Efficient proxy ring signature for VANET

Lianhai Liu1,2, Yujue Wang2, Jingwei Zhang2, Qing Yang2
e1School of Computer Science and Engineering, Central South University, Changsha, People’s Republic of China
2Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin, People’s Republic of China

Abstract: The messages in vehicular ad hoc networks (VANET) are vulnerable to attack in the open wireless environment. Group communication in VANET is receiving more attention, which confronts many security issues. First, only users who have passed legal authentication can communicate in the group. The ring signature is an effective solution. In addition, the group membership in the vehicular self-organising network changes rapidly, which leads to dynamic adjustment of group members. It is necessary to consider the computing power and communication capability of each node in the group members. To speed up the authentication process, a roadside unit with more computing power and communication capability than vehicles is selected as the signature agent, which effectively reduces the computational load of vehicles and accelerates the communication throughput. Meanwhile, the computational task and communication overhead have not been well-solved. To address these issues, this paper proposed an efficient proxy ring signature scheme for VANET to achieve higher signature efficiency and lower transmission overhead. The scheme allows both privacy protection and original signer tracing. Security analysis shows that the proposed scheme meets the security requirements of VANET.

1 Introduction

Vehicular ad hoc network (VANET) has emerged as a very hot research area over the past few years [1, 2]. It is a special mobile ad hoc network for vehicle communication. VANET will become an important part of future intelligent transportation system. VANET can significantly improve the safety and efficiency of transportation systems and connect vehicles to computer networks. VANET can establish wireless communication between vehicles as well as establish wireless communication between vehicles and roadside units (RSUs). VANET can realise road traffic information query, traffic condition prediction, traffic congestion control and vehicle user access to the Internet. It is increasingly concerned by industry companies, standardisation organisations and research institutions. In VANETs, RSUs and vehicles with wireless on-board units (OBU) form self-organised ad hoc network. They communicate with each other through a dedicated short-range communications (DSRC) protocol [3, 4]. They also collect driving status (e.g. location, speed and braking) and road information (e.g. traffic jam and icy road), and regularly broadcast services information to users [5].

While VANETs bring convenience to the driving experience and traffic safety, there are also huge risks of security and user privacy. First, it should prevent a malicious attacker from modifying the delivered messages to keep message integrity [6]. Second, authentication is needed to ensure user legitimacy; meanwhile, it should provide a guarantee to protect user privacy [7] including vehicle owner, driving route etc. and to trace the real sender in some specific situations. To deal with these issues, many schemes have been proposed for VANETs [7–9]. Chen et al. [10] proposed an ID-based proxy ring signature scheme with a certificate. However, their scheme cannot solve the inherent key escrow problem in ID-based applications. Jiang et al. [9] designed an anonymous communication scheme based on a certificate-less ring signature, which is contributed to reduce the length of signature and simplify key management. Zeng et al. [11] introduced a conditionally anonymous ring signature scheme for VANET to address the issues of anonymous authentication and efficient tracking in case of a dispute. Lang et al. [12] and Gao et al. [13] put forward an improved ID-based proxy ring signature scheme using bilinear pairings, which combines the advantages of proxy signature and ring signature. Unfortunately, their ID-based proxy ring signatures with bilinear pairings require high computational costs for performing several pairing operations. Owing to the limited computational ability of OBU, vehicles may concern about the computational costs. Moreover, the effective communication time between vehicle and RSU becomes less because of the fast speed of vehicle and limitation of the communication distance when using the DSRC protocol. Yu et al. [14] proposed a proxy ring signature scheme for an anonymous voting system with higher security and efficiency than related schemes. However, this scheme still heavily depends on the tamper-proof hardware device. Therefore, it is necessary to effectively reduce the computational complexity at the vehicle side. The proxy ring signature can achieve the signature of the agent instead of the original signer, and can also satisfy the anonymity of the signature while tracking the real signer when necessary. To improve the vehicle's signing efficiency and solve the security requirements, we propose an efficient proxy ring signature (EPRS) scheme for VANETs without bilinear pairings. Our contributions are summarised as follows:

- First, to deal with the above-mentioned problems, we propose a new proxy ring signature without bilinear pairings, which achieves higher signature efficiency and lower transmission overhead.
- Second, by using a new key distribution method, the proxy ring signature can be implemented without the need for tamper-proof hardware device.
- Third, our scheme selects RSU with strong computing power and wide communication bandwidth as the signing agent, which effectively reduces the computational load of vehicle nodes with weak computing power and accelerates the communication throughput.

