Telecommun Syst (2012) 50:355–365
DOI 10.1007/s11235-010-9409-9

Privacy preservation in secure group communications for vehicular ad hoc networks

Wen-Bing Horng · Cheng-Ping Lee · Jian-Wen Peng

Published online: 9 December 2010

Abstract Secure communications for vehicular ad hoc networks (VANETs) have become an important research issue these years. Many protocols for secure vehicle-to-vehicle communications and vehicle-to-infrastructure communications have been proposed, yet fewer protocols are concerned with secure group communications for VANETs. Of those existing protocols for group communications, some of them form a group of vehicles based on geographical regions and provide broadcasting to the group members with or without message confidentiality. The others allow secure vehicle-to-vehicle communications within a group with session keys, but they do not preserve user privacy for communicating parties within the group. In this paper, we propose a novel group communication scheme for vehicular networks, in which a group is formed by a set of related vehicles of the same purpose, such as a platoon of recreational vehicles targeted for the same tourist spot. The scheme not only offers efficient and secure group communications but also provides privacy preservation for vehicle-to-vehicle communications within a group. Security analysis is given to demonstrate the robustness of the proposed scheme.

W.-B. Horng (✉) · C.-P. Lee
Department of Computer Science and Information Engineering, Tamkang University, 151 Ying-Chuan Road, Tamsui, Taipei, Taiwan 25137, ROC
e-mail: horng@mail.tku.edu.tw

C.-P. Lee
e-mail: selrahc.charles@msa.hinet.net

J.-W. Peng
Department of Commerce Technology and Management, Chihlee Institute of Technology, 313 Section 1, Wunhua Road, Banciao, Taipei, Taiwan 22050, ROC
e-mail: pchw8598@mail.chihlee.edu.tw

Keywords Group communications · Privacy preservation · Vehicular ad hoc network

1 Introduction

The area of vehicular ad hoc networks (VANETs) [32] has been developed significantly during the past decade. In a VANET, there are two kinds of communicating entities: vehicles and roadside base stations. A typical modern vehicle usually consists of several tens of interconnected processors, a wireless communication equipment (such as on-board unit (OBU)), an event data recorder (EDR), a global positioning system (GPS) receiver, and optionally a navigation system, and one or several radars. The mobile vehicles are self-organized and act both as end points and routers to send, receive, and broadcast information to the vehicular network for traffic safety. Wireless links are used to communicate each other directly by single or multiple hops. There are two types of VANET communications [24]: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). The former allows vehicles to communicate with others. The latter can be further classified into two modes [3]: (1) transmitting messages from fixed roadside base stations to mobile vehicles, and (2) transmitting messages from mobile vehicles to fixed roadside base stations. Since the major components of VANETs are vehicles, the network dynamics can be characterized by quasi-permanent mobility, high speeds, and very short connection times between neighbors [25]. One of the advantages of VANETs over other ad hoc networks is that they provide sufficient computational and power resources.

In addition to enhancing traffic safety and efficiency as in intelligent transportation systems, there are a broad range of applications envisioned for VANETs to comfort or to entertain drivers and passengers. In [25], these applications are

divided into two main categories. The first one is safety-related applications which are relevant to life-critical situations to prevent life-endangering accidents, such as collision avoidance and cooperative driving as in lane merging. All other applications belong to the second category, such as traffic optimization, payment service (e.g., toll collection), location-based services (e.g., finding the closest coffee shops), infotainment (e.g., Internet access), etc. To fulfill these applications, the key issue is to provide secure vehicular communications to preserve the privacy of the network users [5, 9, 16–18, 22, 31]. As suggested in [25, 27], a security system for safety messaging in VANETs should contain the following criteria:

- *Authentication*: Vehicles should authenticate the senders to validate the incoming messages to react events.
- *Integrity*: Vehicles should assure that messages are received without modification, insertion, reordering, replaying, or even masquerading for consistency checking.
- *Non-reputation*: It is crucial to prevent the sender from denying the transmission of a message when causing an accident.
- *Privacy*: User privacy should be preserved from disclosing their identities as well as tracking.
- *Confidentiality*: The security system should protect the communication contents from revealing to others except the communicating parties.
- *Availability*: To avoid attacks which bring down the network, availability should be also supported by alternative means.

Many protocols and architectures for secure V2V and V2I communications have been proposed [1, 2, 4, 7, 10, 12, 13, 15, 19–21, 26, 29, 30, 33, 34]. However, there are some situations, such as a platoon of recreational vehicles targeted for the same tourist spot or a fleet of trucks carrying cargoes targeted for the same destination, in which confidential group communications are necessary. Yet fewer protocols are concerned with secure group communications for VANETs. Raya and Hubaux [22, 25] proposed a naive protocol for group communications, where a group is formed by a geographical region. The protocol focuses on the safety-related messages, which are transmitted in plaintext form accompanied with message authentication codes for authentication. Wang et al. [27] improved Raya-Hubaux's protocol with message confidentiality and non-reputation with symmetric encryption and signatures. On the other hand, Li et al. [11] proposed a secure V2V communication scheme within a group. Although they used session keys to provide message confidentiality, their protocol does not preserve privacy for communicating parties within the group while establishing session keys. Beside the secure group communication protocols proposed above, Wasef and Shen [28] also presented a privacy preserving group rekeying scheme to address key updating management for VANETs. However, the computation overhead is costly.

In this paper, we present a novel secure group communication scheme for VANETs to cope with the above security weaknesses. In our scheme, we provide three different communication modes: public broadcast, public V2V, and private V2V communication modes. Our scheme not only offers efficient and secure group communications but also provides privacy preservation for private V2V communications within a group. We then analyze the security features provided by our scheme to demonstrate the robustness of the proposed scheme. The merits of our scheme includes providing (1) secure and quick detection of group messages, (2) group anonymity and non-traceability, (3) message authentication, non-repudiation, and confidentiality, and (4) authenticated key exchange and privacy preservation in the private communications.

The rest of the paper is organized as follows. In Sect. 2, we briefly review related work. In Sect. 3, we present our secure group communication scheme. In Sect. 4, we analyze the security features of our scheme. The last section concludes this paper.

2 Related work

2.1 Raya-Hubaux's protocol

In 2007, Raya and Hubaux [25] devised a group communication mechanism which aims at VANETs with geographically defined groups for efficiently disseminating messages (the term *group*, interchangeably with the term *cluster*, used in their work is in a networking rather than distributed systems sense [23]). In their protocol, roads are pre-divided into cells. Vehicles in each cell form a group and the one nearest to the center of the cell is designated as the group leader.

