ISSN No. 0976-5697

Volume 3, No. 1, Jan-Feb 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Advanced Encryption Method for VANET

Arun Malik*, Sanjeev Rana
Lecturer in Computer Science and Engg Deptt
Asian Institute of Technology,
Dhaurang, India.
arunmalikhisar@gmail.com

Abstract: Safety messaging is the most important aspect of VANET, where the passive safety (accident readiness) in vehicles was reinforced with the idea of active safety (accident prevention). Vehicular ad hoc networks (VANET) emerge as a contribution to the solution of providing safer and more efficient roads and to increase passenger safety. In this paper, the authentication methods in VANET are focused that provide security services. This paper also compares all the existing authentication methods which are designed for security of VANET and provides an advanced method that reduces delay, jitters and increases throughput and packet delivery ratio by removing attacks from the network.

Keywords: Authentication, Digital Certificates, Proxy Re-encryption, VANET

I. INTRODUCTION

With the proliferation of mobile devices (cell phones, Personal Digital Assistants (PDA), laptops, and other handheld digital devices), and the exponential growth in the wireless sector in the past decade, there is a revolutionary change in the way information is being handled [2]. Users carry mobile devices that run applications and provide network services, among which data services are the most demanded by users. Currently most of these connections between mobile devices are infrastructure based [2, 3]. For example, two or more laptops communicate with each other using a wireless access point; cell phones are connected via cell phone towers. Setting up infrastructure for mobile device communication is potentially costly.

Users will also face instances where the infrastructure required for desired communication is simply not available. Additionally many of the mobile devices in use like laptops and PDA’s have only short range wireless capability. This has prompted the development of an alternative way for mobile device communication in which each mobile device (node) communicates with each other over wireless without the support of an infrastructure, forming a mobile ad hoc network (MANET) [1,3].

To improve safety and traffic efficiency in vehicles, there has been significant research efforts by government, academia and industry to integrate computing and communication technologies into vehicles, which has resulted in the development of Intelligent Transportation Systems (ITS) [4].

Vehicular communication (VC) is an important component of ITS where vehicles communicate with other vehicles and/or road-side infrastructure, analyze and process received information, and makes decisions based on the analysis.

Such a network of self organized vehicles and road-side infrastructure communicating with each other over wireless, with a view to improve traffic safety and efficiency forms a VANET. It is envisioned that VANET will be deployed over the next decade, to achieve considerable market penetration around 2014 [5, 6].

Traffic congestion on the roads is today a large problem in big cities. The congestion and related vehicle accommodation problem is accompanied by a constant threat of accidents as well. Other negative consequences are related to energy waste and environmental pollution. Preliminary precautions like seat belts and airbags are used but they cannot eliminate problems due to driver’s inability to foresee the situation ahead of time. On a highway a vehicle cannot currently predict the speed of other vehicles. However, with use of sensor, computer and wireless communication equipment, speed could be predicted and a warning message sent every 0.5 seconds could limit the risk of potential accidents.

Wireless communication is ubiquitous because of its flexibility to adapt to different scenarios. Mobile Ad Hoc Networks (MANET) is a term coined for the continuously varying network topology handheld mobiles devices. Vehicular Ad Hoc Networks (VANET) is one of its types. The nodes or vehicles as in VANET can move around with no boundaries on their direction and speed. This arbitrary motion of vehicles poses new challenges to researchers in terms of designing a protocol set more specifically for VANET.

II. AUTHENTICATION PROCESS IN VANET

The scenario for VANET communication includes communicating entities of the service providers (SP), the cars, and the access points (AP) operated on behalf of service providers. The SPs and the APs can communicate with each other by some application-layer proprietary protocols via Internet. The APs are deployed along the roadside with reasonable wireless coverage to facilitate communication. A car typically belongs to one wireless network service provider, and communicates with the APs for accessing the internet along the road it travels through. When it travels, it also roams into wireless coverage that provide by other authorities.

In this design, the user authentication will be performed at the APs, i.e., the user will prove to the AP that it is a legitimate one. A more strict security will require the AP to prove it is a legitimate one as well, so to have mutual authentication. During the authentication, the two parties will negotiate a secret session key for the communication afterwards. The session keys could be established in a way that synchronizes the update at both the car and the AP so to allow location privacy countermeasures as reviewed in the previous section. The general authentication process is shown in Figure 1.