The remainder of this paper is organised as follows. We describe related works in Section 2 and define the system model and security requirements for VANET in Section 3. We present an EPRS scheme in Section 4 and analyse its security in Section 5. Finally, Section 6 concludes this paper.
2 Related works

With the wide application of digital signature, an ordinary digital signature has been unable to meet the growing safety requirements. Therefore, digital signature schemes have been put forward according to different specific requirements such as identity-based signature, proxy signature, blind signature etc. For the sake of the signature has been unable to meet the growing safety requirements. However, their scheme did not describe how to distribute the specific member. Thus, the ring signature scheme can effectively avoid privacy leaks. Therefore, many anonymous digital signature schemes such as group signature and ring signature have been proposed. The ring signature can realise anonymous signature unconditionally, and is widely applied in data exchange, electronic money and other application fields. At the same time, considering the different computing powers of OBU and RSU, RSU with strong computing power is selected as the signing agent for VANET.

Mambo et al. [15] introduced proxy signature, where the original signer can delegate signing a power to a proxy signer so that the proxy signer can sign on behalf of the original signer. The verifier needs to verify both signature and entrustment signing protocol between the original signer and proxy signer. In a proxy signature scheme, the proxy signer usually has a powerful computing resource, which can effectively reduce the computational task of generating signature by the original signer, and thus greatly improve the signing efficiency. In 2001, Rivest et al. first proposed a ring signature scheme. Ring signatures are distributed with no organisation administrator to manage ring members. In ring signature scheme, the verifier can verify if the signature is generated by some ring member, but cannot identify the specific member. Thus, the ring signature scheme can effectively protect the privacy of real signer in the ring, which means that it can realise unconditional identity anonymity. However, the ring signature scheme does not allow anyone to trace the real signature members. In some case, malicious attackers may abuse ring signatures. Therefore, the ring signature has been extended to support many applications. Zhang and Chen [16] proposed a ring signature scheme using identity or certificate in bilinear groups, which satisfies unconditional anonymity, and the real signer in the ring cannot deny its signature. Zhang and Safavi-Naini [17] proposed a proxy ring signature scheme combining proxy signature and ring signature. The proxy signer can produce signatures on behalf of the original signer with high anonymity.

Zhang et al. [18] proposed a certificate-less proxy ring signature scheme without bilinear pairings and exponentiations. However, their scheme did not describe how to distribute the private key among partners. Since the proxy and ring members are predefined, there is no process to allow membership change in the ring. Therefore, its scheme is not suitable for dynamic VANET. Cui et al. [8] proposed a privacy-preserving authentication scheme with a cuckoo filter for VANET. However, the vehicle needs to sign every message personally. Owing to the limited computing power of the vehicle, RSU with more powerful computing power can be selected as a signature agent. Chen [19] put forward an anonymous attestation scheme under a trusted computing environment. Although the schemes designed by Chen [19] without using bilinear pairings, their security heavily depends on the tamper-proof hardware device.

### Table 1 Notations

| Notations | Definitions |
|-----------|-------------|
| TA        | trusted authority |
| s         | master key of TA |
| \( P_{pub} \) | public key of TA |
| ID_v       | identity of vehicle or RSU |
| PWD_v      | password of vehicle or RSU |
| E(M)       | encrypting function of M using key k |
| \( Y_i \)  | public key of vehicle or RSU |
| \( y_i \)  | private key of vehicle or RSU |
| \( D_i \)  | public key for proxy signature |
| \( d_i \)  | private key for proxy signature |
| \( V_i \)  | validity value for the proxy signature of vehicle or RSU |
| T_A        | validity value for the proxy signature of TA |
| W_v        | hash value for vehicle or RSU |
| K_t        | hash value for TA |
| \( \parallel \) | concatenation operation |

3 Preliminaries

In this section, we briefly introduce the system model and elliptic curve cryptosystem (ECC). Some notations are shown in Table 1.