First, the group leader L distributes the group key K to members, for example, A, B, and C as follows:

$$L \rightarrow *: H_A, \{K\}_{PuK_A}, H_B, \{K\}_{PuK_B}, H_C, \{K\}_{PuK_C}, Sig_{PrK_L}[\textit{the whole message}]$$

where PrK_L is the private key of the group leader L used to sign *the whole message* to obtain the signature Sig, PuK_A is the public key of member A used to encrypt the group key K (i.e., $\{K\}_{PuK_A}$), and H_A is the hash of the receiver A's public key to help the receiver identify which encrypted group key to decrypt. For message broadcasting, Raya and Hubaux used hash-based message authentication code (HMAC) with the group key K for authentication as follows, for example, for message m:

$$L \rightarrow *: m, HMAC_K(m)$$

When a new vehicle D enters the cell, the group leader L sends the group key K to it as follows:

$$L \rightarrow D : \{K\}_{PuK_D}, Sig_{PrK_L}[\{K\}_{PuK_D}]$$

However, they considered only safety-related applications, such as collision avoidance to prevent life-endangering accidents. Their protocol broadcasts messages in plaintext form accompanied with HMACs for verification. Thus, it provides only authentication service for group communications.

2.2 Wang-Hwang-Chen's protocol

In 2008, Wang et al. [27] enhanced Raya-Hubaux's protocol to provide services on confidentiality and non-repudiation. The distribution of group key K to group members from the group leader L is the same as Raya-Hubaux's protocol [25]. When broadcasting messages, they are protected by encryption with group key K for confidentiality. For example, to broadcast a message m, the group leader L performs as follows:

$$L \rightarrow * : E_K[m]$$

where $E_K[m]$ is the symmetric encryption with group key K on message m. If the non-reputation service is needed, L broadcasts the encrypted message together with the signature of HMAC:

$$L \rightarrow * : E_K[m \parallel Sig_{PrK_L}[HMAC_K(m)]]$$

where '$\parallel$' is the concatenation operator. When a new vehicle D enters the cell, it receives the group key K in the same way as in Raya-Hubaux's protocol [25].

In order to decrease the load of group key distribution, both Raya-Hubaux's and Wang et al.'s protocols allow the group leader to decide the group key and to distribute it to its members for authentication and symmetric encryption/decryption of subsequent messages. As a result, the load of the group leader becomes heavy if the number of group members increases.

2.3 Li-Hwang-Chu's protocol

In 2008, Li et al. [11] proposed a secure V2V communication protocol within a group using the non-interactive ID-based public key cryptography [8, 14] for session key exchange in VANETs. Suppose that a source vehicle V_s (with identity VID_s) initiates a connection with a destination vehicle V_d (with identity VID_d) to exchange a session key $K_{s,d}$. V_s first generates a unique $tag\#$, a random number a, and the current timestamp T_{V_s}. It then computes

$$C = (VID_d^2)^{H(T_{V_s} \parallel r_l) * VK_s} \pmod N$$

and

$$D = C \oplus (tag\# \parallel VID_s \parallel VID_d \parallel T_{V_s} \parallel a),$$

where VK_s is the secret key of V_s, $H(\cdot)$ is a hash function, N is a public parameter, and r_l is the identity of a roadway section. Then, V_s broadcasts the following message to all group members:

$$V_s \rightarrow * : H^t(SK) \oplus (tag\#,\ VID_s,\ VID_d,\ hop,\ T_{V_s},\ r_l,\ D)$$

where $H^t(SK)$ is the group key shared among all group members to protect the message from revealing to outsiders.

Upon receiving the message, if a vehicle is the destination node V_d, it can use its group key $H^t(SK)$ to correctly obtain $(tag\#,\ VID_s,\ VID_d,\ hop,\ T_{V_s},\ r_l,\ D)$ and compute

$$C' = (VID_s^2)^{H(T_{V_s} \parallel r_l) * VK_d} \pmod N$$

where VK_d is the secret key of V_d and $C' = C$. Then, it can decrypt D by computing $D \oplus C'$ to recover the message $(tag\# \parallel VID_s \parallel VID_d \parallel T_{V_s} \parallel a)$. The destination vehicle V_d selects a random number b, generates the current timestamp T_{V_d}, and computes the session key $K_{d,s} = H(a \parallel b \parallel 0)$, message authentication code $MAC = H(K_{d,s} \parallel a + 1)$, and

$$D' = C' \oplus (tag\# \parallel VID_d \parallel VID_s \parallel T_{V_d} \parallel r_l \parallel b \parallel MAC).$$

Finally, V_d sends the following response to V_s:

$$V_d \rightarrow V_s : H^t(SK) \oplus (tag\#,\ VID_d,\ VID_s,\ hop,\ T_{V_d},\ r_l,\ D')$$

After receiving the response message from V_d, V_s first decrypts it with the group key $H^t(SK)$ and C to recover $(tag\# \parallel VID_d \parallel VID_s \parallel T_{V_d} \parallel r_l \parallel b \parallel MAC)$. Then, V_s computes the session key $K_{s,d} = (a \parallel b \parallel 0)$ and verifies the validity of MAC. If it holds, the session keys $K_{s,d} = K_{d,s}$, which are used for securing subsequent message transmissions.

In Li et al.'s scheme, the transmitted messages contain the sender's and recipient's identities which are XORed with the group key to preserve privacy. Though the identities of vehicles are protected from outsiders of the group, they are not protected within the group. Besides, the XOR operation is efficient yet not secure enough. If the identity of a group member is leaked, several bits of the group key will be compromised, which can be used to derive the identities of other members from the eavesdropped messages.

2.4 Wasef-Shen's protocol

In addition to the above group communication protocols, Wasef and Shen [28] also presented a privacy preserving group rekeying scheme, called PPGCV, to address key updating management for VANETs. PPGCV is based on a

probabilistic key distribution approach [35, 36] and a security threshold scheme [6]. However, one of the shortcomings of Wasef-Shen's approach is that the load of updating group key is very heavy.

3 Our proposed scheme

In this section, we propose a novel secure group communication scheme preserving privacy for VANETs. Our scheme consists of three phases: initial setup, group key update, and communication phases. The latter phase also contains three communication modes: public broadcast, public V2V, and private V2V communication modes.

In our scheme, each vehicle V_i has its own unique identity VID_i and a pair of public and private keys. Each group G_j of vehicles has its own unique identity GID_j. In addition, each vehicle in the group G_j shares a group secret key SK_j. Note that among each group, a group leader is assigned, denoted as V_{head}, which is known to all its group members and which can change the group identity GID_j and the group secret key SK_j in the group key update phase. Besides, the public key of each vehicle is known to all the other members within the group. Table 1 lists the notation used in our scheme.

