International Journal of Electrical and Computer Engineering (IJECE)
Vol. 6, No. 1, February 2016, pp. 344~348
ISSN: 2088-8708, DOI: 10.11591/ijece.v6i1.8877

Proposed Potential Security Infrastructure in VANETS using Tamper Registered Hardware

Shaik Mahaboob Jani, Syed Umar
Dept of CSE, K L University, Guntur, AP, India

Article Info

Article history:

Received Aug 21, 2015
Revised Nov 2, 2015
Accepted Nov 17, 2015

Keyword:

Assymmetric
Cryptography
Symmetric
Tamper resistance hardware
VANETS

ABSTRACT

All over the world many road accidents are occurred due to lack of knowledge of vehicle`s distance and speed. But this issue will be solved by using VANETS through which we can well know about the speed of the vehicle and how much distance it is from other vehicles in all sides. So the VANETS will play a very crucial role in the safety and mostly avoidance of accidents like reacting immediately in dangerous situations. In order to prevent the abuse of VANETS a potential security infrastructure is needed to maintain confidential requirements like message integrity & availability. To achieve this we have proposed a concept called A separate Potential security infrastructure facilitated with symmetric & Asymmetric cryptography with TRH. Our proposed theory will give very high efficient in terms of Computational Needs for the VANETS users.

Corresponding Author:

Shaik Mahaboob Jani,
M.Tech Student, Dept of CSE, K L University,
Guntur, AP.
Email: lsntl@ccu.edu.tw

1. INTRODUCTION

In the Manets the Vehicular Adhoc networks is one of the part [1].These types of networks are mainly used and a network is formed in between the vehicles like cars, trucks bikes etc. Some factors like road course, traffic and it regulations will be restricted the movement of the node (Vehicle) because of these factors which will be a feasible imagination and approximation that the VANET will support some infrastructure which is fixed which can assist some services [2]. As it is often having of fixed infrastructure if the nodes are deployed in critical situations like service stations, dangerous intersections, some places like hazardous weather conditions. Generally nodes are supposed to communicate [3] to each other using radio signals which is a standard of IEEE 802.11p and multi hoping will be possible when they interact with other nodes [4]. The main concept of VANETS is to concentrate on road safety. Mainly to achieve road safety using sensors which contain information like speed of the vehicle location etc., which will enables driver alerting to avoid accidents and traffic jams etc.,. The authorized people like police and firefighter will send the signals to the vehicles before they are approaching so the vehicles can leave the space for the vehicle to move aside in the way [5] Generally we have three application categories **W, A, V** ie., **W**arnings, **A**larming & Alerting system, **V**alue Added services. The services of VANETS are shown in the below Figure 1

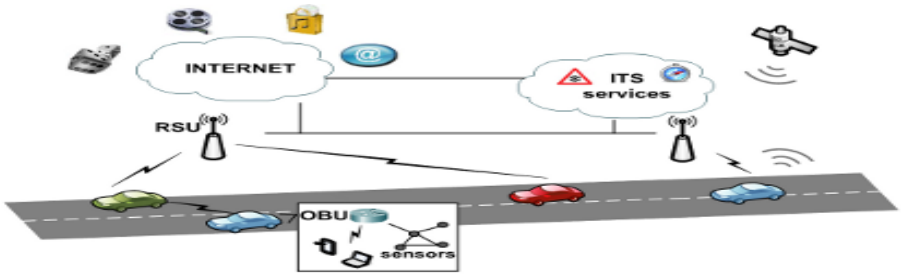

Figure 1. Services of VANETS

2. RELATED WORK

There are many applications using VANETS which can easily receive more and more information and easily communicate with one node to other node. Some funded projects like Network on Wheels [6], WillWarn [7] GST [8]. We are having various approaches one of them are as follows the sensed data will be used as PKI and digitally signs each message. In this each vehicle will have it own electronic license plate and it own chassis number which will be issued by the government and the related information will be stored in the server.

This license plate will have a private key and respective digital signature of the user which is stored in the TPD. To alter this anonymous key to use in the general operation we require three revocation methods [9] like RTPD so called as Revocation Tampered proof device, RCCRL Revocation compressed CRLs, DRP-Distributed Revocation Protocol.