### 3.1 System model

As shown in Fig. 1, a typical VANET system consists of three types of entities, that is, OBU, RSU and TA:

- **OBU** is responsible for communicating with neighbouring OBUs or RSUs using the 802.11p protocol. OBU is semi-trusted in the system. A vehicle with OBU can regularly broadcast messages of its driving state (e.g. emergency braking). In transmission, it is necessary to sign and authenticate the messages sent by vehicles. Otherwise, the transmitted messages would be vulnerable to attacks launched by malicious attackers. In VANET system, OBU usually has only limited computation and storage capabilities.
- **RSUs** are always deployed on both sides of roads and intersections, which are responsible for vehicle-to-infrastructure communication. RSU is also semi-trusted in the system. They regularly broadcast road information (e.g. road congestion) and local environment (e.g. gas station and parking lot). Since RSUs have the wider broadcast range and more powerful computation capability than OBUs, they are very suitable to serve as proxies to generate ring signatures.
- **Trusted Authority (TA)** is responsible for the generation and distribution of the private and public keys for OBUs and RSUs. It is completely trusted by the other entities in the system. At first, the TA initialises the system and produces public system parameters. Each OBU and RSU has to register to TA, so as to get public and private keys of a proxy ring signature scheme. The traceability of the system allows the TA to find out the real signer when it is necessary [20].

### 3.2 System requirements

The proposed EPRS scheme for VANET without using a bilinear map has to meet the following requirements:

- **Identity privacy**: The real identity of every vehicle should be protected. Otherwise, a malicious attacker could track the personal privacy of a vehicle when it communicates with RSUs.
- **Integrity and authentication**: Verifiers must be able to check the validity and integrity of signatures. Otherwise, the transmitted messages may be changed without being detected.
- **Traceability**: The real identity of the vehicle can be only traced in a particular situation with the help of TA.
- **Low computational costs**: Owing to limited communication resources between vehicle and RSU, there should be no time-consuming computations such as bilinear pairings.
- **Light-weight computational capacity for vehicle**: OBU only has the limited computational capacity; most time-consuming computation in a signature generation should be migrated from vehicle to RSU to reduce computing tasks at vehicle side.

### 3.3 Elliptic curve cryptosystem

Assume \( p \) is a prime number and \( F_p \) is a finite prime field. In mathematics, an elliptic curve \( E_p(a, b) \) is a plane algebraic curve defined by the following equation:

\[
y^2 = (x + ax + b) mod p
\]

(1)
where $a$, $b$, $x$, $y$ \(\in F_p\).

Assume $P(x_1, y_1)$ and $Q(x_2, y_2)$ are two distinct points on the elliptic curve $E_y(a, b)$. Draw a line $L$ through $P$ and $Q$, where $L$ will intersect with the curve. Let the intersected point be $R' = (x_3, y_3)$. $R = (x, y)$ is the symmetric point of $R'$ with respect to the X-axis.

We define an additive cyclic group with the special point $O$ at infinity as follows:

$$P + Q = (\mu^2 - x_1 - x_2, \mu(x_1 - x_2) - y_1) \quad (2)$$

where

$$\mu = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{if } P = Q \end{cases} \quad (3)$$

We also define the following equations:

$$(x_1, y_1) + (x_2, -y_2) = O \quad (4)$$

$$P + O = O + P = P \quad (5)$$

$$R = P + Q \quad (6)$$

Some related mathematical problems of ECC are described as follows:

i. **Elliptic curve discrete logarithm problem (ECDLP):** Given any $n \in Z_p$, it is easy to compute $R = np$. However, it is difficult to calculate $n$ from points $P$ and $R$.

ii. **Computational Diffie–Hellman problem:** Given $a, b \in Z_p'$ and $(P, aP, bP)$, it is difficult to calculate $abP$ without $a$ and $b$.

### 4 Proposed scheme

In this section, to address the security requirements in VANET communication security requirements, we design a secure and EPRS scheme without using bilinear paring. The application process of our proxy ring signature scheme is shown in Fig. 2.

i. **Vehicle** sends its signature to **TA**.

ii. **TA** returns a partial proxy ring signature if the vehicle's signature passes the verification.

iii. **RSU** sends its signature to **TA**.

iv. **TA** returns a partial proxy ring signature if the RSU's signature passes the verification.

v. Some new vehicle requests to join the ring.

vi. **RSU** forwards the request to **TA**.

vii. **TA** sends the verification result of the vehicle's request to **RSU**.

x. **RSU** accepts the vehicle to join the ring if its request passes the verification.

x. **Vehicle** sends trusted member authentication information to **RSU**.

x. **RSU** generates a proxy ring signature if the vehicle's authentication succeeds, and sends the signature to the vehicle.