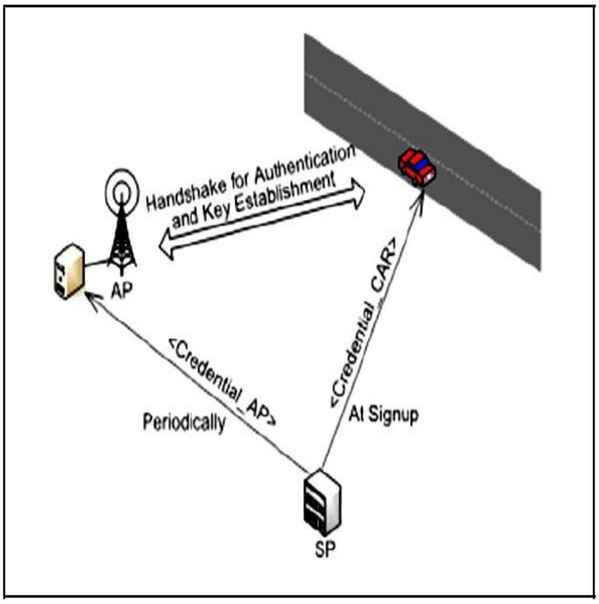

Figure 1 General Authentication Process in VANET

III. EXISTING METHODS FOR AUTHENTICATION IN VANET

There are three existing authentication methods for security:-

A. Authentication using Digital Certificate (DCA):

Earlier digital certificate are used to conduct the car-to-AP authentication. The SP partitions the service duration into time slots. When the car signs up at the SP, SP assigns a series of the car's public keys PK_{CAR} (ti) and their digital certificates $Cert_{CAR}$ (ti) to the car. Only one specific public key and digital certificate pair can be used in the corresponding time slot during subscription. For each time slot during the SP's service, the SP has a corresponding public key. The SP also sends its own time-related public keys *PKSP* (*ti*) to the car. The SP administrates a large number of distributed APs and monitors the behavior of them as shown in Figure 2. The SP distributes its time-related public keys to the APs periodically for the upcoming time slots [7]. The DCA Method is explained as follows:

a. ***Step 1:*** As shown in Figure 2, the authentication request is initiated by the car. According to its clock, it gets the time $t1$ and the corresponding public key $PK_{CAR}(t1)$ and certificate $Cert_{CAR}(t1)$ issued by SP. The car sends a message consisting of the three data fields <$t1$, $PK_{CAR}(t1)$, $Cert_{CAR}(t1)$ > to the AP.

b. ***Step 2:*** After the AP receives these messages, it checks $t1$. If it considers $t1$ unacceptable with regard to a deviation threshold, it can either simply disregard the request, or send a time-correction message to the car in order for it to have its clock adjusted.

c. ***Step 3:*** After the time adjusting, the car can initiate the authentication request again. If the time is validated, the AP tries to verify the certificate of the car's public key carried in the authentication request message by the SP's public key corresponding to $t1$.

d. ***Step 4:*** If the verification is successful, it randomly chooses a nonce $n1$ and generates a temporary public key *PKtemp*. After encrypting them by the PK_{CAR} ($t1$) provided in the request, the AP sends the message back to the car. The car can decrypt the message and get $n1$.

e. ***Step 5:*** After generating another nonce $n2$, it can send verification to the AP consisting $n1$, $n2$ and a success tag encrypted altogether using PK_{temp}. The AP can decrypt the message and get $n2$. Both parties can use some method E to generate session secret key from $n1$ and $n2$.

f. ***Step 6:*** The session key $E(n1, n2)$ is used for the data communication. The last verification message can be also piggybacked to the first data packet sent by the car. Hence authentication is successfully maintained.

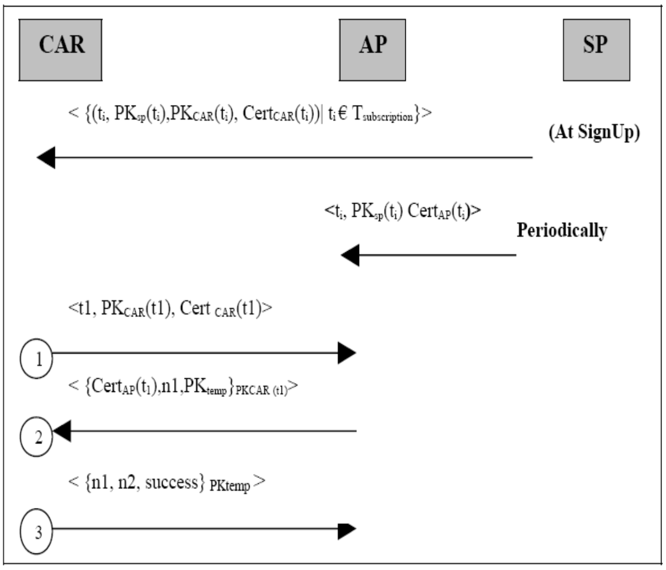
CAR
AP
SP
< {(ti, PKsp(ti),PKCAR(ti), CertCAR(ti))| ti€ Tsubscription}>
(At SignUp)
<ti, PKsp(ti) CertAP(ti)>
Periodically
<t1, PKCAR(t1), Cert CAR(t1)>
1
< {CertAP(t1),n1,PKtemp}PKCAR (t1)>
2
< {n1, n2, success} PKtemp >
3

