Original Research Paper | Computer Science | Volume : 3 ¦ Issue : 12 ¦ Dec 2018 ¦ e-ISSN : 2456-5040

IMPROVEMENT ON A CONDITIONAL PRIVACY-PRESERVING AUTHENTICATION SCHEME FOR VANET

Lin Si [1], Baoyuan Kang [1], Mingming Xie [2]

[1] School of Computer science and software, Tianjin polytechnic university, Tianjin, 300387, China.

ABSTRACT

Based on the roadside unit (RSUB) and tamper proof devices (TPDB) technology, Poursnaghi and Zahednejad proposed a conditional privacy-preserving authentication scheme for intelligent transportation. Through analysis, we found that their scheme can't effectively achieve conditional tracking, and there are loopholes in the tracking identity phase, which makes the scheme vulnerable to internal attacks. At the same time, due to the lack of randomness of the signature of the message, the scheme is vulnerable to spoofing attacks. In order to overcome the shortcomings of the Poursnaghi et al. scheme, an improved scheme is presented. The improvement scheme improves the way of providing the identity information of the onboard unit (OBU) in the original scheme and the signature of the message, so that the trusted authority (TA) can obtain the identity information of the onboard unit (OBU) through calculation, thereby verifying Whether the two sides of the communication are credible, effectively avoiding internal attacks, and improving the randomness of the signature of the message, effectively avoiding the counterfeit attack and improving the security of the solution.

INDEX TERMS: VANET; Authentication Scheme; Conditional Privacy-preserving; Security

I. INTRODUCTION:

The vehicular ad-hoc network (VANET) is a special type of mobile ad-hoc network (MANET) in which vehicles are used as nodes to form a network through interconnections between them, which can enhance the entire network by immediately changing their topology. Flexibility. The various communications carried out in VANET are mainly inter-vehicle communication (V2V), vehicle-to-infrastructure communication (V2I) or vehicle-to-infrastructure communication (V2V2I). Vehicles communicate with each other in an autonomous manner.

The coverage of VANET can be a circle with a radius of several kilometers, and each vehicle can communicate with other vehicles 2-3 km away by using the IEEE 802.11p standard and the dedicated short-range communication protocol (DSRC). DSRC is a communication protocol used between OBUs that operates at 5.9 GHz. Short-range communication is provided through the use of the DSRC vehicular ad hoc network. According to the DSRC agreement, each vehicle periodically broadcasts information about road traffic and vehicle conditions every 100-300 milliseconds. Among them, road traffic conditions include weather conditions, road defects, congestion conditions, etc.; vehicle conditions include location, speed, traffic conditions, and the like. Upon receipt of this information, other vehicles can adjust their route to avoid possible traffic events such as traffic jams, traffic accidents, etc. In addition, the RSU can also send messages about traffic conditions to the traffic control center. Based on the information received, the traffic control center can take timely action (such as adjusting traffic lights) to improve traffic safety and efficiency [1].

A general VANET system model consists mainly of the following entities:

TA: It is the trusted management organization of VANET. It is responsible for the initial setup of the network and provides users with the main and initial parameters of the network, such as private and public keys. Each car should be registered to join the network through the TA. TA has strong computing power and storage capacity. It is the only party that can reveal the identity of the signer. TA defaults to trust. **RSU:** It is a roadside infrastructure that can communicate with the OBU by using the DSRC protocol. It can also connect to VANET's network infrastructure via wired or wireless communication technologies such as the Internet. It can also provide services such as Web and TCP for OBU. RSU is considered a fully trusted party in the system. In our proposed solution, RSU will help TA reveal the identity of the signer.

OBU: It is the internal processing unit of the vehicle. Each car is equipped with an OBU. It stores the public key and the public information of the network. As the vehicle moves, it periodically broadcasts information such as location, time, speed, vehicle path and traffic conditions to other vehicles and RSUs.