In the [10] paper authors suggest that the advanced version of PKI is PKI+ as it includes elliptic curve cryptography, which can easily generate its own pseudonym certificates. For the PKI+ to explain this clearly it has five stages like

a. Setting the application of CA which creates its own private key and selects its own elliptic curve for the strengthen security
b. Setting of Vehicle using this the both private key and the master certification will be used by the user
c. Generation of Pseudonym used to link with CA but internally no use
d. Revelation of Pseudonym, in this CA uses the database and server and users master key and certificate to reveal the identity of the vehicle
e. Revocation of the Key in CA used to recomputes the private message or information and generated the public key.

In this we have some drawbacks with using of only PKI approaches, the VANETS have to participate in the trusted CA. If the CA is not trusted then the maximum information will be leaked to the hackers and the bandwidth usage will be enormous.

3. VANETS SECURING DATA & SATISFY ITS REQUIREMENTS

While we are studying about the VANETS we got major issues arise at the security requirements while sending or receiving data from one node to other. We already known that applications categories called W, A, V. The main requirements are shown in below table: 1

Requirements

Table. 1 W.A.V Security requirements

Abbr.	Security Requirement	W	A	V
I1	Data integrity	x	X	x
I2a	Immediate sender authentication		X	
I2b	Ex post accountability	x		x
C1	Different levels of confidentiality	x	X	x
C2	Protection of the security infrastructure	x	X	x
P1	Protection against profile generation	x	X	x
P2	Protection against surveillance	x	X	x
A1	Computational and bandwidth efficiency	x	(x)	X

4. PROPOSED SYSTEM

4.1 Proposal Theory for High Efficient Security

The infrastructure of the security of VANETS are designed and complied with very efficient computing and communications capabilities to maintain high confidential about the information. When the initialization finished then asymmetric cryptography will be employed with in the PKI to send the messages for the road security. This explains clearly in the below Figure 2.