Figure 2 Authentication using DCA

B. Authentication Using Pairing (PA):

Pairing mechanism can also be used for authentication between the car and the AP. The basic idea of pairing mechanism is that a security authority (SA) can issue pseudonym/secret point pairs based on a master secret as shown in Figure 3. Without the knowledge of the master secret, any two parties who possess a pseudonym/secret point pair can present pseudonyms to each other and a common secret key can be established [7]. The pairing method is explained as follows: -

a. ***Step 1:*** During sign-up stage, when the car subscribes service from the SP, a series of pseudonym/secret point pairs are assigned to the car, with each pair being used in a time slot of subscription. The number of pairs is determined by the subscription length. The APs also get these pseudonym and secret point pairs, but in a periodic way similar to that of DCA. The SP stops assigning these pairs to an AP if the AP's found misbehaving.

b. Step 2: The authentication message exchange still involves a three-way handshake. As shown in Figure 3, the car initiates an authentication by sending a request message to the AP: < $t1$, PN_{CAR} ($t1$) >. The message contains a timestamp $t1$ and the car's pseudonym PN_{CAR} ($t1$) bounded to that timestamp.

c. Step 3: If the time provided by the car is within normal deviation, the service provider picks one of its secret points corresponding to the time provided by the car and computes a shared secret key K; otherwise it can initiate time synchronization with the car as mentioned before.

d. Step 4: It then replies the car with a message containing the pseudonym just used to generate the secret key K: < PN_{AP} ($t1$) >. After the car receives the message, it can calculate the same secret key K based on the pseudonym provided by the AP.

e. Step 5: The car then encrypts a tag indicating successful authentication with the common secret key K and sends the message to the AP. After the AP confirms the message, the trust relationship between the car and the AP is established.

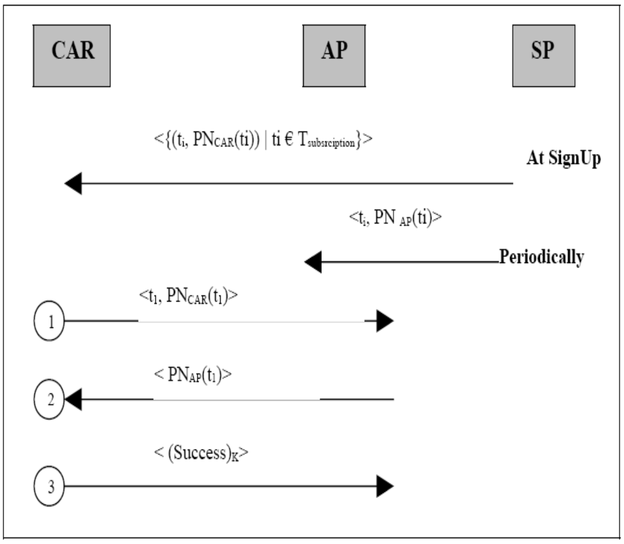

Figure 3 Authentication Using Pairing

C. Proxy Re-encryption (PRE) in Authentication:

Proxy re-encryption is a concept introduced by Blaze et al [8] in that allows a semi trusted entity called the "proxy" to convert cipher texts addressed to an entity B called the "delegators" to another entity C called the "delegate", while maintaining that the proxy cannot learn anything about the underlying plaintext, and C cannot learn anything about the underlying plaintext without co-operation from the proxy. B does this delegation by providing a special piece of information, called the "rekey", to the proxy as shown in Figure 4.

