Indian Journal of Science and Technology, *Vol 8(S7), 443–447, April 2015*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Vehicular Authentication Security Mechanism Modelling using Petri Net

Youngchan Kim, Yoojin Song and Jongkun Lee*

Department of Computer Engineering, Changwon National University, Korea; jklee@changwon.ac.kr

Abstract

Vehicles in the Vehicular Ad-Hoc Network (VANET) environment have been studied gaining much attention and will also be studied actively in the future in order to seek mutual safety and convenience through communications based on network infrastructure. However, most parts of such studies seeking safety and convenience are entering upon a new phase confronting security problems. Therefore, this paper proposes a vehicle authentication security mechanism that should be put in the top priority for efficient and safe transmission of the communications between vehicles in a VANET environment and verifies this through the Petri Net modeling method. The Vehicular Authentication Security Mechanism(VASM) proposed in this paper, by modeling with the Petri Net along with the vehicle authentication function, is able to define, implement and smoothly deal with the security requests in VANET those are inevitably complicated due to numerous changes of vehicles.

Keywords: Modeling, Petri Nets, Security, VANET, Vehicle

1. Introduction

Vehicular Ad-Hoc Network (VANET) is receiving much attention for its application that improves driver safety via the communication between vehicles. Vehicles in the VANET environment are able to receive various services through network infrastructure, and the information is mutually exchanged through frequent communications. Thus, the matters of guaranteeing anonymity between vehicles along with vehicle authentication in order to safely transmit the transmitted and received data for driver safety, and how efficiently and safely composing security mechanism such as integrity, availability and non-repudiation blockade through authentication on messages are being actively studied recently. Thus, this paper proposes a security mechanism for vehicle authentication that should be put in the op priority for efficient and safe transmission of the communication between vehicles in a vehicular Ad-Hoc network and verification of this the Petri net[1,2] modeling method. This paper is structured in the following order. Followed by the introduction of Chapter 1, Chapter 2 deals with the communication between vehicles, Chapter 3 explains about Vehicular Authentication Security Mechanism (VASM) proposed in this study and models with Petri Net, and through this, proposes how smoothly the mechanism that varies frequently according to the security purpose can be applied. Chapter 4 explains about future research assignments along with the conclusion of this study.

2. Communication between Vehicles

VANET is a fixed network for road safety promotion, traffic volume management and information system propagation for drivers and pedestrians. As a communication related equipment, 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

*Author for correspondence

volume remarks, acceleration and deceleration is distributed by Onboard 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[3-6]. This study focuses on the authentication problem on each vehicle in the communication between vehicles. 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 in the communication between vehicles, the transmission/reception media should not be tampered, and confidentiality for the communication messages between entities be guaranteed. Thus, this study proposes a security mechanism for authentication in the communication between vehicles and verifies the efficiency of it.

3. Security Mechanism for Vehicle Authentication

Before the communication in the vehicular Ad-Hoc network is largely classified into two types according to the communication status of the concerning module. The communication between the vehicles through the OBU (On-Board Unit) mounted on each vehicle is called V2V (Vehicle-to-Vehicle), and the communication with the infrastructure through the RSU (Road-Side Unit) located in the OBU and the road is called V2I (Vehicle-to-Infrastructure)[3]. In the two communication methods, a difference lies according to the participation status of the infra communication participation. The communication in this paper is based on the V2I communication through RSU, as this paper proposes the vehicle authentication put into a certain group along with the authentication by time period to block the authenticated vehicles existing for a certain period of time in the group from illegal attack. The Vehicular Authentication Security Mechanism (VASM) 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 V2I communication. The reason for the necessity of the periodic authentication process of OBU is, because the OBU status authenticated for the first time may be exposed to illegal attacks due to some malicioushacking, the purpose is to prepare for such security threats through continuous authentication processes by certain time periods.

The following explains about the OBU authentication and the periodic authentication process through RSU (Figure 1).