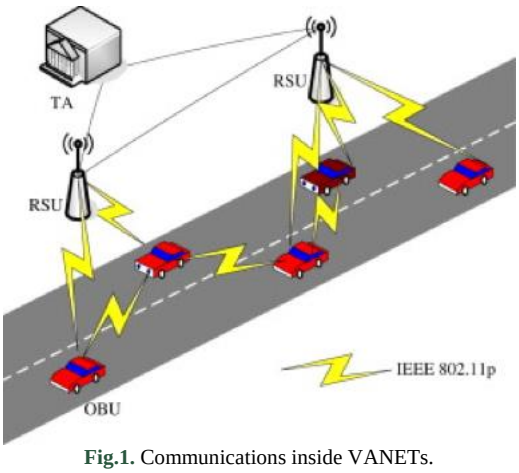

Fig.1. Communications inside VANETs.

In 2006, Gamage et al.[4] proposed an identity-based ring signature scheme to meet the privacy requirements of signers in VANET applications. However, this solution does not enable identity traceability. In 2008, Lu et al.[5] proposed an anonymous anonymous certificate based on group signature for anonymous authentication, which allows group members to sign messages anonymously on behalf of the entire group. In 2013, Horng et al.[8] designed a batch anonymous authentication scheme. RSU generates pseudonyms for each vehicle and communicates by pseudonym, thus avoiding a large number of public and private key pairs for each vehicle, but after analysis, it was found The security of the RSU is difficult to guarantee. In 2015, Bayat et al.[9] proposed a batch verification scheme based on vehicular self-organizing network, which improved the vulnerability of Lee et al., but the cost of communication was too high in the TPD-based authentication scheme. Not solved.

II. POURSNAGHI ET AL.'S SCHEME AND ITS SHORTCOMING:

2.1 Poursnaghi et al.'s scheme:

System Initialization Phase:

(1) G_1 is an addition cycle group with a generator of P, and G_2 is a multiplication cycle group. G_1 and G_2 have the same prime order q. Let be $e: G_1 \times G_1 \to G_2$ a bilinear pairing.

(2) Hash function: $H: \{0,1\}^* \to G_1, h: \{0,1\}^* \to Z_p^*$.

(3) TA chooses a random number $S_{TA} \in {}_R Z_p^*$ as its master key and computes $P_{pub}^{TA} = S_{TA}P$ as its corresponding public key.

(4) TA chooses the symmetric encryption $ENC_x(\cdot)$ and decryption function $DEC_x(\cdot)$. Then TA stores the public parameters $< G_1, G_2, q, P, P_{pub}^{TA}, Cert_{P_{pub}^{TA}}, e(\cdot), H(\cdot), ENC_x(\cdot), DEC_x(\cdot) >$ in RSUs and OBUs.

(5) TA generates S_{RSU_j} as a master key for each RSU_j and then stores S_{TA} and S_{RSU_j} on the tamper proof device of RSU_j.

OBU Joins the RSU Group Phase:
When an OBU_i arrives to the area covered by RSU_j, it should be authenticated to RSU_j to obtain the temporary master key of RSU_j.

(1) OBU_i chooses a random number $r \in {}_R Z_p^*$ and computes its pseudo identity $PID_i =< PID_i^1, PID_i^2 >, PID_i^1 = rP$.

(2) OBU_i Send its pseudo identity to RSU_j. RSU_j Computes OBU_i's real identity by $RID = PID^2{}_i \oplus h(S_{TA} PID_i^1)$.

(3) Then RSU_j checks the certificate revocation list which is transmitted by TA to ensure that OBU_i is not revoked. RSU_j chooses a random integer a and computes the $x = h((aP)_x)$ as the shared secret key between RSU_j and OBU_i where $(aP)_x$ denotes the X-coordinate of the elliptic curve point aP. RSU_j then computes $R = aPID_i^1 = arP$ and sends it to OBU_i.

