J Comput Virol Hack Tech
DOI 10.1007/s11416-016-0269-z

SHORT CONTRIBUTION

A secure analysis of vehicular authentication security scheme of RSUs in VANET

Yongchan Kim[1] · **Jongkun Lee**[1]

Received: 10 September 2015 / Accepted: 4 February 2016

Abstract The Vehicular Ad-Hoc Network (VANET) is a network to provide communication between nearby V2V (Vehicular to vehicular) and V2I(Vehicular to Infrastructure). In order to increase the network efficiency, it is required to have stability of transmission and security of reliability. In this paper, we propose a novel Vehicular Authentication Security Scheme (VASS) guaranteeing secure RSUs (Roadside Units) to OBUs(On-Board Units) in VANET on the basis of the ID-based authentication scheme using hi-pass card (or highway pass ticket) and license plate number. We show a usefulness and effectiveness of VASS after analyzed by the Petri nets.

Keywords ID-based authentication · OBU · Petri nets · RSU · Security · VANET · VASS · Vehicle authentication

1 Introduction

In Vehicular Ad-Hoc Network(VANET)s, it includes the communication between vehicles and the communication with the Roadside Units (RSUs) installed in major regions. In particular, data such as vehicle location, current time, direction, speed, traffic volume remarks, acceleration and deceleration is distributed by On-Board Units (OBUs) in the VANET. According to such data, VANET plays the role of smoothly manipulating road traffic volume through traffic flow control, accident prevention countermeasures, solution for complicated traffic volume and announcement of alternate roads [1–11].

✉ Jongkun Lee
jkleecnu@gmail.com; jklee@cwnu.ac.kr

[1] Department of Computer Engineering, Changwon National University, Kyungnam, Korea

In the VANET, it is one of the important problems to authenticated vehicle successfully. Raya et al. [9] proposed an authenticated method using large numbers of anonymous public and private key pairs, but this work needs high computation cost and high storage cost. Lu et al. [10] introduced ECPP(Efficient Conditional Privacy Preservation) protocol for VANETs which has three levels of user privacy, to achieve authentication, anonymity, and untraceability. In ECPP, RSUs are responsible for issuing temporary public key certificates to vehicles. However, ECPP uses the signatures and public key certificates on each message resulting in high computation cost for verifying the message. Zhang et al. [11] proposed RAISE (RSU-aided messages authentication scheme) method using the symmetric key hash message authentication code (HMAC) to reduce the signature cost. In [8], PPAS(Privacy preservation authentication scheme) was proposed for V2I (Vehicular to Infrastructure) communication environments which has a lightweight authentication. As mentioned above [8–11], we found that designing a security and privacy preservation authentication scheme with low computation and authentication latency in VANET still remains as a major challenge.

This study focuses on the authentication problem on each vehicle in the communication between vehicles in the high way environment. In other words, definite authentication on vehicles in the communication occurred between vehicles not only prevents accidents but can also be used as basic data for post-accident responsibility matters. Especially, it is necessary to a mutually different ID(identity) in the communication between vehicles, the transmission/reception media should not be tampered, and confidentiality for the communication messages between entities be guaranteed. In order to show the safety efficiency on the security, a novel security mechanism has been proposed for VANET and is verified a usefulness and effectiveness by modeling the Petri Net.

Published online: 22 February 2016

Petri nets [12] as a graphical and mathematical tools, are a uniform environment for modeling, analysis, and control of complex systems. The modeling of Petri nets may detect flaws and errors in the security scheme design, and subsequently improve the correctness of the security protocol. We used Petri nets in the security analysis of the proposed scheme.

The remainder of the paper is organized as follows. Followed by the introduction of Sect. 1, Sect. 2 deals with the preliminaries and assumption for this works, Sect. 3 explains about Vehicular Authentication Security Scheme (VASS) proposed in this study. In Sect. 4, models with Petri Net, and through this, proposes how smoothly the mechanism that varies frequently according to the security purpose can be applied. Section 5 explains about future research assignments along with the conclusion of this study.