3.1 Initial setup phase

A set of related vehicles of the same purpose forms a group, such as a platoon of recreational vehicles targeted for the same tourist spot. Each group has a trusted Group Registration Center (GRC). A group G_j has its own group identity GID_j and group secret key SK_j for secure group communications. Besides, a group leader V_{head} is assigned which is in charge of updating group identity and group secret key to provide more secure communications.

Table 1 Notation used in our scheme

Notation	Meaning
V_i	A vehicle
VID_i	Identity of vehicle V_i
G_j	A group of vehicles
GID_j	Identity of group G_j of vehicles
SK_j	Group secret key of group G_j
T	Timestamp
p	A large prime number
g	A primitive root of p
$\oplus$	Exclusive-OR (XOR) operation
$\|$	Concatenation operation
$h(\cdot)$	Secure one-way hash function
$E_k(M)$	Symmetric encryption of M with secret key k
$D_k(M)$	Symmetric decryption of M with secret key k
$E_{puK}[M]$	Asymmetric encryption of M with public key puK
$D_{prK}[M]$	Asymmetric decryption of M with private key prK
$Sig_{V_i}[M]$	Signature of M signed by the private key of vehicle V_i

Each vehicle V_i registers with the GRC using its unique vehicle identity VID_i. In addition, a pair of public key and private key is assigned by the GRC to the registered vehicle V_i. Before group G_j starts its tourist, each OBU of member vehicle V_i in G_j stores the vehicle identities and public keys of all group members, the group identity GID_j, and the initial group secret key SK_j. Furthermore, to preserve privacy in private V2V communications, two public parameters p and g are required, where p is a large prime number and g is a primitive root of p. Therefore, parameters p and g are also recorded in the OBU of each member vehicle.

Note that as in [25], to withstand attacks, our scheme also assumes that the OBU is a tamper-proof device. The information stored in the OBU cannot be retrieved by any means.

3.2 Group key update phase

To provide more secure group communications, the group leader V_{head} requires to change its group identity and group secret key when appropriate, such as starting a new group tourist. If V_{head}, with identity VID_{head}, wants to update its group identity GID_j and its group secret key SK_j, it performs the following steps (as shown in Fig. 1):

U1. Automatically generate a new group identity GID_{new} and a new group secret key SK_{new}.

U2. Compute

$$Sig_h = S_{V_{head}}[GID_{new}, SK_{new}, T],$$
$$VT_h = VID_{head} \oplus T,$$
$$C = E_{SK_j}(Dest, VT_h, GID_{new}, SK_{new}, Sig_h), \quad \text{and}$$
$$D = GID_j \oplus (h(SK_j \| T) \| (SK_j \oplus T)),$$

where T is the current timestamp and $Dest$ is set to *All-update* to indicate that the message is to be read by all the group members within group G_j to update group identity and group secret key.

U3. Broadcast the message $\{D, C\}$ to all of its group members and replace the group identity GID_j and group secret key SK_j with GID_{new} and SK_{new}, respectively.

When a vehicle V_i, belonging to group G_j, receives the message $\{D, C\}$, it proceeds as follows to perform the update procedure:

U4. Compute $GID_j \oplus D$ to obtain $(H_1 \| H_2)$. Then, calculate timestamp $T' = H_2 \oplus SK_j$ and verify the format and the freshness of T'. If they are not both correct, discard the message without further processing. Otherwise, check if $h(SK_j \| T') = H_1$. If so, the message

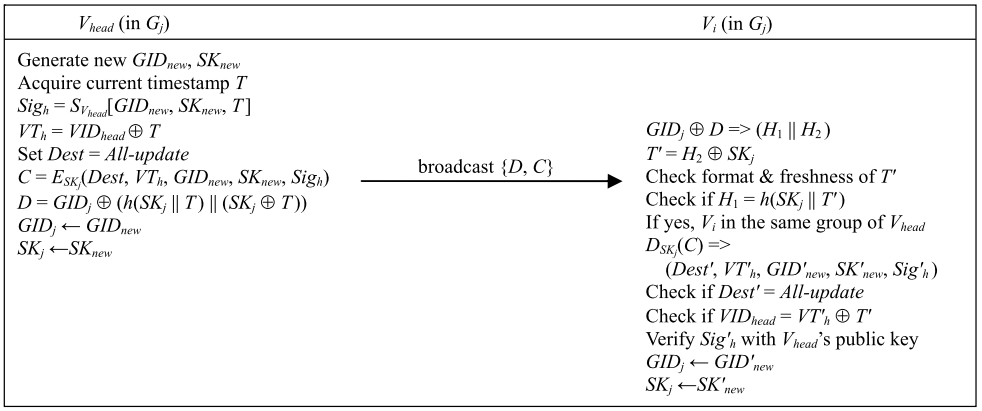

Fig. 1 The group key update phase

$\{D, C\}$ is sent from the same group. Otherwise, discard the message without further processing.

U5. Decrypt the ciphertext C with the group secret key SK_j to obtain $(Dest', VT'_h, GID'_{new}, SK'_{new}, Sig'_h)$. If $Dest' = All\text{-}update$, verify if $VID_{head} = VT'_h \oplus T'$ and check the validity of the signature Sig'_h with the public key of V_{head}. If VID_{head} and the signature Sig'_h are both correct, replace the group identity GID_j and group secret key SK_j with GID'_{new} and SK'_{new}, respectively, for subsequent secure communications. Otherwise, discard the message.

3.3 Communication phase

In our scheme, there are two different types of communications: public communications and private communications. Publication communications mean that messages can be read within the group while they cannot be read outside the group. There are two different modes of public communications: broadcast and V2V unicast. In the former case, messages are sent to all group members, while in the latter case, messages are sent to only one recipient. On the other hand, in private communications, transmitted messages cannot be read not only from outsiders of the group but also within the group except the two communicating parties. In addition, the privacy of communicating parties is preserved in the private communications.

3.3.1 Public broadcast communication mode

When a vehicle V_A, with identity VID_A, wants to broadcast a public message M to all the group members of group G_j, it proceeds as follows (see Fig. 2):

B1. Compute

$$Sig_A = S_{V_A}[M, T],$$
$$VT_A = VID_A \oplus T,$$
$$C = E_{SK_j}(Dest, VT_A, M, Sig_A), \quad \text{and}$$
$$D = GID_j \oplus (h(SK_j \| T) \| (SK_j \oplus T)),$$

where T is the current timestamp, and $Dest$ is set to $All\text{-}read$ to indicate that the message is to be read by all the group members of group G_j.