The proposed scheme consists of seven phases, that is, system initialisation, local key generation, partial proxy ring signing key generation, trusted member authentication, proxy ring signing key generation, proxy ring signing and signature verification.

#### 4.1 System initialisation

Suppose $G_i$ is an addition group on elliptic curves generated by $P$, and its order is a prime number $p$.

**TA** selects two collision-resistant hash functions, that is, $H_i: \{0, 1\}^* \rightarrow G_i$ and $H'_i: \{0, 1\}^* \rightarrow Z_p'$. TA randomly selects $s \in Z_p^*$ as the master key and calculates $P_{pub} = sp$ as the public key of the system.

The system parameters $\text{parame} := \langle G_i, p, P, P_{pub}, H_i, H'_i \rangle$ are broadcasted by **TA** to all users. **TA** keeps the master secret key $s$ secret.

#### 4.2 Local key generation

**Vehicle** randomly selects $y_i \in Z_p'(1 \leq i \leq N)$ as the private key and calculates $Y_i = y_ip$ as the public key. In this paper, let $(y_i, Y_i)$ denote the key pair of the original signer vehicle and $(y_i, Y_i)$ denote the key pair of **RSU**.

#### 4.3 Partial proxy ring signing key generation

The process of partial proxy ring signing key generation is shown in Fig. 3.

i. **With identity ID_v, password PWD, and public key Y_v**, **vehicle** randomly selects $v_i \in Z_p^*$ and computes

$$V_i = v_iP, \quad W_i = H_i(ID_v \parallel PWD_i \parallel Y_v), \quad c_i = v_i + y_iW_i \quad (7)$$

then it sends the signature $\sigma = E_{P_{pub}}(ID_v \parallel Y_v \parallel V_i \parallel c_i)$ to **TA**.

ii. **TA** decrypts $\sigma$. First, **TA** queries the password $PWD_i$ according to the vehicle's identity $ID_v$, computes $W'_i = H_i(ID_v \parallel PWD_i \parallel Y_i)$, and verifies the equality

$$c_iP = V_i + Y_iW'_i. \quad (8)$$

If it holds, **TA** randomly selects $t_i \in Z_p^*$ and computes

$$T_i = t_iP, \quad K_i = H_i(ID_v \parallel Y_i \parallel T_i). \quad (9)$$
\[ d_i = t_i + sK_i. \]  

TA saves \( \{ID_o, Y_o, V_o, d_i, t_i, T_i\} \) at local and sends \( \phi = E_T(ID \parallel T \parallel d_i \parallel K) \) to the vehicle.

iii. Vehicle decrypts \( \phi \) and verifies the following equality:
\[
dP = T_i + KP_{pub}. \tag{11}
\]

If it holds, the vehicle uses the public key \( D_i = V_i + (d_i + \gamma_i)P \) for proxy ring signature and saves \( \{d_i, D_i, T_i, W_i, v_i, V_i\} \) at local.

iv. Denote the information for partial signature (e.g. partial public key and verification information) of the original signer vehicle and RSU by
\[
\{d_o, D_o, T_o, W_o, v_o, V_o\}
\]

and
\[
\{d_i, D_i, T_i, W_i, v_i, V_i\},
\]

respectively.

4.4 Trusted member authentication

The process of trusted member authentication is shown in Fig. 4.

i. When the original signer vehicle goes into the communication range of an RSU, it sends a request to join the trusted member list. That is, the vehicle computes
\[
W_o = H_I(ID_o \parallel PWD_o \parallel Y_o), \quad c_o = v_o + y_oW_o \tag{12}
\]

and sends \( \sigma = E_{pub}(ID_o \parallel Y_o \parallel V_o \parallel c_o) \) to RSU.

ii. RSU forwards the signature \( \sigma \) to TA.

iii. TA decrypts \( \sigma \). TA queries the password \( PWD_o \) according to the vehicle’s identity \( ID_o \) and computes
\[
W_o = H_I(ID_o \parallel PWD_o \parallel Y_o),
\]

and verifies the following equality:
\[
c_oP = V_o + Y_oW_o. \tag{13}
\]