Here, RSU uses an open key algorithm for the RSU authentication process and OBU uses a secret key algorithm:

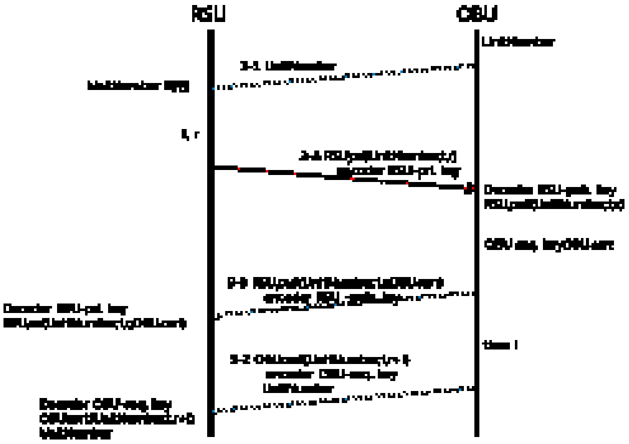


Figure 1. Security mechanism.

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

2 OBU delivers its Unit Number to RSU as it goes into the RSU group. RSU checks the Unit Number obtained by OBU from the list. If the Unit Number is normal, RSU generates a number t which has Time Stamp - the time information of the instant, and a random number r implying a certain time interval, and delivers to OBU after encoding them into RSU secret key along with OBU Unit Number.

3 OBU decodes the Unit Number, t and r by using the open keys of RSU those are only open to OBUs with normal Unit Numbers, and sends them to RSU after encoding the values and their secret keys into RSU open keys. Here, it can be known that RSU is not reliable if the decoded Unit Number value differs from their own value.

4 RSU releases the information obtained by OBU with its own secret key, and if it matches the Unit Number, t and r received at the initial registration, RSU saves the secret key of OBU and uses it in the next periodic authentication stage.

5 After a certain period of time, OBU encodes its Unit Number, the number t which has the initial starting Time Stamp and the number r+i which is the number after a certain time interval of i of the time interval randomly pre-set in each RSU group into its secret key and sends them to RSU along with the Unit Number of OBU.
6 RSU checks the Unit Number of OBU, decodes t, r+i and the Unit Number by using the regarding OBU secret keys, and it can be known that OBU has been operated within the group without being exposed to external attacks, if the initial starting time t of OBU matched the r+i value applied with the preliminarily set certain time interval.
7 Above 5 6 stages are repeated until OBU exits the group.
8 Lastly, if the values differ in the 2 4 6 stages, the regarding OBU is removed from the RSU group, as OBU is exposed to a security threat.

4. Verification of VANET used Petri Nets

In this time, the proposed VASM using Petri Net is as follows in Figure 2.
The number of tokens marked in P1 of Figure 2 defines the number of vehicles that can be managed by RSU. That is, if the regarding RSU is able to model by defining with the token numbers how much vehicle authentication can be managed, and the existence and removal of OBU can be known through the existence of this token as the token marked in P3 is for a single authentication of OBU. The following states about each role of the places and transitions in (Figure 2) are showed in Table 1.

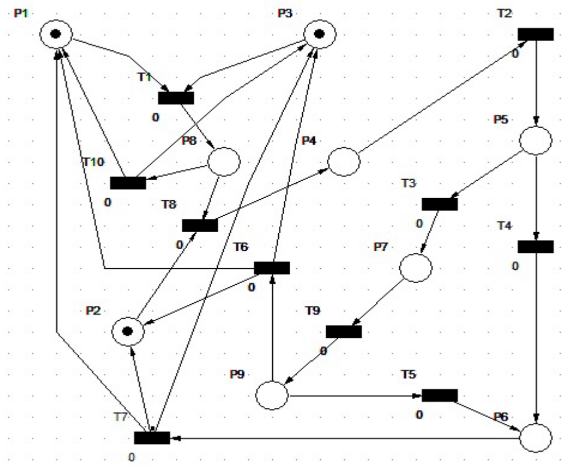
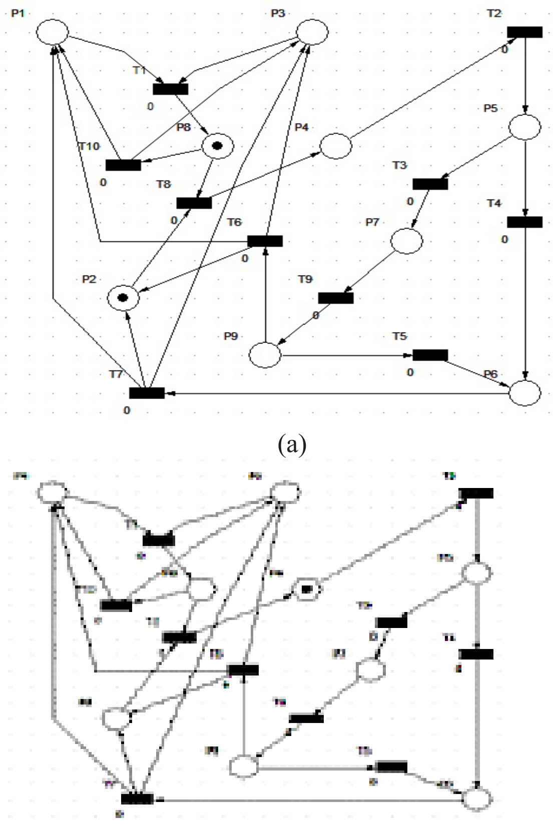


Figure 2. Initial petri net model of VASM.