B2. Broadcast the message $\{D, C\}$ to all group members.

If a vehicle V_i receives the message $\{D, C\}$, it performs the following steps to authenticate M:

B3. Perform Step U4 in the update phase to check whether the sender belongs to the same group of V_i. If V_A and V_i are not in the same group, discard the message. Otherwise, they are in the same group G_j and T' is obtained.

B4. Decrypt the ciphertext C with the group secret key SK_j to obtain $(Dest', VT'_A, M', Sig'_A)$. If $Dest' = All\text{-}read$, compute $VID_A = VT'_A \oplus T'$ and check the validity of the signature Sig'_A with the public key of V_A. If it is correct, the message M' is authenticated (i.e., $M' = M$).

3.3.2 Public V2V communication mode

When a vehicle V_A wants to send a private message m_1 to another vehicle V_B within the same group G_j, it proceeds as follows (as depicted in Fig. 3):

P1. Compute

$$Sig_A = S_{V_A}[VID_B, m_1, T_1],$$
$$VT_{A1} = VID_A \oplus T_1,$$
$$VT_{B1} = VID_B \oplus T_1,$$
$$C_1 = E_{SK_j}(VT_{B1}, VT_{A1}, m_1, Sig_A), \quad \text{and}$$
$$D_1 = GID_j \oplus (h(SK_j \| T_1) \| (SK_j \oplus T_1)),$$

where T_1 is the current timestamp.

P2. Send the message $\{D_1, C_1\}$ to V_B.

When vehicle V_B receives the message $\{D_1, C_1\}$, it performs the following steps to read m_1:

P3. Perform Step U4 in the update phase to check whether the sender belongs to the same group of V_B. If they are

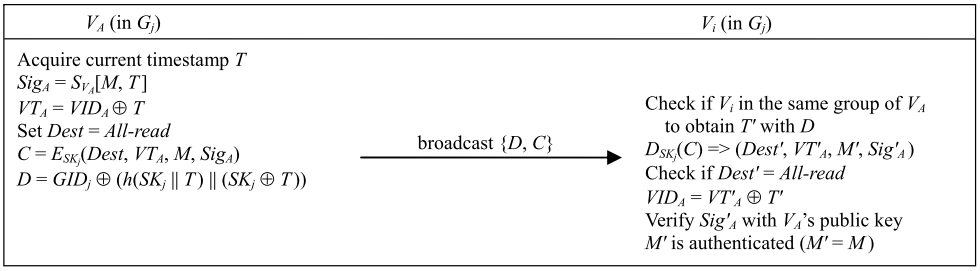

Fig. 2 Public broadcast communication mode

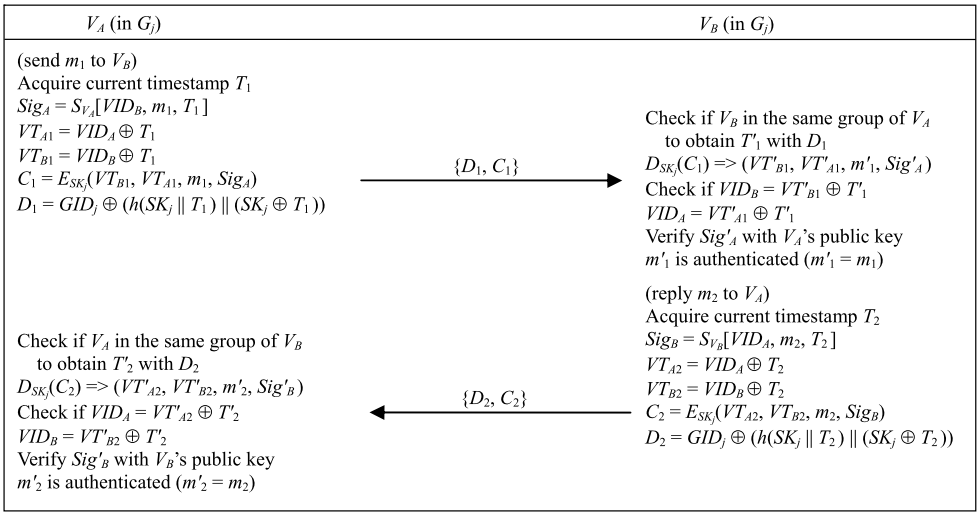

Fig. 3 Public V2V communication mode

not in the same group, discard the message. Otherwise, V_A and V_B are in the same group G_j and T'_1 is obtained.

P4. Decrypt the ciphertext C with the group secret key SK_j to obtain $(VT'_{B1}, VT'_{A1}, m'_1, Sig'_A)$. Verify if $VID_B = VT'_{B1} \oplus T'_1$. If it is, V_B is the correct recipient of the message.

P5. Compute $VID_A = VT'_{A1} \oplus T'_1$ and check the validity of the signature Sig'_A with the public key of V_A. If it is correct, the message m_1 is authenticated.

If V_B wants to reply a message m_2 to V_A, it performs a similar procedure as in Steps P1 and P2 stated above. First, it computes

$$Sig_B = S_{V_B}[VID_A, m_2, T_2],$$

$$VT_{A2} = VID_A \oplus T_2,$$

$$VT_{B2} = VID_B \oplus T_2,$$

$$C_2 = E_{SK_j}(VT_{A2}, VT_{B2}, m_2, Sig_B), \quad \text{and}$$

$$D_2 = GID_j \oplus (h(SK_j \| T_2) \| (SK_j \oplus T_2)),$$

where T_2 is the current timestamp. Then, V_B sends the message $\{D_2, C_2\}$ to V_A. On receiving the message, V_A performs a similar procedure as in Steps P3 to P5 stated above to authenticate m_2 (as shown in Fig. 3).

Note that in both modes of the public communications, the sender and the recipient are known to the other members within the same group. In addition, the transmitted messages M, m_1, and m_2 are also known to all other group members. To protect privacy and confidentiality in private V2V communications, the vehicle identities and the transmitted messages of the two communicating parties should not be revealed to other group members. In the next subsection, we provide a private V2V communication mode to preserve privacy and confidentiality.

3.3.3 Private V2V communication mode

To provide private V2V communications, a session key is needed to be established first. Then, the session key is used to encrypt/decrypt the subsequent messages for secure private communications.