The basic concept of proxy re-encryption [9] says that, a cipher text for Alice that is encrypted by Alice's public key can be transformed by a proxy to a cipher text for Bob that can be decrypted by Bob's private key. The proxy however cannot read the cipher text. In this procedure, Alice delegates her decryption right to Bob. The key that the proxy uses to do the transformation is called re-encryption key $rk_{a \rightarrow b}$. The authentication process is depicted in Figure 4 and explained as follows:-

a. Step 1: The car sends an authentication request to the AP detected in its range. The request message just contains the time of request t and a random number n1: <t1, n1>.

b. Step 2: After the AP receives this message, it compares the time t1 provided by the car to its own clock. If the time is considered to be within normal deviation, the access point sends a message back to the car. The message constitutes a new random number n2 encrypted by the public key of the service provider of the time slot related to t1: < (n2) PK_{SP} (t1) >.

c. Step 3: After the car receives the reply, it uses the re-encryption key corresponding to t1 to re-encrypt the message. The outcome is thus available for it to decrypt using its own private key, and the n2 is revealed.

d. Step 4: It then takes n1 and n2, combines them by some cryptographic algorithm E known to both parties to generate E(n1, n2), and uses it as a symmetric key to encrypt a success tag as the authentication proof.

e. Step 5: The encrypted message is sent back to the AP separately, or the car can also choose to immediately start sending data packets, with the authentication proof piggy-backed to the first data packet.

f. Step 6: After the AP verifies the message by decrypting it using E(n1, n2), a secure and trusted connection is established. For the AP to show itself as authorized, it needs to answer a challenge just as it posts to the car. For this purpose the AP needs to get time-related re-encryption keys along with the SP's public keys from the SP in a periodic fashion.

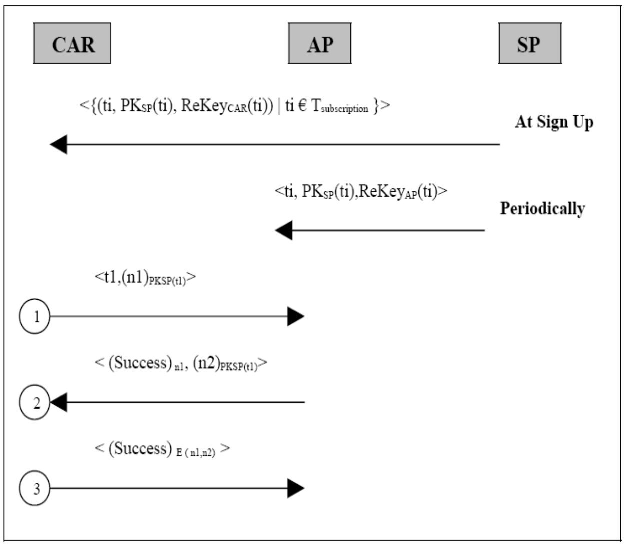
CAR
AP
SP
<{(ti, PK$_{SP}$(ti), ReKey$_{CAR}$(ti)) | ti € T$_{subscription}$ }>
At Sign Up
<ti, PK$_{SP}$(ti),ReKey$_{AP}$(ti)>
Periodically
<t1,(n1)$_{PKSP(t1)}$>
1
< (Success)$_{n1}$, (n2)$_{PKSP(t1)}$>
2
< (Success) $_{E(n1,n2)}$ >
3

Figure 4 Authentication using Proxy Re-encryption

Out of three authentication methods, in DCA and PA session keys are used during authentication process whereas PRE has the higher level of anonymity it achieves. In PRE, the cryptographic material (re-encryption key) is not included in any of the authentication messages exchanged. Instead, the car only uses the re-encryption key to respond to the challenge from the AP. So, that is why PRE method is preferred over DCA and PA methods of authentication.

But still, the existing methods have various possible common attacks and hence are not suitable for secure communication. The common attacks are:

i. Denial of Service (DoS) attack

ii. Eavesdropping
iii. Masquerade attack
iv. Key bootstrapping and rekeying
v. Tamper-proof device

The three methods can be compared based on the factors shown in Table 1.

Table 1. Comparison between authentication methods

	Encryption Technique	**Messages required for authentication**	**Point of compromise**
Digital Certificate	Asymmetric key	Large no of messages required for authentication	If a node knows the public key of the signing node.
Pairing	Symmetric key	Extra messages not required	If an attacker gets the secret key of communication
Proxy Re-encryption	Re-Encryption	AP to show itself as authorized	If re-encryption key is compromised

IV. ADVANCED ENCRYPTION METHOD FOR VANET

The advanced Proxy Re-encryption method comprises of all the features of earlier method – Proxy Re-encryption method with the addition of private key in it. The private key is known only to the AP and to the car. In this manner the message can be securely transmitted between vehicles after authentication.

