, r, T_{V_j}, M)$, V_j decrypts the message by $H'(SK)$. Then, V_j computes $C' = (ID^2_{V_i})^{H(T_{V_i}||r)K_{V_i}}$ to reveal S. And, V_j checks the validity of hop and ID_{V_j}. If they are valid, then V_j selects a random number b to compute a session key $K_{V_j,V_i} = H(a||b||0)$.

4) V_j sends $H'(SK) \oplus (tag\#, ID_{V_i}, ID_{V_j}, T_{V_j}, r, S')$ to V_i, where $M' = C' \oplus (tag\#||ID_{V_i}\ ||ID_S\ ||T_{V_i}||r||b||MAC)$ and $MAC = H(K_{V_j,V_i}; a+1)$.

5) After receiving $H'(SK) \oplus (tag\#,\ ID_{V_i},\ ID_{V_j},\ T_{V_j},\ r, S')$, A reveals $(tag\#, ID_{V_i}, ID_{V_j}, T_{V_j}, r||b||MAC)$. Then, V_i can compute the session key $K_{V_i,V_j} = H(a||b||0)$ and verifies the correctness of MAC. If the above verifications hold, then V_i and V_j can share a common session key and use it to communicate with each other.

2.1.2 The Vehicle-to-RSU Communication Scheme

Assume that an ambulance V_A transmits an emergency signal to the RSU, then V_A can control traffic lights on its way to a hospital. The detailed steps are shown as follows.

1) V_A generates a random number a to compute $M = C \oplus (ES||ID_{V_A}\ ||ID_R\ ||T_{V_i}||a)$ and $C = (ID^2_R)^{H(T_{V_A}||r)K_{V_A}}$, where ID_R is the identity of RSU, ES is the emergency signal, and K_A is the secret key. Then, V_A sends $H'(SK) \oplus (ES,\ ID_{V_A},\ ID_R,\ r,\ T_{V_A},\ M)$ to R.

2) Upon receiving the above messages, R reveals the message by $H'(SK)$ and checks the validity of V_A. If the above verification is correct, then RSU computes $C' = (ID^2_{V_A})^{H(T_{V_A}||r)K_R}$ to reveal S. Afterward, RSU selects a random number b to compute the session key $K_{R,V_A}(a||b||0)$.

3) RSU sends $H'(SK) \oplus (ES,\ ID_R,\ ID_{V_A},\ r,\ T_R,\ S')$ to A, where $M' = C' \oplus (ES||ID_R||ID_{V_A}\ ||T_R||r||b||MAC)$ and $MAC = H(K_{R,V_A}||a+1)$.

Table 1: The notations of Li et al.'s scheme

ID_X	The identity of the entity X
$PK'_S SK_S$	The public/private key of the service provider
K_X	The secret key of the entity X
$tag\#$	An unique tag number for a request
hop	The number of hops
r	The identity of roadway section
ES	An emergency signal
MAC	The message authentication code
$H(\cdot)$	A collision-free and public one-way hash function
M_X	The receipt of the service access for the vehicle X
T_X	A timestamp generated by the entity X
$H(SK)$	The group secret key shared among all nodes in the VANET
$\|\|$	The concatenation operation
$E_{PK_S}\{\cdot\}$	The asymmetric encryption function using the public key
$D_{SK_S}\{\cdot\}$	The asymmetric decryption function using the private key

4) After receiving the above messages, V_A uses $H'(SK)$ and C to reveal $(ES||ID_R||ID_{V_A}||T_B||r||b||MAC)$. Next, V_A computes $K_{V_A,R} = (a||b||0)$ to verify the correctness of MAC. If the above verifications are correct, then V_A and RSU can use the session key to communicate with each other.

2.1.3 The RSU-to-Vehicle Communication Scheme

Assume that RSU wants to update the shared group key $H'(SK)$ to all vehicles within its transmission range, and then the detailed steps are shown as follows.

1) RSU generates a new shared key c and $nonce_R$. Next, the RSU broadcasts the following message $H'(SK) \oplus (Update\_Key,\ H^{t-1}(SK),\ ID_R,\ r,\ T_R,\ nonce_R)$ to all vehicles in its transmission range.

2) After V_i receiving the following message: $H'(SK) \oplus (Update\_Key, H^{t-1}(SK), ID_R, r, T_R, nonce_R)$, then V_i can decrypt it by using $H'(SK)$. Next, V_i verifies the shared key $H^{t-1}(SK)$ by checking if the equation $H'(SK) = H(H^{t-1}(SK))$ holds or not. If the equation holds, then V_i updates the shared key with $H^{t-1}(SK)$ and broadcasts the following message $H^{t-1}(SK) \oplus (ID_{V_i}, T_{V_i}, r, nonce_R + 1)$ to RSU.