(1) Session key establishment subphase When a vehicle V_A (in group G_j) wants to communicate with another member vehicle V_B privately, they need to establish a session key first. This involves two public parameters p and g, where p is a large prime number and g is a primitive root of p. The vehicle V_A first performs the following procedure to exchange the session key with V_B as follows (Fig. 4):

K1. Generate a random number a and compute

$$Q_A = g^a \bmod p,$$

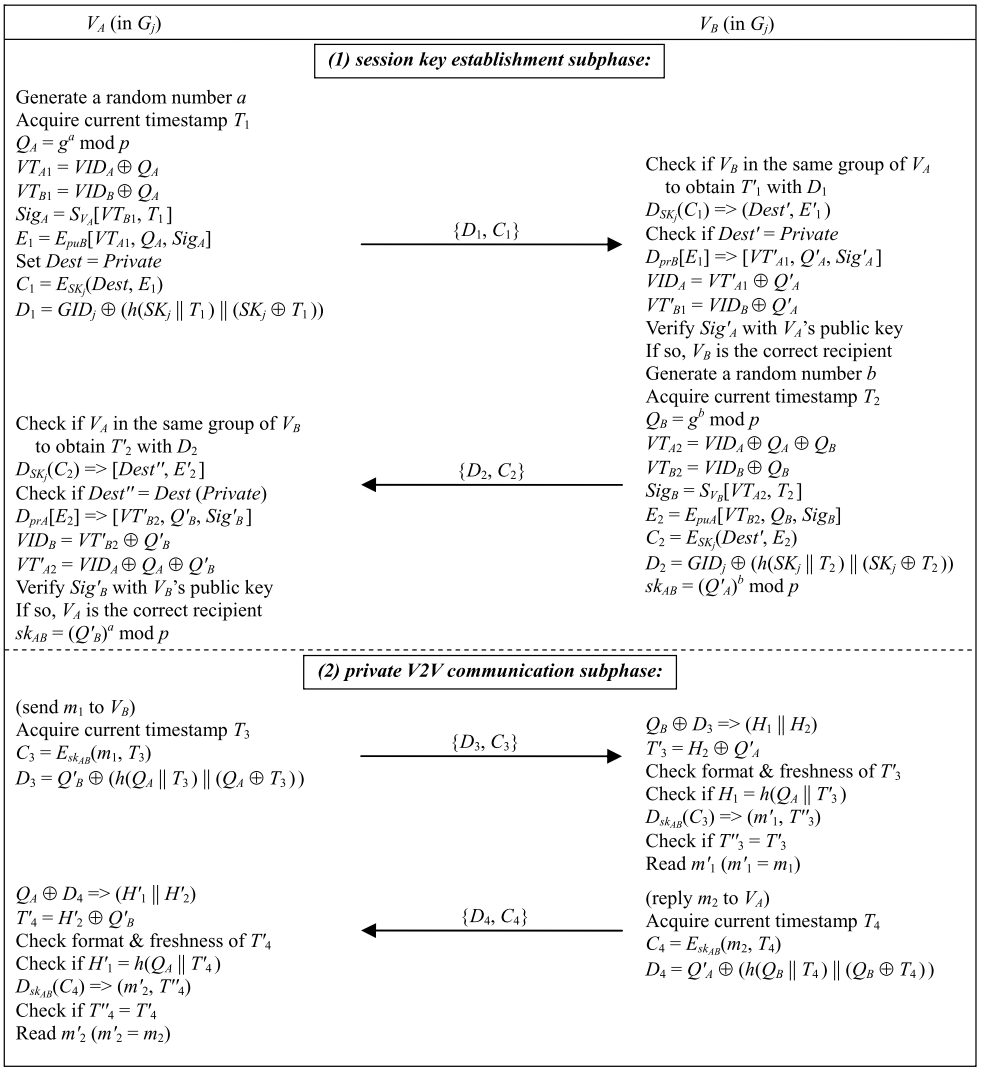

Fig. 4 Private V2V communication mode

$$VT_{A1} = VID_A \oplus Q_A,$$

$$VT_{B1} = VID_B \oplus Q_A,$$

$$Sig_A = S_{V_A}[VT_{B1}, T_1],$$

$$E_1 = E_{puB}[VT_{A1}, Q_A, Sig_A],$$

$$C_1 = E_{SK_j}(Dest, E_1), \quad \text{and}$$

$$D_1 = GID_j \oplus (h(SK_j \| T_1) \| (SK_j \oplus T_1)),$$

where T_1 is the current timestamp, *Dest* is set to *Private* to mean that it is a private communication, and *puB* is the public key of V_B.

K2. Send the message $\{D_1, C_1\}$ to V_B.

When the vehicle V_B receives the message, it performs the following steps:

K3. Perform Step U4 in the update phase to check whether the sender belongs to the same group of V_B. If they are not in the same group, discard the message. Otherwise, V_A and V_B are in the same group G_j and T'_1 is obtained.

K4. Decrypt the ciphertext C_1 with the group secret key SK_j to obtain $(Dest', E'_1)$. If $Dest'$ is equal to *Private*, it means that this is a private communication. Otherwise, discard the message. Decrypt the ciphertext E'_1 with the private key (*prB*) of V_B to obtain $[VT'_{A1}, Q'_A, Sig'_A]$. Compute $VID_A = VT'_{A1} \oplus Q'_A$, $VT'_{B1} = VID_B \oplus Q'_A$, and check the validity of the signature Sig'_A with the public key of V_A. If it is correct, V_B is the correct recipient. Otherwise, discard the message.

K5. Generate a random number b and compute

$$Q_B = g^b \bmod p,$$

$$VT_{A2} = VID_A \oplus Q_A \oplus Q_B,$$

$$VT_{B2} = VID_B \oplus Q_B,$$

$$Sig_B = S_{V_B}[VT_{A2}, T_2],$$

$$E_2 = E_{puA}[VT_{B2}, Q_B, Sig_B],$$

$$C_2 = E_{SK_j}(Dest', E_2), \quad \text{and}$$

$$D_2 = GID_j \oplus (h(SK_j \parallel T_2) \parallel (SK_j \oplus T_2)),$$

where T_2 is the current timestamp and *puA* is the public key of V_A.

K6. Compute the session key $sk_{AB} = (Q'_A)^b \bmod p$ and send $\{D_2, C_2\}$ to V_A.

When the vehicle V_A receives the message, it performs the following steps:

K7. Perform Step U4 in the update phase to check whether the sender belongs to the same group of V_A. If they are not in the same group, discard the message. Otherwise, V_A and V_B are in the same group G_j and T'_2 is obtained.