Fig. 2 Sample of the Highway ticket and card **a** express ticket **b** *hi-pass* card

2 Preliminaries and asumption

The communication in VANET is divided into three types as OBU2RSU(On-Board Unit to Roadside Unit) communication between OBU and RSU which is located in the road, OBU2OBU(On-Board Unit to On-Board Unit) communication between OBU and RSU2RSU communication [3]. Usually, these communication structures require an authentication process of each OBU and RSU in the network. This means that OBUs and RSUs are authenticated by trusted third party at the initialization of a VANET [6] (Fig. 1a). Also, this communication structure requires many communicated messages to keep the certification after identifying authentication.

For authentication it is necessary to have many communications with CA. If the secure scheme minimize the authentication activities, it is possible to reduce the communication volumes among RSU2RSU, RSU2OBU and OBU2OBU. To reduce the communication message to keep the authentication we consider two ideas, such as (1) used first RSU instead of CA, such as tollgate in highway, and (2) periodic authentication process in RSU (Fig. 1b).

When we get on highway, anyone should be passed a tollgate through a pass ticket (Fig. 2) or *hi-pass* card. With pre-registering any pass ticket or hi-pass card, we are able to figure out the entered time, gate number as well as sequence number. ID-based encryption system was proposed by Adi Shamir [13] using the difficulty of integer factoring [14]. The ID-based authentication system is an efficient scheme for a VANET which has not require to store, fetch and verify the public key with CA [14]. In this works, we used the pre-registered hi-pass card number and license plate number, as passed tollgate in highway (Fig. 2a, b).

For authentication OBU in VANET, we provide the following two leveled process for RSU-OBU communication: (1) Authentication of OBU as a valid member of the corre-

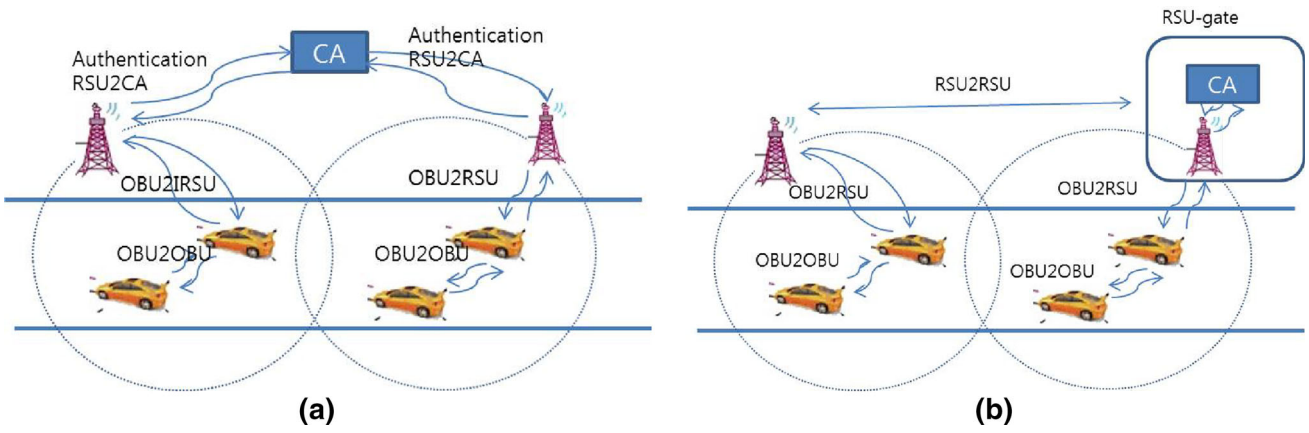

Fig. 1 VANET **a** General Environment **b** Proposed Environment

sponding RSU and (2) Delivering the message to the OBU signed by the RSU. This means that the first step is for a register step of OBU to RSU and the second one for an authentication step by period time to keep the authentication status. Based on these concepts, we show a relationship between RSU and OBU in Fig. 3.