3) After receiving $H^{t-1}(SK) \oplus (ID_{V_i}, T_{V_i}, r, nonce_R + 1)$, RSU can obtain $(ID_{V_i}, T_{V_i}, r, nonce_R + 1)$ by $H^{t-1}(SK) \oplus (ID_{V_i}, T_{V_i}, r, nonce_R + 1) \oplus H^{t-1}(SK)$. Then, RSU verifies if $(nonce_R + 1)$ is correct or not. If it is correct, then RSU knows that V_i has updated its shared key.

2.2 The Drawbacks of Li et al.'s Scheme

For the traffic control, Li et al. proposed a communication model containing three schemes: the vehicle-to-vehicle, the vehicle-to-RSU, and the RSU-to-vehicle communication schemes. However, this model is too complicated and inefficient. For example, in Li et al.'s vehicle-to-vehicle scheme, a vehicle V_i needs to share a session key and keep it to communicate with another vehicle V_j. If V_i wants to communicate with a large amount of vehicles, then V_i also needs to share and keep a large number of session keys for different vehicles. To communicate with RSU, the vehicle V_i also needs to share another session key with RSU. This drawback increases the communication and computation costs of each vehicle in Li et al.'s communication model for the VANET. In addition, to communicate with another vehicle or RSU, each vehicle needs to perform three different schemes. This drawback also makes Li et al.'s model impractical for the VANET.

3 The Proposed Scheme

For the traffic control on the VANET, Li et al. proposed a model containing three communication schemes as follows: the vehicle-to-vehicle, the vehicle-to-RSU, and the RSU-to-vehicle communication schemes. However, we point out that this model is inefficient and impractical in Subsection 2.3. If a vehicle V_i can communicate with the other vehicles through RSU, then V_i only needs to share and keep one session key for RSU on the VANET. Based upon this conception, we propose an efficient vehicle-RSU-vehicle communication scheme for the VANET in this section. Then, Li et al.'s three communication schemes can be simply simplified by the proposed scheme. Therefore, the proposed communication model for the traffic control on the VANET is more efficient and simpler than Li et al.'s model.

Table 2 shows the notations used in the proposed schemes. Now, we present the proposed schemes as follows.

Before describing the proposed scheme, we define some

Table 2: The Notations of the proposed scheme

ID_X	The identity of the entity X
K_{V_i}	A pre-shared key shared between a vehicle V_i and RSU
M	The transmitted message such as traffic information and emergency signal
T_X	A timestamp generated by the entity X
$H(\cdot)$	A secure one-way hash function
ES	The entertainment service such as online music and movies
x	The secret key of RSU
$\|\|$	The concatenation operation

notations as follows. In the proposed scheme, the system chooses $E_p(a, b)$: $y^2 = x^3 + ax + b(\text{mod}p)$ over a prime finite field F_p with the order n, where $a, b \in F_p$, $p > 3$, and $4a^3 + 27b^2 \neq 0(\text{mod}p)$ [6, 7, 8, 9]. Then, the system selects $x \in Z_n*$ to be the secret key of RSU and computes $X = x * Q$ to be the public key of RSU, where Q is a base point over E_p and "*" is the point multiplication over E_p. When a vehicle V_i wants to join into the proposed system, V_i first registers with RSU. Then, RSU generates a pre-shared key $K_{V_i} = H(ID_{V_i}||x)$ for V_i, and thus V_i can use K_{V_i} to communicate with RSU.

Assume that V_i wants to send the message M to another vehicle V_j, then V_i broadcasts M and some authentication information to RSU. Then, RSU can authenticate the source and the validity of M using the pre-shared key K_{V_i}. Also, RSU generates a signature for M using ECDSA [7] and broadcasts it to V_j. Finally, V_j can verify the signature to authenticate the validity of M. The detailed steps are shown as follows.

1) V_i broadcasts $\{ID_{V_i}.ID_{V_j}, M, T_{V_i}, K_{V_i} \oplus H(M||T_{V_i})\}$ to all vehicles and the RSU within its transmission range.

2) After receiving the above message, V_j does not need to authenticate it immediately. V_j just stores this message into its database until it receives the authenticated message from RSU. If V_j does not receive the authenticated message in a pre-defined expiration time, then it discards this message.