Table 1. Content of place and transition of VASM petri Net model

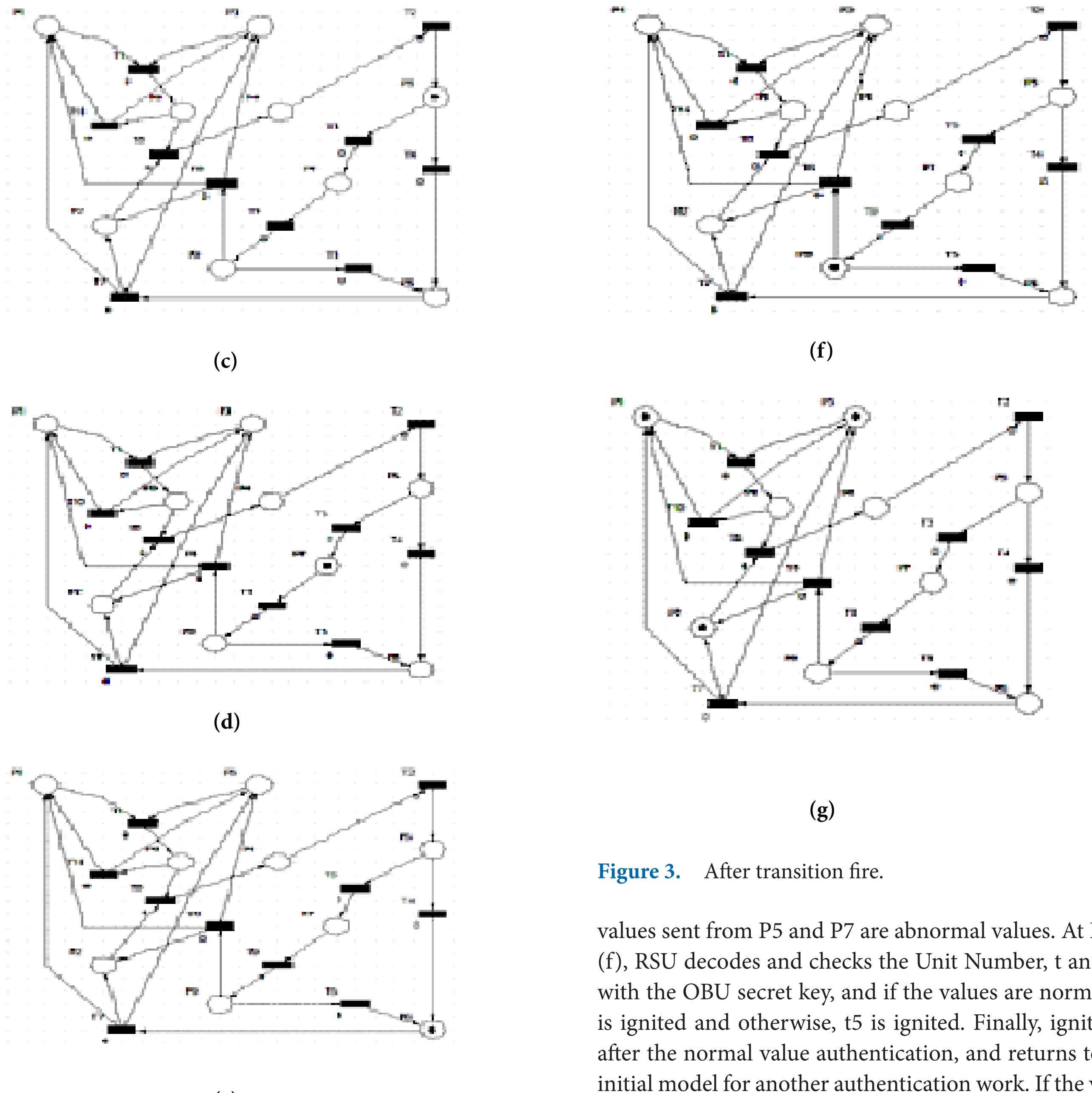
Place	Content	Transition	Content
		T1	OBU UnitNumber transmission to RSU
P1	RSU(Manageable OBU number setting)	T2	UnitNumber, t, and OBU secret key encoding with RSU open key
P2	RSU(t and r values creation)	T3	OBU authentication
P3	OBU(UnitNumber)	T4	OBU removal
P4	OBU(UnitNumber, t, r) OBU secret key	T5	OBU removal
P5	RSU(OBU secret key saving)	T6	OBU authentication
P6	RSU(OBU removal)	T7	OBU removal
P7	OBU(t, time interval value after a certain period of time r+i)	T8	UnitNumber, t and r encoding with RSU secret key and transmission to OBU.
P8	RSU(Check for normal status of OBU UnitNumber)	T9	OBU UnitNumber, t and r+i encoding with OBU secret key and transmission to RSU along with OBU UnitNumber,
P9	RSU(Check UnitNumber, t and r+i with OBU secret key))	T10	OBU removal