3 Authentication (VASS)

The Vehicular Authentication Security Scheme (VASS) in highway proposed in this study includes the OBU authentication process of RSU coming into the group of itself and the periodic authentication process of the authenticated OBU in the OBU2RSU communication. After the first authentication, it is necessary that the OBU should be to prepare against security threat through periodic authentication processes by certain time periods.

OBU registers to first RSU when passed tollgate with OBU-ID (OBU number) and hi-pass card number. RSU checks the OBU-id and hi-pass card number for authentication. If the OBU registered number and ID are the same as the RSU checked ones, then send to ack message to OBU for authentication. However, but if those are different, then this OBU could not be authenticated,. Also, The TPD (Tamper Proof Device) in OBU stored unique OBU-id, Hi-pass card number, password. Table 1 denotes the notations used throughout in this paper.

In this section, we describe VASS(Vehicular Authentication Security Scheme) for V2I communication environment in VANET. The VASS has two main procedure include first authentication process and period authentication process:

3.1 First authentication process

For efficient authentication management of OBU, RSU sets OBU numbers to a certain level.

OBU delivers its ID to RSU as it goes into the RSU group. And, OBU decodes the ID, t and r by using the open keys of RSU which are only open to OBUs with normal IDs, and

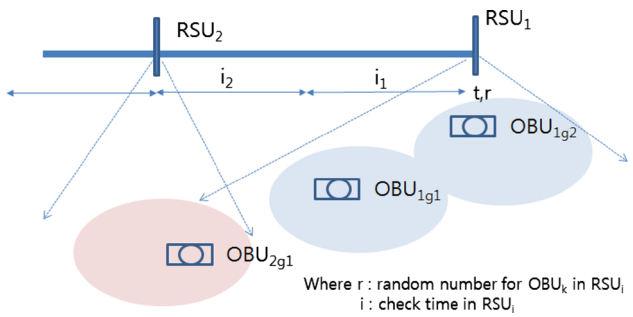

Fig. 3 Communication relationship between RSU and OBU

Table 1 Notations in this study

Notations	Descriptions
E	Encription
D	Decription
OBU_V	Vehicular number of OBU
$OBU_{Hi\text{-}pass}$	Hi-pass number of OBU
H	Hash function
t	Timestamp
r	Random number
i	Period time
RSUr	ID of RSU

sends them to RSU after encoding the values and their secret keys into RSU open keys. In this time, RSU releases the information obtained by OBU with its own secret key, and if the ID, t and r received at the initial registration, are the same, RSU will save the secret key of OBU and use it in the next periodic authentication stage (Fig. 4a, b).

The detailed process of first authentication is shown as follows:

1. RSU get OBU_v and $OBU_{hi-pass}$ and password and send to CA for verify
2. CA(in RSU) check OBU_v and $OBU_{hi-pass}$, if correct send ACK message to RSU
3. RSU create OBUid as follow:

   $$OBUid = OBUv||H(OBU_{hi\text{-}pass})||t(TIMESTAMP)$$

4. RSU make a RSUI based on RSU_R(RSU sequence number) and RSU_{locat}(location)

   $$RSUid = RSU_R||RSU_{locat}$$

5. RSU made $Aut_{OBUID} = (OBU_{ID}||\ H(r))$ and send to OBU for authentication

3.2 Periodic authentication process

In order to maintain the authentication from RSU, OBU must obtain a periodic certification from the RSU. For this issue, RSU must check the OBU's authentication in periodic time(i) after accepting the first authentication based on the first timestamp and hash function(r). Every periodic time, OBU must send TPD information such as ID, hi-pass number, and timestamp to RSU. However, if the values are difference, the regarding OBU should be removed from the RSU group since OBU is exposed to a security threat (Fig. 5a, b).