3) After receiving $\{ID_{V_i}, ID_{V_j}, M, T_{V_i}, K_{V_i} \oplus H(M||T_{V_i})\}$, RSU computes $K'_{V_i} = H(ID_{V_i}||x)$ according to ID_{V_i}. RSU computes $H'(M||T_{V_i}) = K'_{V_i} \oplus K_{V_i} \oplus H(M||T_{V_i})$. Then, RSU checks if the equation $H'(M||T_{V_i}) = H(M||T_{V_i})$ holds. If it holds, then RSU authenticates the validity of M and T_{V_i}.

4) RSU randomly selects an integer $t \in Z_n^*$ and computes $T = t * Q = (x_1, y_1)$, where x_1 and y_1 are x-coordinate and y-coordinate of T, respectively. RSU computes $r = x_1 \bmod n$ and $s = t^{-1} \cdot [H(M||T_R) + x \cdot t] \bmod n$. Finally, RSU broadcasts $\{ID_R, ID_{V_j}, M, (r, s), T_R\}$ to all vehicles within its transmission range.

5) After receiving the above authenticated message, V_j checks whether the received message is in its database or not. If the message exists, then V_j computes the following $H(M||T_R) \cdot s^{-1} \bmod n$, $r \cdot s^{-1} \bmod n$, and $(H(M||T_R) \cdot s^{-1}) * Q + (r \cdot s^{-1}) * X = (x'_1, y'_1)$. Then, RSU computes $r' = x'_1 \bmod n$ and checks if $r' = r$ holds. If it holds, then V_j confirms that the message is really sent from V_i and M is valid.

Figure 1 illustrates the steps of the proposed vehicle-RSU-vehicle communication scheme. To broadcast a large number of vehicles and RSU, a vehicle only needs to share and keep one session key with RSU in our scheme. Therefore, the proposed scheme greatly reduces the communication loads and computation costs.

Based on the proposed scheme, if RSU wants to broadcast a message M to a vehicle V_i, we only need to perform the similar steps according to Step 1 and Step 3. For example, the RSU replaces $\{ID_{V_i}, ID_{V_j}, M, T_{V_i}, K_{V_i} \oplus H(M||T_{V_i})\}$ with $\{ID_R, ID_{V_j}, M, T_R, K_{V_i} \oplus H(M||T_R)\}$ in Step 1, and then RSU broadcasts it in its broadcast range. Then, V_i can authenticate M by K_{V_i} according to the verification equations in Step 3. Note that only the correct V_i can verify the validity of M. Similarly, if V_i wants to broadcast a message to RSU, then V_i only needs to perform Step 1 and Step 3 by replacing some messages. Therefore, we successfully simplify Li et al.'s three schemes into the proposed vehicle-RSU-vehicle communication scheme.

4 The Security Analysis

To analyze the security of the two proposed schemes, we discuss some possible attacks as follows.

Replay attack. Assume that an attacker wiretaps the communications between the vehicles in the proposed vehicle-RSU-vehicle scheme, then the attacker can obtain $\{ID_{V_i}, ID_{V_j}, M, T_{V_i}, K_{V_i} \oplus H(M||T_{V_i})\}$. Furthermore, the attacker wants to re-broadcast the following message $\{ID_{V_i}.ID_{V_j}, M, T'_{V_i}, K_{V_i} \oplus H(M||T_{V_i})\}$ at the time T'_{V_i}. However, this attack cannot work because RSU computes K_{V_i} and checks if $H(M||T'_{V_i})$ is equal to $H(M||T_{V_i})$. Then, RSU can discover that the message $\{ID_{V_i}, ID_{V_j}, M, T'_{V_i}, K_{V_i} \oplus$