(4) RSU_j computes a new temporary key $S_{RSU_j}^{Ts} = h(S_{RSU_j} \| Ts)$, and its public key $P_{RSU_j}^{Ts} = S_{RSU_j}^{Ts} P$ that is valid in Ts. It then periodically broadcasts its public key $(P_{RSU_j}^{Ts})$ whit its stamp on Ts its coverage area.

(5) RSU_j encrypts its private key $S_{RSU_j}^{Ts}$ as $ENC_x(S_{RSU_j}^{Ts}, Cert_{P_{RSU_j}^{Ts}})$ with the shared secret key x. RSU_j sends $< R, ENC_x(S_{RSU_j}^{Ts}, Cert_{P_{RSU_j}^{Ts}}) >$ to OBU_i.

(6) When OBU_i receives the parameters, it computes $x = h((Rr^{-1})_x) = h(arp \times r^{-1}) = h(h(aP)_x)$ to get the shared key x. Then TPD decrypts $DEC_x(S_{RSU_j}^{Ts}, Cert_{P_{RSU_j}^{Ts}})$ and store $S_{RSU_j}^{Ts}$.

Message signing phase:
OBU_i has to generate a pseudo-ID and the relevant private key for each message according to the temporary key valid in Ts.

(1) OBU_i chooses a random number $z_i \hat{I} {}_R Z_q^*$.

(2) OBU_i generates the pseudo-ID $pID_i =< pID_i^1, pID_i^2 >$ by computing $pID_i^1 = z_i P, pID_i^2 = RID_i \oplus h(z_i S_{RSU_j}^{Ts})$ and its relevant private key $sK_i =< sK_i^1, sK_i^2 >$ by computing $sK_i^1 = S_{RSU_j}^{Ts} pID_i^1, sK_i^2 = S_{RSU_j}^{Ts} H(pID_i^1 \| pID_i^2 \| Ts)$.

(3) OBU_i signs the message M_i: $\delta_i = sK_i^1 + h(M_i) sK_i^2$.

(4) OBU_i sends the signature $< pID_i, \delta_i, M_i, ID_{RSU_j} >$ to the receiver.

Message verification phase:
After receiving the message, the receiver first verifies the authenticity of the message and then accepts the message.

$$e(\delta_i, P) = e(pID_i^1, P_{RSU_j}^{Ts}) \cdot e(h(M_i) H(pID_i^1 \| pID_i^2 \| Ts) P_{RSU_j}^{Ts})$$

Vehicle real identity tracking and revocation phase:
TA and RSU are the only entities who can both trace and revoke a malicious vehicle. TA can then obtain the true identity of the malicious vehicle through the temporary master key of the RSU that has been sent to the malicious vehicle:

$$pID_i^2 \oplus H(S_{RSU_j}^{Ts} pID_i^1) = RID_i.$$

2.2 Problems of Poursnaghi et al.s scheme:
Internal attack:
The attacker ***Eve*** submitted the relevant materials to the TA to complete the vehicle registration and become a legitimate user. After the attacker ***Eve's*** vehicle OBU_E enters the coverage area of RSU_j to complete authentication and revocation list verification:

(1) RSU_j computes a new temporary key $S_{RSU_j}^{Ts_E}$ valid in Ts.

(2) ***Eve*** chooses a random number $z_E \in {}_R Z_q^*$ and generates its pseudo-ID $pID_E =< pID_E^1, pID_E^2 >, pID_E^1 = z_E P, pID_E^2 = X \oplus h(z_E S_{RSU_j}^{Ts_E})$.
Note that since there is no verification of the true identity in this phase, the attacker ***Eve*** can use any number X in this phase to impersonate its true identity.

(3) ***Eve*** computes the relevant private key of pseudo-ID $sK_E =< sK_E^1, sK_E^2 >, sK_E^1 = S_{RSU_j}^{Ts_E} pID_E^1, sK_E^2 = S_{RSU_j}^{Ts_E} H(pID_E^1 \| pID_E^2 \| Ts_E)$.