The detailed process of first authentication is shown as follows:

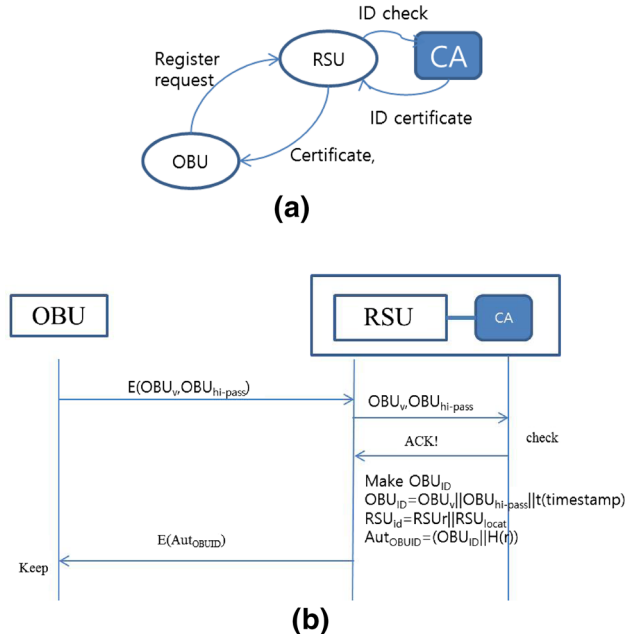

Fig. 4 The first authentication process **a** Automat of first authentication. **b** First authentication protocol

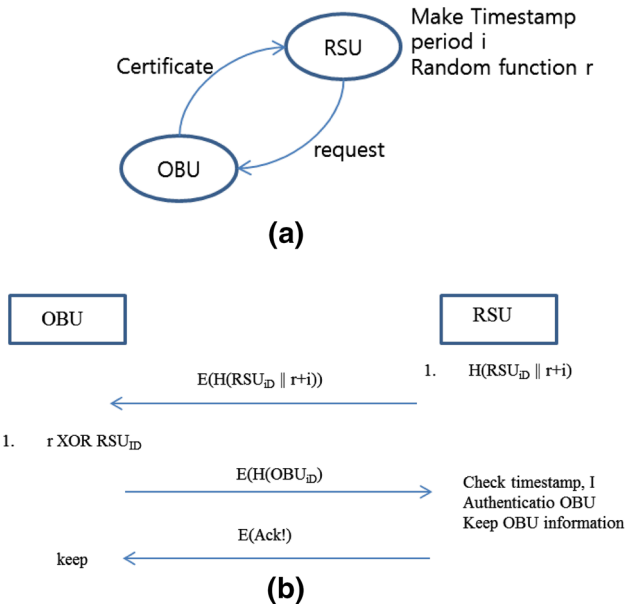

Fig. 5 The periodic authentication procedure **a** Automata of period authentication. **b** Period authentication process

1. RSU send a message to OBU after generated short random number r used hash function $H(RSU_{ID}||r+i)$
2. OBU received hash function r and generated r XOR RSU_{ID}, and send $H(OBU_{ID})$ to RSU
3. RSU checks the OBUID for authenticity. If OBU is a legitimate member then go to 4, else drop this OBU_{ID}.
4. OBU received $H(r(RSU_{ID}||r+i)$

4 Verification of proposed model used Petri nets

4.1 Verification

Petri nets have been widely used in various application domains for its simplicity and flexibility in depicting dynamic system behaviors. Their inherently asynchronous concurrent semantics matches that of many physical systems of interest. For example, they are very suitable to describe a network's architecture, services, and protocol. Petri nets have advantages in modelling, analysis, and verification because of their intuitive graphical representation and rigorous mathematical theory and their wealth of analytical techniques and tools [12,15,16].

From the previous section, we proposed VASS for OBU and RSU in VANET. In this time, we want to verify our mechanism used Petri Nets. According to the above VASS, the corresponding Petri conversion model was established in Fig. 6 and the list of places and transitions are shown in Table 2.