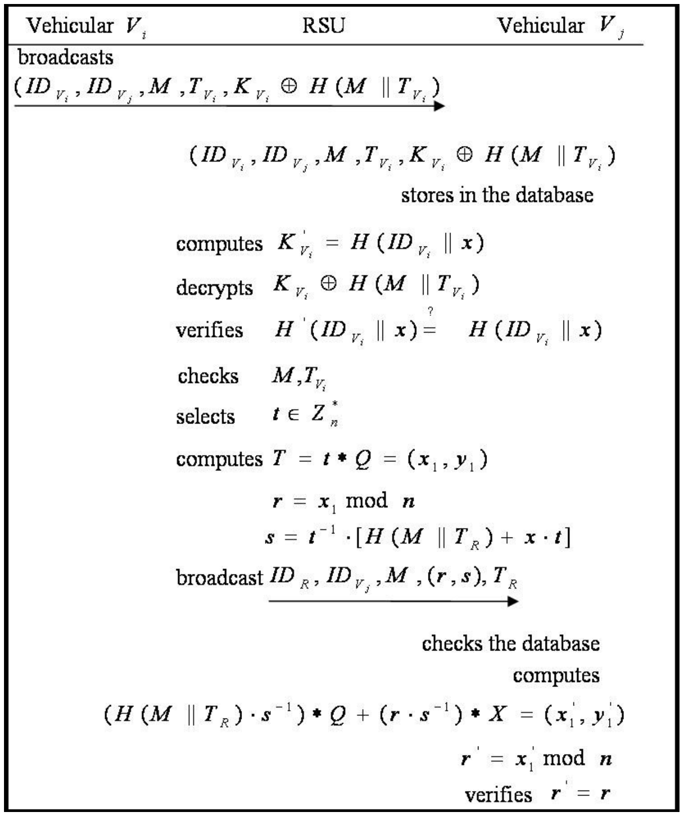

Figure 1: The proposed scheme

$H(M||T_{V_i})\}$ is sent by the attacker because of $H(M||T'_{V_i}) \neq H(M||T_{V_i})$. Hence, this attack is infeasible for the proposed scheme.

Impersonation attack. Assume that an attacker wants to impersonate the vehicle V_i to broadcast the following message $\{ID_{V_i}, ID_{V_j}, M^*, T^*_{V_i}, K^*_{V_i} \oplus H(M^*||T^*_{V_i})\}$ in the proposed vehicle-RSU-vehicle scheme, then he/she selects a random number $x* \in Z_n*$ to compute the pre-shared key $K^*_{V_i} = H(ID_{V_i}||x*)$. In addition, the attacker broadcasts $\{ID_{V_i}, ID_{V_j}, M^*, T^*_{V_i}, K^*_{V_i} \oplus H(M^*||T^*_{V_i})\}$. After receiving the message, RSU computes $K_{V_i} = H(ID_{V_i}||x)$ and checks if $H(M^*||T^*_{V_i})$ is equal to $K_{V_i} \oplus K^*_{V_i} \oplus H(M^*||T^*_{V_i})$ or not. Obviously, RSU can discover that the message $\{ID_{V_i}, ID_{V_j}, M^*, T^*_{V_i}, K^*_{V_i} \oplus H(M^*||T^*_{V_i})\}$ is broadcasted by the attacker because $K^*_{V_i} \neq K_{V_i}$. Therefore, this attack is impossible for the vehicle-RSU-vehicle scheme.

Outsider attack. Assume that an attacker wants to obtain the symmetric key K_{V_i}, then he/she intercepts the communication between a vehicle V_i and RSU to get the messages $\{ID_{V_i}, ID_{V_j}, M, T_{V_i}, K_{V_i} \oplus H(M||T_{V_i})\}$. However, it is infeasible to derive the symmetric key K_{V_i} because the attacker does not know the secret key x of the RSU, where $K_{V_i} = H(ID_{V_i}||x)$. To compute K_{V_i}, the attacker has to know the secret key x. Hence, the outsider attack is impossible for the proposed scheme.

5 Conclusions

In this paper, we propose an efficient authenticated communication scheme for the traffic control on the VANET. In the proposed scheme, a vehicle communicates with the other vehicles through RSU. Based upon this idea, a vehicle only needs to share one session key with RSU to communicate with the other vehicles in the proposed schemes. In addition, the communication model of the proposed schemes is simpler than that of Li et al.'s schemes. Therefore, the proposed schemes are more efficient and practical than the previously proposed schemes for the VANET. In the future, we will investigate a new communication scheme without using the elliptic curve cryptosystem so the vehicle communications on the VANET can become more efficient in practice.

References

[1] M. S. Bouassida, I. Chrisment, and O. Festor, "Group key management in MANETs," *International Journal of Network Security*, vol. 6, no. 1, pp. 67–79, 2008.

[2] D. Chaum, "Blind signature systems," in *Proceedings of Advances in Crypto'83*, pp. 153, 1983.

[3] A. K. Das, "An identity-based random key pre-distribution scheme for direct key establishment to prevent attacks in wireless sensor networks," *International Journal of Network Security*, vol. 6, no. 2, pp. 129–139, 2008.

[4] T. ElGmal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp.469–472, 1985.