(4) ***Eve*** uses its private sK_E to sign the harmful message M_E: $\delta_E = sK_E^1 + h(M_E) sK_E^2$.

(5) ***Eve*** sends $< pID_E, \delta_E, M_E, ID_{RSU_j} >$ to others.

(6) TA and RSU can only restores the number X by computing $pID_E^2 \oplus H(S_{RSU_j}^{Ts_E} pID_E^1) = X$, and the X is just a number not the ***Eve's*** real ID.

Impersonation attack:
Since a vehicle can issue multiple messages within a certain period of time, the attacker ***Eve*** can receive multiple message-signature pairs issued by the vehicle during the Ts_E period. Moreover, due to the low randomness of the signature of the message in this scheme, the attacker ***Eve*** can use the signature of the message to calculate the private key pair corresponding to the temporary pseudo identity of the vehicle, and use the private key pair to issue harmful information. The attack mode is as follows:

Suppose that OBU_i send messages and signatures $< pID_i, \delta_1, M_1, ID_{RSU_j} >$, $< pID_i, \delta_1, M_1, ID_{RSU_j} >$ during the Ts_E period, ***Eve*** can obtain δ_1, δ_2 and copmute:

$$\delta_1 = sK_i^1 + h(M_1)sK_i^2 \quad (1)$$

$$\delta_2 = sK_i^1 + h(M_2)sK_i^2 \quad (2)$$

Equation (1) is multiplied by $h(M_2)$ on both sides, equation (2) is multiplied by $h(M_1)$ on both sides:

$$h(M_2)\delta_1 = h(M_2)sK_i^1 + h(M_1)h(M_2)sK_i^2 \quad (3)$$

$$h(M_1)\delta_2 = h(M_1)sK_i^1 + h(M_1)h(M_2)sK_i^2 \quad (4)$$

Equation (3) subtract equation (4):

$$h(M_2)\delta_1 - h(M_1)\delta_2 = (h(M_2) - h(M_1))sK_i^1$$

$$sK_i^1 = (h(M_2)\delta_1 - h(M_1)\delta_2)(h(M_2) - h(M_1))^{-1}$$

And then computes:

$$sK_i^2 = (\delta_1 - (h(M_2)\delta_1 - h(M_1)\delta_2)(h(M_2) - h(M_1))^{-1})h(M_1)^{-1}$$

At this point, the attacker ***Eve*** gets the private key $< sK_i^1, sK_i^2 >$, it can use the key to sign the harmful messages.

III. THE PROPOSED SCHEME:

In order to overcome the security weaknesses and shortcomings of the Poursnaghi et al.'s scheme, we propose an improved authentication scheme. The improved scheme includes the system initialization phase, the OBU joins the RSU group phase, the message signing phase, the message verification phase, and the vehicle real identity tracking and revocation phase. The system initialization phase in the improvement scheme and the vehicle real identity tracking and revocation phase in the improvement scheme is the same as the corresponding phase of the Poursnaghi et al.'s.

OBU Joins the RSU Group Phase:

When an OBU_i arrives to the area covered by RSU_j, it should be authenticated to RSU_j to obtain the temporary master key of RSU_j.

(1) OBU_i chooses a random number $r \in {}_R Z_q^*$ and computes its pseudo identity $PID_i =< PID_i^1, PID_i^2 >$, $PID_i^1 = rP$.

(2) OBU_i send its pseudo identity to RSU_j. RSU_j computes OBU_i's real identity by $RID = PID^2{}_i \oplus h(S_{TA}PID_i^1)$.

(3) Then RSU_j checks the certificate revocation list which is transmitted by TA to ensure that OBU_i is not revoked. RSU_j chooses a random integer a and computes the $x = h((aP)_x)$ as the shared secret key between RSU_j and OBU_i where $(aP)_x$ denotes the X-coordinate of the elliptic curve point aP. RSU_j then computes $R = aPID_i^1 = arP$ and sends it to OBU_i.