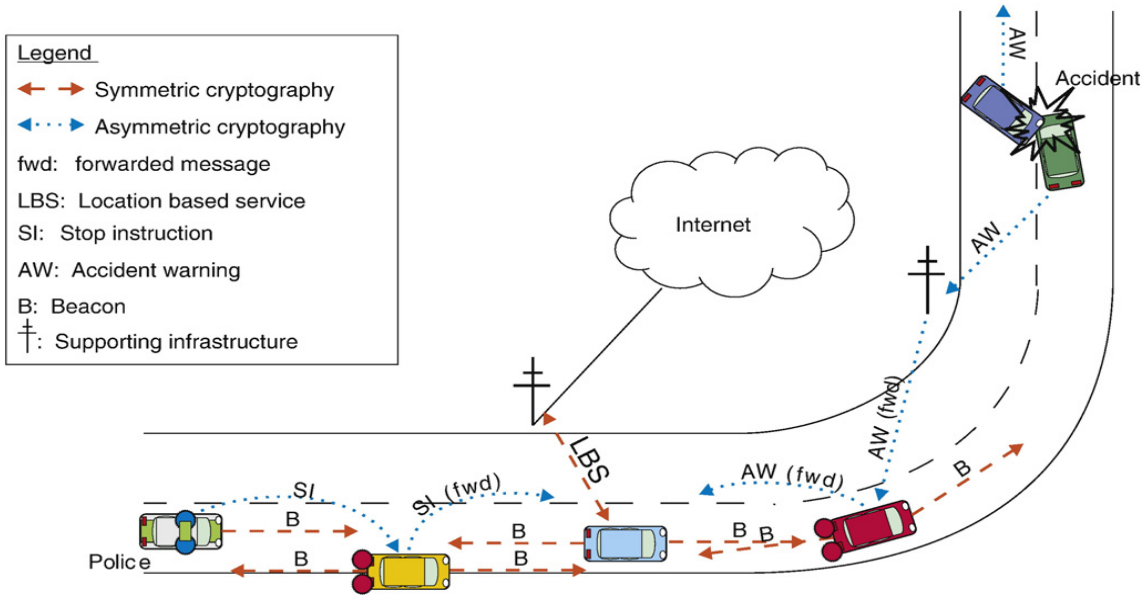

Figure 2. MANETS based VANETS send the messages from one node (vehicle) to other

In the above Figure 2 in the top right we can observe that accident occur between the two vehicle. Using the VANETS we can reduce this type of accidents by sending the alerting accidents like warnings to the other vehicles which sides to the one. By using the asymmetric cryptography an internal infrastructure will be created between the vehicle. By AW accident warnings will warn the vehicles near and sides and similarly if any registered vehicle like ambulance or police vehicles are entered in the network then from that a message called SI will be passed to all the vehicles nearby the way SI is nothing but Stop Instructions.

4.2 Analysis and Briefing of Asymmetric Participate

In VANETS we employ PKI as an asymmetric cryptography which have VRI in the form of private key and related CA which was operated by government of their country GTA. The VRI was suggested by the GTA to overcome the following reasons

a. To identify the owner of the vehicle generally user will have his own licensce plate which has a fixed pesudonym and this will be linked by the GTA people using VRI

b. The GTA was trusted by the citizens and it well known as government organization

c. The CA should be employed GTA which will more cost efficient because of the usage of the tachograph which will demand the CA issues [11]

The warnings integrity and authentication will be ensured by adding digital signature and CERT Sender which is shown in below Figure 3. The receiver who receives this will checks the digital signature & ID of the certificate.

Data with address information	Digital Signature	CERTSender

Figure 3. Message with Asymmetric protection

4.3 Initialization of the System

We are well familiar that at the production of the vehicles the TRH is equipped internally and we cannot remove it without destroying it , the manufacturer also install the CERT root certificate in which the preshared key used to encrypt the data between the TRH & smart card. While initialization of the system if there are no errors then there will be easy way to generate the TRH key pair (PK TRHA & SK TRHA) which are physically destroyed The VRI is then registered with the GTA in the normal registration process while registering vehicle at the local admission office. This means the local admission office can easily read PK TRH A and must check that key pair generation is deactivated. Then it saves VRI within the existing GTA registers and therefore is able to link VRI to owner identity. Then GTA issues a certificate (CERT TRH A) that is saved in vehicle's TRH. The initialization was shown in the below Figure 4.