[5] S. Eichler, F. Dotzer, C. Schwingenschologl, F. J. F. Vehicleo, and J. Eberspacher, "Secure routing in a vehicular ad hoc network," in *Proceedings of IEEE 60th Vehicular Technology Conference*, pp. 3339–3343, 2004.

[6] M. S. Farash and M. A. Attari, "A pairing-free ID-based key agreement protocol with different PKGs," *International Journal of Network Security*, vol. 16, pp. 144–149, 2014.

[7] D. Johnson, A. Menezes, and S. Vanstone, *The Elliptic Curve Digital Signature Algorithm (ECDSA)*, Techical Report CORR 99-34, 1999.

[8] J. Kar, "ID-based deniable authentication protocol based on Diffie-Hellman problem on elliptic curve," *International Journal of Network Security*, vol. 15, pp. 347–354, 2013.

[9] N. Koblitz, A. J. Menezes, and S. A. Vanstone, "The state of elliptic curve cryptography," *Design, Codes and Cryptography*, vol. 19, no. 2-3, pp. 173–93, 2000.

[10] J. S. Lee and C. C. Chang, "Secure communications for cluster-based ad hoc networks using node identities," *Journal of Network and Computer Applications*, vol. 30, no. 4, pp. 1377–1396, 2006.

[11] C. T. Li, M. S. Hwang, and Y. P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Computer Communications*, vol. 31, no. 12, pp. 2803–2814, 2008.

[12] T. Leinmuller, C. Maihofer, E. Schoch, and F. Karql, "Improved security in geographic ad hoc routing through autonomous position verification," in *Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks*, pp.57–66, 2006.

[13] T. Leinmuller, E. Schoch, and F. Karql, "Position verification approaches for vehicular ad hoc networks," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 16–21, 2006.

[14] J. V. D. Merwe, D. Dawoud, and S. Mcdonald, "A survey on peer-to-peer key management for mobile ad hoc networks," *ACM Computing Surveys*, vol. 39, no. 1, pp. 1–45, 2007.

[15] U. M. Maurer and Y. Yacobi, "A non-interactive public-key distribution system," *Design, Codes and Cryptography*, vol. 9, no. 3, pp. 305–316, 1996.

[16] K. Plossl, T. Nowey, and C. Mletzko, "Towards a security architecture for vehicular ad hoc networks," in *Proceedings of the First International Conference on Availability, Reliability and Security*, pp. 374–381, 2006.

[17] W. Ren, "Pulsing RoQ DDoS attacking and defense scheme in mobile ad hoc networks," *International Journal of Network Security*, vol. 4, no. 2, pp. 227–234, 2007.

[18] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[19] B. Sieka and A. D. Kshemkalyani, "Establishing authenticated channels and secure identifiers in ad-hoc networks," *International Journal of Network Security*, vol. 5, no. 1, pp. 51–61, 2007.

[20] Y. M. Tseng and J. K. Jan, "ID-based cryptographic scheme using a non-interactive public-key distribution system," in *Proceedings of the 14th Annual Computer Security Applications Conference (IEEE ACSAC'98)*, pp. 237–243, 1998.

[21] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 4, pp.386–399, 2006.

Chin-Chen Chang received his Ph.D. degree in computer engineering from National Chiao Tung University. His first degree is Bachelor of Science in Applied Mathematics and master degree is Master of Science in computer and decision sciences. Both were awarded in National Tsing Hua University. Dr. Chang served in National Chung Cheng University from 1989 to 2005. His current title is Chair Professor in Department of Information Engineering and Computer Science, Feng Chia University, from Feb. 2005. He is currently a Fellow of IEEE and a Fellow of IEE, UK. His current research interests include database design, computer cryptography, image compression and data structures.

Jen-Ho Yang received the BS degree in Computer Science and Information Engineering from I-Shou University, Kaoshiung, Taiwan in 2002. He received his Ph.D. degree in Computer Science and Information Engineering from National Chung Cheng University, Chiayi County, Taiwan in 2009. Since 2009, he has been an assistant professor of Department of Multimedia and Mobile Commerce in Kainan University, Taoyuan County, Taiwan. His current research interests include electronic commerce, information security, cryptography, authentication mechanisms, digital right management, and fast modular multiplication algorithm.

Yu-Ching Wu received the BS degree in Computer Science and Information Engineering from National Chung Cheng University, Chiayi County, Taiwan in 2009. His current research interests include information security, cryptography, and vehicular ad hoc networks.