If it holds, TA randomly selects \( m_o \in \kappa Z_q^\phi \) and computes
\[
M_o = m_oP, \tag{14}
\]

\[
J_o = H_I(ID_o \parallel Y_o \parallel T_o \parallel M_o), \quad j_o = t_o + sJ_o, \tag{15}
\]

\[
\lambda_j = E_T(ID_o \parallel Y_o \parallel T_o \parallel J_o \parallel j_o), \tag{16}
\]

\[
\lambda_j = E_T(ID_o \parallel Y_o \parallel T_o \parallel J_o \parallel j_o). \tag{17}
\]

Then TA sends \( \lambda = (\lambda_o, \lambda_j) \) to RSU and saves \( \{ID_o, Y_o, T_o, J_o, j_o\} \) at local.

iv. When receiving \( \lambda \), RSU decrypts \( \lambda \) and checks the following equality:
\[
j_oP = T_o + J_oP_{pub}. \tag{18}
\]

If it holds, RSU saves \( \{ID_o, Y_o, T_o, J_o, j_o\} \) at local and forwards \( \lambda \) to the requested vehicle.

v. The vehicle decrypts \( \lambda_j \) and checks the following equality:
\[
j_oP = T_o + J_oP_{pub}. \tag{19}
\]

If it holds, the vehicle saves \( \{ID_o, Y_o, T_o, J_o, j_o\} \) at local.
\[ X_i = x_i H_i(\xi)(D_i + D_i) - \sum_{i=1, i \neq r}^{M} (X_i + h_i H_i(\xi)D_i) \] (25)

\[ h_i = H_i(m || L || X_i) \] (26)

\[ K = \{x_i k_o + (v_i + x_i + d_i h_i H_i(\xi))p \} \] (27)

iv. RSU outputs the ring proxy ring signature \( \sigma \) on the message \( m \) under the trusted member list \( L \)

\[ \sigma = \{m, X_1, X_2, \ldots, X_i, X_6, X_7, \ldots, X_M, K, L\} \] (28)

\subsection*{4.7 Signature verification}

After receiving the trusted member list \( L \) and signature \( \sigma \), the receiver performs as follows:

i. Compute

\[ h_i = H_i(m || L || X_i) \quad (i = 1, 2, \ldots, M) \] (29)

ii. Verify the equality

\[ K = \sum_{i=1}^{M} (X_i + h_i H_i(\xi)D_i) \] (30)

iii. If it holds, the proxy ring signature is legal. Otherwise, the signature is invalid and would be denied.

\section*{5 Security analysis}

In this section, we analyse our proposed scheme in terms of verifiability, unconditional anonymity and unforgeability:

i. **Verifiability:** OBU can trust that the RSU has the original signer's signature of authorisation information \( m \) according to the \( K \) in the signature \( \sigma \) generated by the signature agent RSU. From the process of generating a proxy ring signature, we can get the following formula:

\[ K = x_i k_o p + h_i H_i(\xi)(v_i + x_i + d_i)p \]

\[ = x_i ((v_i + y_i + d_i)H_i(\xi) + (v_i + y_i + d_i)H_i(\xi))p \]

\[ + h_i H_i(\xi)D_i \]

\[ = x_i H_i(\xi)(D_i + D_i) + h_i H_i(\xi)D_i \]

\[ = x_i H_i(\xi)(D_i + D_i) - \sum_{i=1, i \neq r}^{M} (X_i + h_i H_i(\xi)D_i) \]

\[ + \sum_{i=1, i \neq r}^{M} (X_i + h_i H_i(\xi)D_i) + h_i H_i(\xi)D_i \]

\[ = X_i + \sum_{i=1, i \neq r}^{M} X_i + \sum_{i=1, i \neq r}^{M} h_i H_i(\xi)D_i + h_i H_i(\xi)L \]

\[ = \sum_{i=1}^{M} (X_i + h_i H_i(\xi)D_i) \] (31)

Therefore, proxy ring signatures are verifiable:

ii. **Unconditional anonymity:** Our proposed scheme offers unconditional anonymity, except that only TA is able to trace the real signer anytime. The probability that an attacker can correctly identify the real proxy signer is not more than \( 1/M \).