(4) RSU_j's TPD computes a new temporary key , and its public key $S_{RSU_j}^{Ts} = h(S_{RSU_j} \| Ts)$ that is valid in Ts. It then periodically broadcasts its public key $(P_{RSU_j}^{Ts})$ with its stamp on Ts its coverage area.

(5) RSU_j's TPD chooses a random number $z_i \in {}_R Z_q^*$ and generates OBU_i's temporary pseudo-ID $pID_i =< pID_i^1, pID_i^2 >$, $pID_i^1 = z_i P$, $pID_i^2 = RID_i \oplus h(z_i S_{RSU_j}^{Ts})$.

(6) RSU_j encrypts its private key and OBU_i's temporary pseudo-ID $S_{RSU_j}^{Ts}, pID_i$ as $ENC_x(S_{RSU_j}^{Ts}, Cert_{P_{RSU_j}^{Ts}}, pID_i)$ with the shared secret key x. RSU_j sends $< R, ENC_x(S_{RSU_j}^{Ts}, Cert_{P_{RSU_j}^{Ts}}, pID_i) >$ to OBU_i.

(7) When OBU_i receives the parameters, it computes $x = h((Rr^{-1})_x) = h(arp \times r^{-1}) = h(h(aP)_x)$ to get the shared key x. Then TPD decrypts $DEC_x(S_{RSU_j}^{Ts}, Cert_{P_{RSU_j}^{Ts}}, pID_i)$, stores $S_{RSU_j}^{Ts}$, and use pID_i as its temporary pseudo-ID.

Message signing phase:

OBU_i uses RSU_j's temporary private key and OBU_i's temporary pseudo-ID to generate its private key.

(1) $sK_i =< sK_i^1, sK_i^2 >$, $sK_i^1 = S_{RSU_j}^{Ts} pID_i^1$, $sK_i^2 = S_{RSU_j}^{Ts} H(pID_i^1 \| pID_i^2 \| Ts)$.

(2) OBU_i chooses a random number $u_i \in {}_R Z_q^*$.

(3) OBU_i signs the message $M_i : \delta_i = sK_i^1 + h(M_i)sK_i^2 + u_i$.

(4) OBU_i sends signature $< pID_i, \delta_i, M_i, ID_{RSU_j} >$ to receiver.

Message verification phase

After receiving the message, the receiver first verifies the authenticity of the message and then accepts the message.

$$e(\delta_i, P) = e(pID_i^1, P_{RSU_j}^{Ts}) \cdot e(h(M_i)H(pID_i^1 \| pID_i^2 \| Ts)P_{RSU_j}^{Ts}) \cdot e(u_i, P)$$

IV. SECURITY ANALYSIS:

4.1 Proof of correctness:

$$L.H.S = e(\delta_i, P) = e(sK_i^1 + h(M_i)sK_i^2 + u_i, P)e(u_i, P)$$
$$= e(sK_i^1, P) \cdot e(h(M_i)sK_i^2, P) \cdot e(u_i, P)$$
$$= e(S_{RSU_j}^{Ts}, pID_i^1, P) \cdot e(h(M_i)S_{RSU_j}^{Ts} H(pID_i^1 \| pID_i^2 \| Ts), P) \cdot e(u_i, P)$$
$$= e(pID_i^1, S_{RSU_j}^{Ts} P) \cdot e(h(M_i)H(pID_i^1 \| pID_i^2 \| Ts), S_{RSU_j}^{Ts} P) \cdot e(u_i, P)$$
$$= e(pID_i^1, P_{RSU_j}^{Ts}) \cdot e(h(M_i)H(pID_i^1 \| pID_i^2 \| Ts), P_{RSU_j}^{Ts}) \cdot e(u_i, P)$$
$$= R.H.S$$

4.2 Resistance Impersonation attack:

According to $\delta_i = sK_i^1 + h(M_i)sK_i^2 + u_i$, the attacker ***Eve*** needs to know the key sK_i in order to generate a valid signature. The key is generated based on a temporary key that is valid in Ts. Since each message should be signed with this key, it can only be sent to the authenticated message along with the encrypted message, and the signature of the message contains a random number u_i, which improves the randomness of the signature. Therefore, forgery of signatures is not feasible.