K8. Decrypt the ciphertext C_2 with the group secret key SK_j to obtain $(Dest'', E'_2)$. If $Dest''$ is equal to $Dest$ (which was set to *Private*), it means that this is a private communication. Otherwise, discard the message.

K9. Decrypt the ciphertext E'_2 with the private key (prA) of V_A to obtain $[VT'_{B2}, Q'_B, Sig'_B]$. Compute $VID_B = VT'_{B2} \oplus Q'_B$, $VT'_{A2} = VID_A \oplus Q_A \oplus Q'_B$ and check the validity of the signature Sig'_B with the public key of V_B. If it is correct, V_A is the correct recipient and computes the session key $sk_{AB} = (Q'_B)^a \bmod p$. Otherwise, discard the message.

(2) Private V2V communication subphase After the session key sk_{AB} is established between V_A and V_B, they can communicate privately without revealing their privacy. When V_A wants to send a message m_1 to V_B privately, it proceeds as follows (Fig. 4):

R1. Compute

$$C_3 = E_{sk_{AB}}(m_1, T_3) \quad \text{and}$$

$$D_3 = Q'_B \oplus (h(Q'_A \parallel T_3) \parallel (Q'_A \oplus T_3)),$$

where T_3 is the current timestamp.

R2. Send $\{D_3, C_3\}$ to V_B.

On receiving the message, V_B performs the following steps to read m_1:

R3. Compute $Q_B \oplus D_3$ to obtain $(H_1 \parallel H_2)$. Compute timestamp $T'_3 = Q'_A \oplus H_2$ and verify the format and freshness of T'_3. If they are not both correct, discard the message. Otherwise, check if $h(Q'_A \parallel T'_3) = H_1$. If so, the message $\{D_3, C_3\}$ is sent from the same group. Otherwise, discard it.

R4. Decrypt the ciphertext C_3 with the session key sk_{AB} to obtain (m'_1, T''_3). Check if $T''_3 = T'_3$. If it is, m'_1 $(= m_1)$ is a new message sent from V_A. Otherwise, discard the message.

If V_B wants to reply a message m_2 to V_A, a similar procedure as stated above in Steps R1 to R4 is performed (as depicted in Fig. 4).

4 Security analysis

4.1 Secure and quick detection of group messages

In our scheme, we use $D = GID_j \oplus (h(SK_j \parallel T) \parallel (SK_j \oplus T))$ for detecting whether messages are sent from within the same group, where T is a timestamp for freshness checking to avoid replay attacks. Since only the member vehicles have the same group identity GID_j and group secret key SK_j, simply using the hash and XOR operations with D, the member vehicle can quickly identify whether the received message $\{D, C\}$ is a message from the same group. Without correct GID_j and SK_j, an outsider adversary of the group is difficult to derive (or guess) the group identity GID_j and the group secret key SK_j from D. Therefore, in our scheme, we use the two factors (GID_j and SK_j) to provide a secure and efficient way to detect group messages.

4.2 Group anonymity and non-traceability

In our scheme, instead of transmitting the group identity GID_j explicitly (i.e., in plaintext form), we embed it in $D = GID_j \oplus (h(SK_j \parallel T) \parallel (SK_j \oplus T))$, where the timestamp T is also sent implicitly in D. As discussed in Sect. 4.1, a member vehicle V_i of G_j can quickly and securely verify if the message $\{D, C\}$ is sent from within the same group. Since an outsider adversary cannot derive group identities from the transcripts, our proposed scheme provides *group anonymity*; it protects group identities from leaking to outsiders. In addition, due to the freshness of the timestamp T, D keeps changing from time to time, instead of a fixed value, and thus the outsider adversary cannot link it to a specific group. Hence, our proposed scheme will not suffer from group tracing; it provides *group non-traceability*.

4.3 Message authentication and non-repudiation

In our scheme, we provide message authentication by the digital signature of the sender as well as the public keys of all group members. Each message is transmitted with the sender's signature, which is generated with sender's private key. The private key is kept secretly, which cannot be leaked to anyone else. Without the sender's private key, no one can forge a sender's signature. Since each signature includes a fresh timestamp T which will be checked with the transmitted message, it cannot be replayed. Therefore, our scheme provides *message authentication* and *non-repudiation*.

4.4 Authenticated key exchange in private communications

In our scheme, during the session key establishment phase in the private V2V communication mode, vehicle V_A sends $E_1(= E_{puB}[VT_{A1}, Q_A, Sig_A])$, encrypted in $C_1(= E_{SK_j}(Dest,\ E_1))$ with group secret key SK_j, to V_B for authentication and session key exchange, where *puB* is the public key of V_B. Only the recipient V_B can correctly decrypt E_1 with its private key (*prB*) to obtain $[VT_{A1}, Q_A, Sig_A]$, where $VT_{A1} = VID_A \oplus Q_A$, $Q_A = g^a \bmod p$, and $Sig_A = S_{V_A}[VT_{B1}, T_1]$. From VT_{A1}, V_B can derive identity of sender VID_A by computing $VT_{A1} \oplus Q_A$, and thus it can verify the signature Sig_A with sender's public key (*puA*) using the information $VT_{B1}(= VID_B \oplus Q_A)$ and T_1, where T_1 can be obtained from D_1 with its group identity GID_j and group secret key SK_j. Since signature Sig_A is signed by V_A's private key (*prA*) with timestamp T_1, it cannot be replayed. Without knowing the private key of V_A, Sig_A cannot be forged. In addition, the signature Sig_A contains the recipient information VT_{B1}. Therefore, if the signature Sig_A is verified successfully, V_B is the correct recipient and V_A is authenticated.

Similarly, V_B sending $E_2(= E_{puA}[VT_{B2}, Q_B, Sig_B])$, encrypted in $C_2(= E_{SK_j}(Dest', E_2))$, to V_A will pass the authentication of V_A, where $Q_B = g^b \bmod p$. Therefore, the generated session key $sk_{AB} = (Q_A)^b \bmod p = (Q_B)^a \bmod p = g^{ab} \bmod p$ will also be authenticated. Thus, our scheme provides *authenticated key exchange* (i.e., session key exchange with mutual authentication) in private V2V communication mode.