Let \( \sigma = \{m, X_1, X_2, \ldots, X_i, X_6, X_7, \ldots, X_M, K, L\} \) be a ring proxy ring signature on the message \( m \) under the trusted member list \( L \). During the process of proxy ring signing, RSU randomly selects different \( x_i \in_R Z_p^r \) and

\[ x_i \in_R Z_p^r, x_i \neq x_i (i = 1, 2, 3, \ldots, M, i \neq r) \]

thus the probability of \( X_i \) is

\[ (1/M) \times (1/(M - 1)) \times \cdots \times (1/(q - M)) \].

\begin{table}[h]
\centering
\caption{Computation overhead comparison}
\begin{tabular}{|c|c|c|}
\hline
Scheme & Sign & Verify \\
\hline
AAS [21] & \((4n - 2)T_{GA} + (2n + 2)T_{Cim} + nT_{GA} + nT_{Cim} + 2T_{par} \) & \\
EPRS [14] & \((2n - 1)T_{GA} + (n + 1)V_{GA} + 2T_{par} \) & \\
our scheme & \((2n - 1)T_{GA} + 2nT_{Cim} + 2nT_{GA} + nT_{Cim} \) & \\
\hline
\end{tabular}
\end{table}

In this way, no matter who has signed the message \( M \), and no matter how large the number of ring members is, the probability of generating \( \sigma \) is the same to each of the other ring members. This implies that the probability of determining the identity of a real signer will not exceed \( 1/M \).

iii. **Unforgeability:** The private key \((y_o, d_o)\) of the original signer vehicle and the proxy ring signature key \( k_o \) are all safe. To crack the private key, its hardness is equivalent to solving the ECDLP. In addition, since the proxy signing private key simultaneously includes the private keys of the original signer and proxy signer, anyone cannot forge a proxy ring signature.

Therefore, the proposed scheme offers unforgeability.

iv. **Uncollectability:** In addition to the real signer, other users do not know who the signer is. If there is user collusion in the member list \( L \), all members are required to participate in the collusion; otherwise, the real signer cannot be known either. However, the real signer would rather protect its privacy than risk participating in collusion. Otherwise, it will reveal privacy too.

v. **Performance:** In this section, the proposed scheme is compared with schemes [14, 21] in terms of computation overhead. For comparison, only the time-consuming add/multiplication and bilinear pairing operations are considered. Let \( T_{par} \) be the execution time of a pairing operation, \( T_{GA} \) be the execution time of performing an addition operation over an elliptic curve, \( T_{Cim} \) be the execution time of performing a scalar multiplication over an elliptic curve and \( n \) is the number of vehicles signed by the agent. The comparison of computation costs between the proposed scheme and the existing schemes [14, 21] is summarised in Table 2.

As shown in Table 2, the signature and verification efficiencies of our scheme have been improved in comparison with other schemes. The signature verification of the proposed scheme does not require pairing operations, whereas the other two schemes require two pairing operations. Signature verification is generally performed in OBU with weak computing power. In this way, the computational load of OBU is greatly reduced, and the communication bottleneck in the signing process can be effectively solved.

\section*{6 Conclusions}

In this paper, an EPRS scheme for VANET without bilinear pairing is proposed. Our scheme effectively reduces the vehicle's computing task and communication overhead by introducing a proxy signer. The security analysis demonstrates that our scheme well meets the security requirements for VANET.

\section*{7 Acknowledgments}

This work was supported by the National Natural Science Foundation of China (Nos. 61462017, 61662015, 61662013, 61662013, U1501252, 61502014, 61862012), the Guangxi Key Lab of Wireless Wideband Communication and Signal Processing (GXKL061508), the Guangxi Young Teachers’ Basic Ability Improvement Program under Grant no. 2018KY0194 and the Guangxi Natural Science Foundation (Nos. 2017GXNSFAA198055, 2017GXNSFAA198372, 2016GXNSFAA380149, 2018JJA170035).