4.3 Privacy-preserving:

The improved scheme implements conditional privacy-preserving in two aspects. First, each time the OBU joins the RSU group, it must obtain a temporary key valid in Ts of the RSU, and use its real identity information and the public parameters of the TA to generate a new pseudo identity. The attacker ***Eve*** cannot track because it moves between different RSUs.

Secondly, the temporary key will be encrypted by the symmetric secret key x shared between RSU_j and OBU_i. Then, RSU_j will generate a new pseudo identity and its associated private key of OBU_i, such as $sK_i^1 = S_{RSU_j}^{Ts} pID_i^1$.

Since messages are signed by different temporary private keys, no entity other than TA and RSU can establish signatures, pseudo-identities, and OBU_i's connections. Therefore, our proposed scheme satisfies the conditional privacy-preserving.

4.4 Traceability and revocability:

In special cases, TA can use the equation $pID_i^2 \oplus H(S_{RSU_j}^{Ts} pID_i^1) = RID_i$ to get the real identity of a malicious vehicle. The TA then adds the real identity of the malicious vehicle to the revocation list and sends the updated revocation list to all RSUs. Therefore, the cancelled vehicle cannot join the RSU group to obtain the temporary master key of the RSU and sign any message. So our solution meets traceability and revocability.

4.5 Resistance Man-in-the-Middle Attack:

To achieve a man-in-the-middle attack, the attacker Eve first needs to maintain a communication connection with both parties communicating with each other, and then both parties to each other believe in each other and implement information interaction in a secure connection in order to obtain useful information for the purpose of attack. In this scenario, the RSU and the OBU need to establish a link by selecting a random number in each communication. Since the random numbers used by Eve and RSU, Eve and OBU, and communication between RSU and OBU are completely different, attacker Eve cannot establish a communication connection with legitimate users through man-in-the-middle attacks to achieve the purpose of attack.

4.6 Resistance replay attack:

Replay attacks cannot be implemented after the attacker ***Eve*** intercepts any message. Because every time a message is received, it will be verified by Ts. Each time a message is signed and sent, a temporary key that is valid in Ts is used. After receiving the message, the receiver judges whether the temporary key expires based on the current time. Therefore, the attacker Eve is unable to perform replay attacks.

V. CONCLUSION:

In VANET, it is necessary to meet the transient characteristics of communication, so the efficiency of message signature, vehicle privacy protection and authentication is very important. In this paper, we have improved a new and efficient conditional privacy protection authentication scheme, and analyzed and improved the security vulnerability of the original scheme in terms of traceability, thus improving the security of the original scheme. However, we have also found that improved solutions inevitably increase the communication burden in order to improve security. In future research, we will conduct further research on improving the efficiency and security of the agreement.

ACKNOWLEDGMENT:

This work is supported by the Applied Basic and Advanced Technology Research Programs of Tianjin (No.15JCYBJC15900).

REFERENCES:

[1] L B Wu ,Y Xie , et al. EIAS: new efficient identity-based authentication scheme with conditional privacy-preserving for VANETs[J]. Telecommunication System, 2017, 65(2):229-240.

[2] C Gamage,B Gras, B Crispo, et al.An identity-based ring signature scheme with enhanced privacy[J].Secure communication Workshops, 2006, pp. 1–5.

[3] R Lu, X Lin, H Zhu,et al.ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications[J]. In The 27th conference on computer communications,2008.