The authentication process of Advanced Proxy Re-encryption method is shown in Figure 5:-

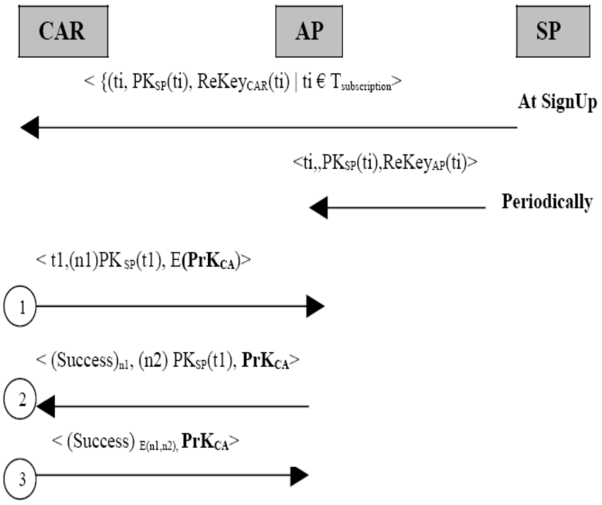
CAR
AP
SP
< {(ti, PKSP(ti), ReKeyCAR(ti) | ti € Tsubscription>
At SignUp
<ti,,PKSP(ti),ReKeyAP(ti)>
Periodically
< t1,(n1)PK SP(t1), E(PrKCA)>
1
< (Success)n1, (n2) PKSP(t1), PrKCA>
2
< (Success) E(n1,n2), PrKCA>
3

Figure 5 Authentication using Advanced Proxy Re-Encryption

ALGORITHM: Advanced Proxy Re-Encryption (APRE): -

Step 1: A pair of public and private key is assigned at sign up.
Step 2: The Car sends time slot t1 and nonce n1 and an encrypted private key <$\mathbf{PrK}_{ca}$> to the AP. Since this private key is also known to the AP, it will decrypt it and check with its own private key.
Step 3: After the two keys matches and the time t1 provided by the car comparable to its own clock, the AP sends a message back to the car. The message constitutes a new random number n2 encrypted by the public key of the service provider of the time slot corresponding to < t1, E($\mathbf{PrK}_{ca}$) > : < (n2) PK_{SP} (t1), $\mathbf{PrK}_{ca}$ >.
Step 4: After the car receives the reply, it uses the re-encryption key corresponding to t1 to re-encrypt the message. The outcome is thus available for it to decrypt using its own private key, and the n2 is revealed.
Step 5: It then takes n1 and n2, combines them by some cryptographic algorithm E known to both parties to generate E(n1, n2), and uses it as a symmetric key to encrypt a success tag as the authentication proof.

V. CONCLUSION

Vehicular ad hoc network (VANET) can offer various services and benefits to vehicular users and thus deserves deployment effort. In this paper, three authentication methods are discussed for VANET namely- authentication using digital certificate, authentication using pairing, and proxy re-encryption. The various aspects of Security and Privacy challenges in VANET are discussed. The authentication scheme- proxy re-encryption is reviewed which helps in reducing authentication overheads in rapid roaming networks with the use of public key assigned to the “delegate” and private key assigned to the “delegator”. Further, the advanced proxy re-encryption scheme is presented in which the private key is maintained between car and AP, so as to get better result for authenticity and privacy in rapidly changing networks.

VI. REFERENCES

[1] Lidong Zhou and Zygmunt J. Haas. “Securing Ad Hoc Networks”. IEEE Network Magazine, 13:24–30, 1999.

[2] Imrich Chlamtac, Marco Conti, and Jennifer J Liu. “Mobile Ad Hoc Networking: Imperatives and Challenges”. Ad Hoc Networks Ad Hoc Networking book contents, volume1 (1): pages:13–64, Jul 2003.

[3] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, and Piet Demeester. “An Overview of Mobile Ad Hoc Networks: Applications and Challenges”. The Communications Network, 3(3), 2004.

[4] Y. Qian and N. Moayeri. “Design of Secure and Application-Oriented VANETs”. In Vehicular Technology Conference, pages 2794–2799. VTC Spring 2008, IEEE, 2008.

[5] P. Samuel. Of Sticker Tags and 5.9 GHz. In ITS International, 2004.

[6] K. Matheus, R. Morich, I. Paulus, C. Menig, A. Lübke, B. Rech, and W. Specks. “Car- to-Car Communication-Market Introduction and Success Factors”. In ITS 2005: 5th European Congress and Exhibition on Intelligent Transport Systems and Services, Jun 2005.

[7] Jun Liu, Xiaoyan Hong, Qunwei Zheng, Lei Tang: Privacy-Preserving Quick Authentication in Fast Roaming Networks**.** LCN 2006: 975-982.

[8] M. Blaze, G. Bleumer, and M. Strauss. “Divertible protocols and atomic proxy cryptography”. In *Eurocrypt’98, LNCS 1403*, 1998.

[9] G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. *ACMTrans. Inf. Syst. Secur.*, 9(1):1–30, 2006.