\section*{References}

J. Eng., 2019, Vol. 2019 Iss. 9, pp. 5449-5454

This is an open access article published by the IET under the Creative Commons Attribution License

(http://creativecommons.org/licenses/by/3.0/)
8 References

[1] Al-Fuqaha, A., Gharaibeh, A., Mohammedi, I., et al.: ‘Online algorithm for opportunistic handling of received packets in vehicular networks’, IEEE Trans. Intell. Transp. Syst., 2018, PP, (99), pp. 1–12

[2] Yan, G., Olariu, S.: ‘A probabilistic analysis of link duration in vehicular ad hoc networks’, IEEE Trans. Intell. Transp. Syst., 2011, 12, (4), pp. 1227–1236

[3] Chang, C.J., Cheng, R.G., Shih, H.T., et al.: ‘Maximum freedom last scheduling algorithm for downlinks of DSRC networks’, IEEE Trans. Intell. Transp. Syst., 2007, 8, (2), pp. 223–232

[4] Oh, H., Yae, C., Ahn, D., et al.: ‘5.8 GHz DSRC packet communication system for its services’. IEEE VTS 50th Vehicular Technology Conf., Amsterdam, Netherlands, 1999, 4, pp. 2223–2227

[5] Liu, L., Wang, J., Huang, J., et al.: ‘Encounter prediction-based data forwarding for high reliability in bus networks’, Ad Hoc Sens. Wirel. Netw., 2018, 41, (1–2), pp. 137–164

[6] Dahiya, P.K., Singh, V.: ‘Security issues in VANEts’. TEQIP Sponsored National Conf. Technical Collaboration with IEEE-EMBS/IMS Delhi chapter, Anaheim, USA, 2010

[7] Emara, K., Woerndl, W., Schlichter, J.: ‘Poster: context-adaptive user-centric privacy scheme for VANEIT’. Int. Conf. Security and Privacy in Communication Systems, Dallas, USA, 2015, pp. 590–593

[8] Cui, J., Zhang, J., Zhong, H., et al.: ‘SPACF: a secure privacy-preserving authentication scheme for VANEIT with cuckoo filter’, IEEE Trans. Veh. Technol., 2017, PP, (99), p. 1

[9] Jiang, Y., Ji, Y., Liu, T.: ‘An anonymous communication scheme based on ring signature in VANEIT’, abs/1410.1639, pp. 1–20

[10] Chen, H., Li, W., Su, Y.: ‘Certificate-based proxy ring signature scheme’, Comput. Eng., 2012, 38, (16), pp. 149–152

[11] Zeng, S., Huang, Y., Liu, X.: ‘Privacy-preserving communication for VANEITs with conditionally anonymous ring signature’, Int. J. Netw. Secur., 2015, 17, (2), pp. 135–141

[12] Lang, W., Yang, Z., Cheng, W., et al.: ‘A new improved ID-based proxy ring signature scheme from bilinear pairings’, J. Harbin Inst. Technol. (New Series), 2006, 13, (6), pp. 688–691

[13] Gao, T., Miao, Q., Guo, N.: ‘Anonymous authentication scheme based on proxy group signature for wireless mesh network’, EURASIP J. Wirel. Commun. Netw., 2016, 2016, (1), pp. 533–537

[14] Yu, Y., Yan, G., Li, F., et al.: ‘An efficient proxy ring signature scheme’, Beijing Univ. Posts Telecommunic., 2007, 30, (3), pp. 23–26

[15] Mambo, M., Usuda, K., Okamoto, E.: ‘Proxy signatures: delegation of the power to sign messages’, IEICE Trans. Fundam. A, 1996, 79, (9), pp. 1338–1354

[16] Zhang, J., Chen, H.: ‘An efficient t-times proxy ring signature scheme with revocable anonymity’. IEEE Int. Conf. Communication Software and Networks, X’an, China, 2011, pp. 6–10

[17] Zhang, F., Safavi-Naini, R.: ‘New proxy signature, proxy blind signature and proxy ring signature schemes from bilinear pairings’, Naini, 2003, 2003, pp. 1–11

[18] Zhang, C., Su, B., Yao, S.: ‘Certificate-less proxy ring signature scheme without bilinear pairings’, Appl. Rev. Comput., 2013, 30, (12), pp. 3797–3799

[19] Chen, K.: ‘Research on identity based ring signature and proxy ring signature’. PhD dissertation, University of Science & Technology China, 2008

[20] Pournaghi, S.M., Zahednejad, B., Bayat, M., et al.: ‘NECPPA: a novel and efficient conditional privacy-preserving authentication scheme for VANEIT’, Comput. Netw., 2018, 134, pp. 78–92

[21] Wang, Y.: ‘Research on anonymous authentication based on agent ring signature’. PhD dissertation, Yunnan University, 2012

This is an open access article published by the IET under the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/)