We used VisObjNet to analyze the model of VASS in IBM-PC with Windows 8.1 environment. We can found this proposed model satisfy the reachability and liveness. As shown in the above simulation result, it could be known that the OBU authentication process and the periodic OBU authentication process have been smoothly carried out at the initial entry of the vehicle OBU into the RSU group. Additionally, various problematic situations during the authentication process, such as security strength on the vehicle authentication in a vehicle Ad-Hoc network could be known through the igni-

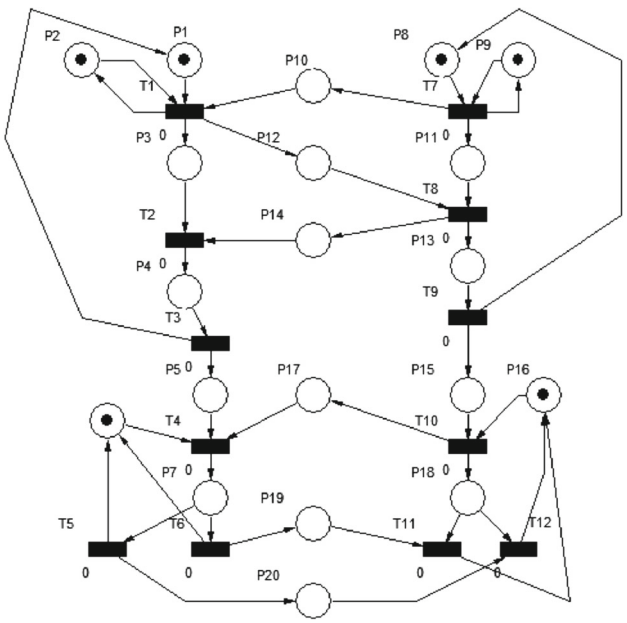

Fig. 6 Petri Net Model of VASS

Table 2 List of Places and Transitions in Petri model of VASS

Places	Notations
pl	Initial place of RSU
p2	Working place
p3	Waiting place
p4	Keep OBU information
P5	Waiting place
P6	Working place
P7	Verify OBU
P8	Initial place OBU
P9	Working place
P10	UnitNumber
P11	Waiting place
P12	ACK
P13	Waiting place
P14	RSU_pri(UnitNumber,t,r)
P15	Waiting place
P16	Working place for authentication
P17	OBU_pub(UnitNumber,t,r+i)
P18	Working place
P19	Verify-yes
P20	Verify-no
Transition	**Notations**
tl	Receive OBU UnitNumber
r2	Verify OBU UnitNumber
t3	Information of OBU
T4	Received duration information
T5	Verify information-no
T6	Verify information-yes
T7	Send UnitNumber of OBU
T8	Received RSU information
T9	Waiting time
T10	Send request duration authentication i
T11	Verify-yes
T12	Verify-no

tion status frequency of t4, t5, t7 and t10 those implemented the removal of OBU.

4.2 Analysis

In this section, we discuss the security analysis and computation overhead for the proposed mechanism.

4.2.1 Security analysis

This mechanism used ID-based cryptography based on the OBU ID number and Hi-pass card number and password.

Table 3 Computation overhead

	Registration	Authentication
PPAS[8]	n(3Ch)	$9Ch+2Cr+2C_{XOR}$
Ashritha [17]		$3Ch+2Cr+2C_{XOR}$
VASS		$2Ch+2Cr+C_{XOR}$

C_h cost of hash function, C_{XOR} Cost of executing XOR, C_r Cost of random number, n number of OBUs in the VANET [8]

In addition, since RSU with CA conforms the pre-registered Hi-pass number and password to OBU-ID and TPD, the mechanism could be safe from the privacy security issues. After authenticating the validity of the first OBU by RSU, the OBU will be verified periodically. This system guarantees the safety of the OBU authentication. The communication between OBU and RSU will be safe against Sybil attackers since RSU has recent time stamp.

4.2.2 Computation overhead

The computational overhead of VASS and comparative methods [8,17] is shown in Table 3.