4.5 Privacy preservation in private communications

Consider the case that vehicle V_A sends $\{D_1, C_1\}$ to V_B in the session key establishment subphase. The sender information VT_{A1} is encrypted in $E_1(= E_{puB}[VT_{A1}, Q_A, Sig_A])$ with the public key (*puB*) of V_B. Only the correct recipient V_B can use its private key *prB* to obtain VT_{A1} so that it can derive the sender's identity $VID_A = VT_{A1} \oplus Q_A$. Without *prB*, other group members cannot obtain the sender's identity. On the other hand, the recipient information can only be verified by the signature $Sig_A(= S_{V_A}[VT_{B1}, T_1])$ signed by the private key (*prA*) of sender V_A, which is also encrypted in E_1. Without knowing *prB*, there is no way to obtain signature Sig_A to guess the intended recipient V_B. The same conclusion will also be drawn for the case that V_B sends $\{D_2, C_2\}$ to V_A. Therefore, in the session key establishment subphase, sender and recipient identities will not be revealed to others; i.e., during this subphase, our scheme protect *user (vehicle) anonymity*. In addition, each time E_1 and Sig_A are sent differently since they contains random number a (in Q_A) and timestamp T_1, respectively. Thus, the sender and the recipient will be *non-trackable*.

Now, consider the case that V_A sends $\{D_3, C_3\}$ to V_B in the private V2V communication subphase, where $D_3 = Q'_B \oplus (h(Q_A \| T_3) \| (Q_A \oplus T_3))$ and $C_3 = E_{sk_{AB}}(m_1, T_3)$. Only the recipient V_B has the correct Q_A and $Q_B(= Q'_B)$ to obtain the timestamp T_3 for freshness check. In addition, only the recipient V_B has the correct authenticated session key sk_{AB} to decrypt C_3 to obtain (m_1, T_3) for confirmation of T_3 in reading m_1. From the above observation, there is no sender and recipient information conveyed in the message $\{D_3, C_3\}$. Besides, each transmitted message $\{D_3, C_3\}$ are different; there is no way to trace the sender and the recipient. This is the same for $\{D_4, C_4\}$ sent from V_B to V_A. Therefore, we can conclude that our proposed scheme preserve *user (vehicle) privacy* and *non-trackability* in the private V2V communications.

4.6 Message confidentiality

In our scheme, each message is encrypted with a group secret key, SK_j, for public communications or V2V session key, sk_{AB}, for private communications in our scheme. For public communications, without the group secret key, an outsider adversary cannot decrypt the transmitted messages. On the other hand, for private communications, without session keys, even the group members, except the communicating parties, cannot decrypt the private messages. Therefore, our scheme protects *message confidentiality*.

5 Conclusion

It is believed that VANETs will be deployed in the very near future due to the technology advancement. One of the interesting applications is the group communications in VANETs, such as a platoon of recreational vehicles targeted for the same tourist spot, in which security and privacy are two main concerns of the users. In this paper, we proposed an application-layer protocol to satisfy these two criteria. In our protocol, we provide three communication modes: public broadcast, public V2V, and private V2V. We showed that our protocol protects group anonymity. In addition, our scheme also provides message authentication, non-repudiation, and confidentiality. On the other hand, in the private communications, our protocol provides authenticated key exchange to preserve user privacy and non-traceability. Before VANETs to be fully deployed, security on some applications, such as payment service, still need to pay more attention to.

Acknowledgements The authors would like to thank the anonymous reviewers for their valuable comments and constructive suggestions. This research was partially supported by the National Science Council, Taiwan, ROC, under contract no. NSC 98-2631-S-032-003.