The simulation result simulated by the Petri Net simulation tool after modelling the proposed VASM with Petri Net is illustrated in stages in the following Figure 3.



(a)

(b)



(c)

(f)

(d)

(g)

(e)

Figure 3. After transition fire.

In (a), for P8, t8 is ignited if the OBU Unit Number is a normal value, and t10 is ignited if it is an abnormal value. In (b), at P4, OBU secret key and the encoded values of the Unit Number, t and r encoded with the RSU open key are sent. In (c), at P5, RSU decodes into its personal keys, and if the values are normal, it saves OBU secret key and ignites t3, and otherwise ignites t4. For P7 in (d), after a certain period of time, OBU encodes the Unit Nmber, t and r+i values into OBU secret keys and sends them to RSU. In (e), at P6, OBU is removed as the values sent from P5 and P7 are abnormal values. At P9 in (f), RSU decodes and checks the Unit Number, t and r+i with the OBU secret key, and if the values are normal, t6 is ignited and otherwise, t5 is ignited. Finally, ignites t6 after the normal value authentication, and returns to the initial model for another authentication work. If the value is abnormal, t7 and t10 are ignited, OBU is removed and returns to the initial model for another authentication work. 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 entery 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 ignition status frequency of t4, t5, t7 and t10 those implemented the removal of OBU.

5. Conclusion

The vehicular authentication security mechanism, VASM, in the V2I communication proposed in this paper uses encoded algorithm and time random numbers for the mutual authentication between RSU and OBU, and as the authentication of RUS is needed for the OBU side and the authentication of OBU that enters into the group of RSU is also necessary, for this, it has enabled all the mutual authentications by appropriately mixing and using the open key algorithm and encoded key algorithm. Additionally, thanks to the Petri Net modelling, the benefits lie on being able to appropriately simulate by marking the limited vehicle numbers of the RSU group with the number of tokens and measure the strength of security through the frequency of the transition ignition. As such, Petri Net modeling enables to smoothly cope with defining and implementing security requests in VANET, complicated with many changes of vehicles. In future studies, besides the authentication mechanism, it is necessary to propose a mechanism suitable for each of the environments, using Petri Net modeling by simulating and modeling after expanding the proposed mechanisms into many OBUs and defining the mechanisms on security requests such as message integrity and non-repudiation.

6. Acknowledgment

This work is financially supported by the ministry of education through the fostering project of University in Industrial Complexes and Changwon National University in 2014–2015.

7. References

1. Peterson JL. Petri Net theory and modeling of systems. Englewood Cliffs. NJ: Prentice Hall; 1981.
2. Murata T. Petri Nets: Properties, analysis and applications. Proceedings of IEEE. 1989; 77:541–80.
3. Zhang C, Lin X, Lu R, Ho PH, Shen X. An efficient message authentication scheme for vehicular communications. IEEE Transaction on Vehicular Technology. 2008 Nov; 57(6):3357–68.
4. Wang N-W et al. A novel secure communication schemd in vehicular ad hoc networks. Computer communication. 2008; 31:2827–37.
5. Sun X, Lin X, Ho P-H. Secure vehicular communications based on group signature and ID-based signature scheme. Proceedings on ICC 2007; 2007. p. 1539–45.
6. 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. Computer Communication. 2008; 31:2803–14.