The VASS, which is proposed mechanism, is one of the efficiencies in computation effort rather than other methods in hash function problem.

5 Conclusions

The vehicular authentication security scheme VASS in highway has been proposed in this paper using encoded algorithm and time random numbers for the mutual authentication used Petri Net. As such, Petri Net modeling enables to smoothly cope with defining and implementing security requests in VANET, complicated with many changes of vehicles. Performance results show that the computation effort is much lower than other methods in hash function and VASS has the properties of security such as privacy, authentication and Sybil attack. In future work, we will extend our scheme for vehicle to infrastructure communication based on reduce the cost and communication message volume.

Acknowledgments This research is financially supported by Changwon National Univ. in 2015-2016.

References

1. Zhang, C., Lin, X., Lu, R., Ho, P.H., Shen, X.: An efficient message authentication scheme for vehicular communications. IEEE Trans. Veh. Technol. **57**(6), 3357–3368 (2008)
2. Biswas, S., Tatchikou, R., Dion, F.: Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety. Proc. IEEE Commun. Mag. **44**(1), 74–82 (2006)

3. Sun, X., Lin, X., Ho, P.-H.: Secure Vehicular Communications Based on Group Signature and ID-based Signature Scheme. In: Proceedings of International Conference on Communications ICC 2007, pp. 1539–1545 (2007)
4. Li, C.-T., Hwang, M.-S., Chu, Y.-P.: A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. Comput. Commun. **31**, 2803–2814 (2008)
5. Eiza, M-H., Ni, Q.: A reachability-Based Routing Scheme for Vehicular Ad Hoc Networks, In: Proceedings of the 11th IEEE ICTSPCC, pp. 1578–1584 (2012)
6. Biswas, S., Misic, J.: Proxy Signature-based RSU Message Broadcasting in VANET. In: Proceedings of the 25th Biennial Symposium On Communication, pp. 5–9 (2010)
7. Hesham, A., A-Hanid, A., El-Nasr, M.A.: A Dynamic Key Distribution Protocol for PKI-based VANETs. In: Proceedings of the Wireless day, IFIP, pp. 1–3 (2011)
8. Chuang, M-C., Lee, J-F: PPAS: A Privacy Preservation Authentication Scheme for Vehicle-to-Infrastructure Communication Networks. In: Proceedings CECNet, pp. 1509–1512 (2011)
9. Raya, M., Hubaux, J.P.: Securing vehicular ad hoc networks. J. Comput. Secur. **15**(1), 39–68 (2007)
10. Lu, R., Lin, X., Zhu, H., Ho, P-H., Shen, X.: ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications. In: IEEE INFOCOM, pp. 1229–1237 (2008)
11. Zhang, C., Lin, X., Lu, R., Hp, P-H: RAISE: An Efficient RSU-Aided Message Authentication Scheme in Vehicular Communication Networks. In: IEEE ICC, pp. 1451–1457 (2008)
12. Peterson, J.L.: Petri Net Theory and the Modeling of Systems. Prentice-Hall, Englewood Cliffs (1981)
13. Shamir, A.: Identity Based Cryptosystems and Signature Schemes. In: CRYPTO 1984, pp. 47–53 (1984)
14. Biswas, S., Misic, J., Misic, V.: ID-Based Safety Message Authentication for Security and Trust in Vehicular Networks. In: 31th ICDCS 2011, pp. 323–331 (2011)
15. Murata, T.: Petri nets: properties, analysis and applications. Proc. IEEE **77**, 541–580 (1989)
16. Gniewek, L., Kluska, J.: Hardware implementation of fuzzy Petri net as a controller. J. IEEE Trans. Syst. Man. Cybern. Part B Cybern. **34**(3), 1315–1324 (2004)
17. Ashritha, M., Sridhar, C.S.: RSU Based Efficient Vehicle Authentication Mechanism for VANETs. In: IEEE ISCO 2015, pp. 1–5 (2015)