[4] Hrong S J,Tzeng S F,Fan Y,et al. B-SPECS+: Batch verification for secure pseudonymous authentication in VANET[J]. IEEE Transactions on Information Forensics and Security,2013,p:1860-1875

[5] M Bayat, M Barmshoory, M Rahimi, et al. A secure authentication scheme for VANETs with batch verification[J]. Wireless Netwrrk,2015,21 (5):1733–1743.

[6] J Harding, G Powell, R Yoon, et al. Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application[J]. Technical Report, 2014.

[7] S Al-Sultan, M M Al-Doori, A H Al-Bayatti, et al. A comprehensive survey on vehicular ad hoc network[J]. Network Computer,2014,(37) :380–392.

[8] Y Liu, Y Wang, G Chang. Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm[J]. IEEE Transactions on Intelligent Transportation System, 2017,18(10):2740-2749.

[9] J Li, H Lu, M Guizani. ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for vanets[J]. IEEE Transactions on Parallel and Distributed Systems, 2015,26 (4): 938–948.

[10] F Wang, Y Xu, H Zhang, et al.2Flip: a two-factor lightweight privacy-preserving authentication scheme for vanet[J]. IEEE Transactions on Vehicular Technology, 2016,65(2):896–911.

[11] F Qu, Z Wu, F Y Wang, et al. A security and privacy review of VANETs[J]. IEEE Transactions on Intelligent Transportation Systems,2015,16 (6):2985–2996.

[12] Lin I C, Hwang M S, Li L H, et al. A new remote user Authentication scheme for multi-server architecture[J].Future Generation Computer System,2003,19(1):13-22.

[13] M Raya, J P Hubaux ,et al. Securing vehicular ad hoc networks[J].Computer Security,2007,15 (1) :39–68.

[14] J Huang, L Yeh, L Y, et al. ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks[J]. IEEE Transactions on Vehicular Technology, 2011,60(1):248–262.

[15] T W Chim, S M Yiu, L C Hui, et al. MLAS: multiple level authentication scheme for VANETs[J]. Ad Hoc Netwwork,2012,10 (7):1445–1456.

[16] H Xiong, K Beznosov, Z Qin, M Ripeanu, Efficient and spontaneous privacy-preserving protocol for secure vehicular communication, in: Communications (ICC), IEEE International Conference on, 2010, pp. 1–6.

[17] H Xiong, Z Chen, F Li, Efficient and multi-level privacy-preserving communication protocol for VANET, Compute Electronic. Eng. 38 (3), 2012, 573–581.

[18] Y Wang, H Zhong, Y Xu, J Cui, ECPB: efficient conditional privacy-preserving authentication scheme supporting batch verification for vanets, IJ Network Security. 18 (2), 2016, 374–382.

[19] J Shao, X Lin, R Lu, C Zuo, A threshold anonymous authentication protocol for VANETs, IEEE Trans. Vehicle Technology. 65 (3) , 2016, 1711–1720.

[20] S M Pournaghi, B Zahednejad, NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET.2018.

[21] J Li, H Lu, M Guizani, ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for vanets, IEEE Trans. Parallel Distribute. Syst. 26 (4) , 2015, 938–948.

[22] F Wang, Y Xu, H Zhang, Y Zhang, L Zhu, 2Flip: a two-factor lightweight privacy-preserving authentication scheme for vanet, IEEE Trans. Vehicle Technology. 65(2), 2016, 896–911.

[23] F Qu, Z Wu, F Y Wang, W Cho, A security and privacy review of VANETs, IEEE Trans. Intell. Transp . System. 16 (6),2015, 2985–2996.

[24] J Harding, G Powell, R Yoon, J Fikentscher, C Doyle, D Sade, M Lukuc, J. Simons, J Wang, Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application, Technical Report, 2014.

[25] S Al-Sultan, M M Al-Doori, A H Al-Bayatti, H Zedan, A comprehensive survey on vehicular ad hoc network, J. Network Computer. Appl. 37, 2014, 380–392.