References

1. Choi, J. Y., Jakobsson, M., & Wetzel, S. (2005). Balancing auditability and privacy in vehicular networks. In *Proceedings of the 1st ACM international workshop on quality of service and security in wireless and mobile networks* (pp. 79–87). Montreal, Quebec, Canada, October 2005.
2. Choi, J., & Jung, S. (2009). A security framework with strong non-repudiation and privacy in VANETs. In *Proceedings of the 6th IEEE conference on consumer communications and networking* (pp. 835–839). Las Vegas, Nevada, USA, January 2009.
3. Dötzer, F., Kohlmayer, F., Kosch, T., & Strassberger, M. (2005). Secure communication for intersection assistance. In *Proceedings of the 2nd international workshop on intelligent transportation*. Hamburg, Germany, March 2005.
4. Dötzer, F. (2006). Privacy issues in vehicular ad hoc networks. In *Lecture notes in computer science* (Vol. *3856*, pp. 197–209).
5. Hubaux, J. P., Capkun, S., & Luo, J. (2004). The security and privacy of smart vehicles. *IEEE Security and Privacy Magazine*, *2*(3), 49–55.
6. Jiang, Y., Lin, C., Shi, M., & Shen, X. (2006). Multiple key sharing and distribution scheme with (n, t) threshold mechanism for NEMO group communications. *IEEE Journal on Selected Areas in Communications*, *24*(9), 1738–1747.
7. Kim, S. H., Kim, B. H., Kim, Y. K., & Lee, D. H. (2008). Auditable and privacy-preserving authentication in vehicular networks. In *Proceedings of the 2nd international conference on mobile ubiquitous computing, systems, services and technologies* (pp. 19–24). Valencia, Spain, September 2008.
8. Lee, J. S., & Chang, C. C. (2007). Secure communications for cluster-based ad hoc networks using node identities. *Journal of Network and Computer Applications*, *30*(4), 1377–1396.
9. Leinmuller, T., Schoch, E., & Kargl, F. (2006). Position verification approaches for vehicular ad hoc networks. *IEEE Wireless Communications*, *13*(5), 16–21.
10. Leinmuller, T., Schoch, E., & Maihofer, C. (2007). Security requirements and solution concepts in vehicular ad hoc networks. In *Proceedings of the 4th IEEE annual conference on wireless on demand network systems and services* (pp. 84–91). Obergurgl, Austria, January 2007.
11. Li, C. T., Hwang, M. S., & Chu, Y. P. (2008). A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. *Computer Communications*, *31*(12), 2803–2814.
12. Lin, X., Sun, X., Ho, P. H., & Shen, X. (2007). GSIS: a secure and privacy preserving protocol for vehicular communications. *IEEE Transactions on Vehicular Technology*, *56*(6), 3442–3456.
13. Lu, R., Lin, X., Zhu, H., Ho, P. H., & Shen, X. (2008). ECPP: efficient conditional privacy preservation protocol for secure vehicular communications. In *Proceedings of the 27th IEEE conference on computer communications* (pp. 1229–1237). Phoenix, Arizona, USA, April 2008.
14. Maurer, U. M., & Yacobi, Y. (1996). A non-interactive public-key distribution system. *Designs, Codes and Cryptography*, *9*(3), 305–316.
15. Moustafa, H., Bourdon, G., & Gourhant, Y. (2005). AAA in vehicular communication on highways with ad hoc networking support: a proposed architecture. In *Proceedings of the 2nd ACM international workshop on vehicular ad hoc networks* (pp. 79–80). Cologne, Germany, September 2005.
16. Papadimitratos, P., Kung, A., Hubaux, J. P., & Kargl, F. (2006). Privacy and identity management for vehicular communication systems: a position paper. In *Proceedings of the workshop on standards for privacy in user-centric identity management*. Zurich, Switzerland, July 2006.
17. Papadimitratos, P., Gligor, V., & Hubaux, J. P. (2006). Securing vehicular communications—assumptions, requirements, and principles. In *Proceedings of the workshop on embedded security in cars* (pp. 5–14). Berlin, Germany, November 2006.
18. Parno, B., & Perrig, A. (2005). Challenges in securing vehicular networks. In *Proceedings of the 4th workshop on hot topics in networks* (pp. 2803–2814). Maryland, USA, November 2005.
19. Plößl, K., Nowey, T., & Mletzko, C. (2006). Towards a security architecture for vehicular ad hoc networks. In *Proceedings of the 1st international conference on availability, reliability and security* (pp. 374–381). Vienna, Austria, April 2006.
20. Plößl, K., & Federrath, H. (2008). A privacy aware and efficient security infrastructure for vehicular ad hoc networks. *Computer Standards & Interfaces*, *30*(6), 390–397.
21. Raya, M., & Hubaux, J. P. (2005). Security aspects of inter-vehicular communications. In *Proceedings of the 5th Swiss transport research conference*. Monte Verità, Ascona, Switzerland, March 2005.
22. Raya, M., & Hubaux, J. P. (2005). The security of vehicular ad hoc networks. In *Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks* (pp. 11–21). Alexandria, Virginia, USA, November 2005.
23. Raya, M., Aziz, A., & Hubaux, J. P. (2006). Efficient secure aggregation in VANETs. In *Proceedings of the 3rd international workshop on vehicular ad hoc networks* (pp. 67–75). Los Angeles, California, USA, September 2006.
24. Raya, M., Jungels, D., Papadimitratos, P., Aad, I., & Hubaux, J. P. (2006). *Certificate revocation in vehicular ad hoc networks* (LCA-Report-2006-006). School of Computer and Communication Sciences, EPFL, Switzerland, 2006.
25. Raya, M., & Hubaux, J. P. (2007). Securing vehicular ad hoc networks. *Journal of Computer Security*, *15*(1), 39–68.
26. Teo, J. C. M., Ngoh, L. H., & Guo, H. (2009). An anonymous DoS-resistant password-based authentication, key exchange and pseudonym delivery protocol for vehicular networks. In *Proceedings of the IEEE 23rd international conference on advanced information networking and applications* (pp. 675–682). Bradford, United Kingdom, May 2009.
27. Wang, N. W., Huang, Y. M., & Chen, W. M. (2008). A novel secure communication scheme in vehicular ad hoc networks. *Computer Communications*, *31*(12), 2827–2837.
28. Wasef, A., & Shen, X. (2008). PPGCV: privacy preserving group communications protocol for vehicular ad hoc networks. In *Proceedings of 2008 IEEE international conference on communications* (pp. 1458–1463). Beijing, China, May 2008.
29. Xu, Q., Mak, T., Ko, J., & Sengupta, R. (2004). Vehicle-to-vehicle safety messaging in DSRC. In *Proceedings of the 1st ACM international workshop on vehicular ad hoc networks* (pp. 19–28). Philadelphia, Pennsylvania, USA, October 2004.
30. Yang, X., Liu, J., Zhao, F., & Vaidya, N. H. (2004). A vehicle-to-vehicle communication protocol for cooperative collision warning. In *Proceedings of the 1st annual international conference on mobile and ubiquitous systems: networking and services* (pp. 114–123). Boston, Massachusetts, USA, August 2004.
31. Zarki, M. E., Mehrotra, S., Tsudik, G., & Venkatasubramanian, N. (2002). Security issues in a future vehicular network. In *Proceedings of European wireless* (pp. 270–274). Florence, Italy, February 2002.
32. Zeadally, S., Hunt, R., Chen, Y. S., Irwin, A., & Hassan, A. (2010). Vehicular ad hoc networks (VANETs): status, results, and challenges. *Telecommunication Systems*. doi:10.1007/s11235-010-9400-5.
33. Zhang, C., Lin, X., Lu, R., & Ho, P. H. (2008). RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks. In *Proceedings of the 2008 IEEE international conference on communications* (pp. 1415–1457). Beijing, China, May 2008.

34. Zhang, C., Liu, R., Ho, P. H., & Chen, A. (2008). A location privacy preserving authentication scheme in vehicular networks. In *Proceedings of IEEE wireless communications and networking conference* (pp. 2543–2548). Las Vegas, Nevada, USA, March 2008.
35. Zhu, S., Xu, S., Setia, S., & Jajodia, S. (2003). Establishing pairwise keys for secure communication in ad hoc networks: A probabilistic approach. In *Proceedings of the 11th IEEE international conference on network protocols* (pp. 326–335). Atlanta, Georgia, USA, November 2003.
36. Zhu, S., Setia, S., Xu, S., & Jajodia, S. (2006). GKMPAN: An efficient group rekeying scheme for secure multicast in ad-hoc networks. *Journal of Computer Security*, *14*(4), 301–325.

Wen-Bing Horng was born in 1958. He received the B.S. degree from National Cheng Kung University, Tainan, Taiwan, ROC, in 1980, and both the M.S. and Ph.D. degrees in Computer Science from University of North Texas, USA, in 1989 and 1992, respectively. Since 1992, he has been an associate professor at the Department of Computer Science and Information Engineering, Tamkang University, Taipei, Taiwan, ROC. His current research interests include information security, image processing, computer vision, pattern recognition, soft computing, and artificial intelligence.

Cheng-Ping Lee was born in 1971. He received the B.S. degree in Mathematics from National Hsinchu University of Education, Hsinchu, Taiwan, ROC, in 1994, and the M.S. degree in Computer Science and Information Engineering from Tamkang University, Taipei, Taiwan, ROC, in 2001. Lee is currently a Ph.D. candidate in the Department of Computer Science and Information Engineering, Tamkang University. His current research interests include information security, machine learning, and image processing.

Jian-Wen Peng received both the M.S. and Ph.D. degrees in Computer Science and Information Engineering from Tamkang University, Taipei, Taiwan, ROC, in 2001 and 2007, respectively. He is currently an assistant professor in the Department of Commerce Technology and Management, Chihlee Institute of Technology, Taipei, Taiwan, ROC. His research interests are in image processing, information security, and artificial intelligence.