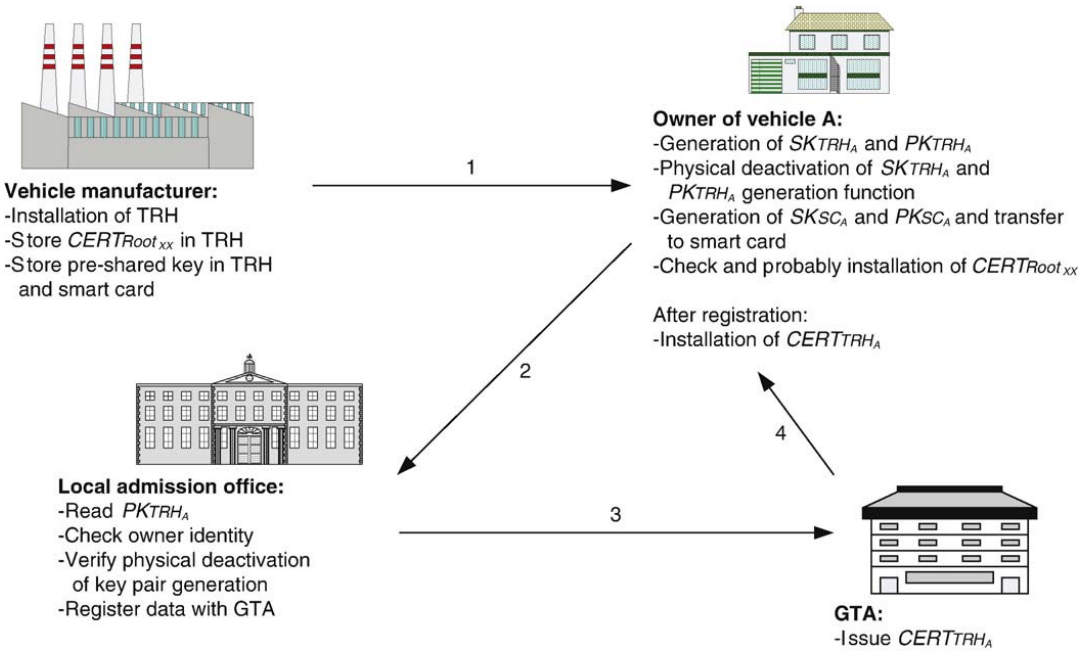

Figure 4. Initialization Process of the system

4.4 Symmetric Analysis of the Proposed System

We are well known that the value added services will be protected by means of symmetric cryptography. With the participation of node A uses the challenge response protocol and CERT TRH A used to authenticate with the local GTTP, as to increase the availability of GTTP must and should be nearer to the VANETS to communicate with other sources or devices like GSM etc., After authenticate itself with GTTP issues a pseudonym PA will be generated and associated symmetric key is k MAC PA is generated that is unique to the VRI for a certain period of time and stores the relation between VRI and PA. It also issues the symmetric keys k MAC ALL and k c. Many messages are assembled inside the TRH. First PA is added the data before it sent to the receiver. Then a message with authentication code MAC1 is computed with K MAC PA which is added and followed by MAC2 computed with K MAC ALL then the whole message will be encrypted like as shown below in Figure 5.

Data with address information	PA	MAC_1 with $KMAC_{PA}$	MAC_2 with $KMAC_{ALL}$

Ciphered with k_c

Figure 5. Message frame format of the Symmetric part

Computation times shown in Table 2.

Table 2. The Computational Periods of Symmetric and Asymmetric cryptography

	Asymmetric cryptography	Symmetric cryptography
Signature generation	98 ms	2 0.035 ms
Signature verification	2.9 ms	0.035 ms
Encryption	–	0.029 ms
Decryption	–	0.031 ms
Total	100.9 ms	0.165 ms

5. CONCLUSION

In this paper we made a proposed based on the infrastructure of the security using symmetric and asymmetric cryptography and TRH to satisfy required identities. While satisfying the requirements of our proposed concept will assure the high security to the VANETS and assures a good computational need. In this paper we explains how the communication done between the vehicles while any registered vehicles like Ambulance or police are entered in the way, by that signals then other normal vehicles will give a way to that registered vehicles. The future scope of this work changing of the pseudonym keys and symmetric keys to which consists of private and public keys. We can extend this work to define the geographic region of GTTP.

REFERENCES

[1] J. Munoz, N. Syracuse, Proc. of the 53. Internet engineering task force, 2002.
[2] M. Raya, J.P. Hubaux, *The security of vehicular ad hoc networks*, Proceedings of SASN 2005, ACM, 2005.
[3] IEEE, Dedicated Short Range Communication Standard (DSRC), http://grouper.ieee.org/groups/scc32/dsrc/namerica/.
[4] J. Tian, L. Coletti, *Routing approach in cartalk 2000 project*, Proceedings of the IST Mobile & Wireless Communications Summit 2003, vol. 2, 2003.
[5] K. Plößl, T. Nowey, C. Mletzko, *Towards a security architecture for vehicular ad hoc networks*, Proceedings of ARES 2006, IEEE Computer Society, 2006.
[6] M. Raya, J.P. Hubaux, *The security of vehicular ad hoc networks*, Proceedings of SASN 2005, ACM, 2005.
[7] M. Raya, P. Papadimitratos, J.P. Hubaux, Securing vehicular communications, *IEEE Wireless Communications, Special Issue on Inter Vehicular Communications*, 2006.
[8] M. Raya, J.P. Hubaux, Securing vehicular ad hoc networks, *Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks*, 2007.
[9] D. Jungels, I. Aad, M. Raya, J.P. Hubaux, *Certificate revocation in vehicular ad hoc networks*, Tech. Rep. LCA-Report-2006-006, EPFL, 2006.
[10] F. Armknecht, A. Festag, D. Westhoff, K. Zeng, Cross-layer privacy enhancement and non-repudiation in vehicular communication, 4h *Work- shop on Mobile Ad-Hoc Networks (WMAN)*, 2007.
[11] Council of the EU, Council Regulation (EC) No 2135/98, 1998.