International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Improved Secure Authentication Mechanism for Vehicular Ad Hoc Networks

Asmitha shree R[1], Ms. J. Arunanto[2]
Dept of Computer Science and engineering, Sri Krishna College Of and Technology, Coimbatore, India

Abstract: ***The security issues of vehicular ad hoc networks (VANETs) has been receiving a significant amount attention in the field of wireless mobile networking .Security is an important concern area for vehicular network application. Many authentication schemes based on asymmetric cryptography have been proposed for security but not very suitable for highly dynamic environment of VANET which cannot provide efficient authentication mechanism. Hence to provide efficient authentication scheme for dynamic environment, proposed a decentralized light weight authentication scheme named as TRUST WORTHY SECURITY AUTHENTICATION MECHANISIM FOR VEHICULAR AD HOC NETWORK for communication between vehicle to vehicle (V2V) done through wireless communication. To reduce the storage cost and to make the communication light and faster, the concept of trust relation which increases the performance of authentication procedure is introduced. Security requirements such as mutual authentication, modification attack resistance, replay attack resistance, Man-in-the-middle attack resistance and session key agreement are considered.***

Keywords: Vehicular ad hoc network (VANET), authentication, trust worthy.

I. INTRODUCTOIN

An ad-hoc network is a local area network (LAN) that is built spontaneously as devices connect. Ad hoc network is an autonomous system node connected with Wireless link. Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual nodes in the network forward packets to and from each other. Ad hoc structure does not require an access point to connect with other nodes, it is easy to setup, especially in a small or temporary network. Each node in the network forwards the packet without the need of central administration. In ad hoc network, node acts as a router to send and receive the data.

A. Vehicular Ad Hoc Network (Vanet)

Vehicular Ad hoc Network (VANET), a subclass of mobile ad hoc networks (MANETs), is a promising approach for the intelligent transportation system (ITS). Vehicular Ad-Hoc Networks (VANETs) make it possible for vehicles to broadcast warnings messages. The important step for the vehicle to be registered with some central authority (CA) so that nodes caught sending erroneous and malicious messages can be determined and held accountable. Authentication is initial step of security so very important for any communication to start sending information to other vehicles , only authenticated vehicles can make valid messenger and that messages are received and valid only by the another authenticated user. Authentication increase privacy concern surrounds information privacy and communication privacy. Authentication can increase the secure communication between authenticated vehicles from attacks by mistrustful vehicles.

VANETs are made up of vehicles (which are equipped with on board units) and road-side infrastructure units (RSUs). The on board units (OBUs) have on-board sensors inside car with wireless communication modules for communication. The RSUs are fixed entities and the vehicles are the moving entities.

II. RELATED WORK

Authentication in VANETs a (Public Key Infrastructure) PKI system, users communicate securely through use of a public-private key pair. The public key is known and the private key is secured. The public and private keys are mathematically calculated and linked. Law executor is the trusted authority in the network, and is responsible for handing out the initial authoritative information. Authenticity requires that an identity is assigned to a vehicle in order to verify the source of a message and protect the vehicle from any malicious use. Vehicles have a large number of anonymous public and private key pairs, as well as the corresponding public key certificates. Each of the public key certificates contains a pseudoidentity. Then, traffic messages are signed with a public key-Infrastructure scheme, and each pair of public and private key has a short lifetime to preserve its privacy. However, PKI based approach works with high computation cost, high storage cost, and high communication overhead.

The cryptographic used to enhance the location privacy, and provided location privacy by utilizing the group navigation of vehicles. PKI approaches do not work well in highly dynamic environments like VANETs because they use asymmetric cryptography or a digital signature scheme for verification, which have drawbacks like high computation costs, long authentication latency and results in large storage space. Public key infrastructure-based message signature used to reduce the signature cost but maintain the table for ID-key, resulting in more storage cost. Hence, there is still a need for an efficient authentication scheme for VANETs with low computation and low storage costs. So new authentication must introduced overcoming all drawbacks in VANET's authentication.

A. Security Requirements

Since the authentication scheme is susceptible to many malicious attacks, the main objective is to design an authentication scheme that is robust to malicious attacks. Thus the following key security requirements for VANETs.

1) *Efficiency:* The computational cost of vehicles must be as low as possible in order to have a real-time response in order to increase the efficiency of authentication scheme.
2) *Anonymity:* In VANET's anonymous authentication steps verifies that an OBU does not use its real identity to execute the authentication procedure for verification.
3) *Location Privacy:* Vehicle nodes collects the serial authentication messages of the OBU for security reasons but fails to track the location of the vehicle.
4) *Mutual Authentication:* A mutual authentication procedure is implemented. The LE must verify that the OBU is a legal user and the OBU in turn ensure that the LE is trustful.
5) *Integrity:* The authentication message integrity means that data cannot be modified.

III. PRPOSED WORK

A. Design Of Vanet Communication

Communication in VANET provides the V2I and V2V authentication mechanisms to protect trustful users. However, the design for an efficient V2V communication the authentication mechanism is more challenge than that for V2I authentication mechanism in VANETs because the vehicle cannot be authenticated via the infrastructure directly in V2V communications. Therefore, focus on V2V network environments and propose an efficient authentication scheme.V2I communication with have long range communication are partially infrastructure, road side unit is connected to the OBU unit present inside the vehicles so the form VEHICLES TO INFRASTUCTURE (V2I) authentication. When considering V2V communication is between vehicles. V2V communication is highly dynamic environment. Authentication is done between two vehicles for secure V2V communication.

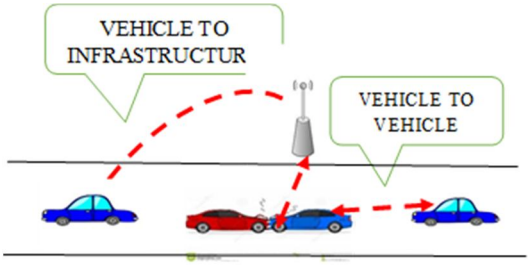

Fig 1.1 VANET COMMUNICATION

B. Registartion Procedure

1) *LE Registration:* The LE performs the LE registration procedure with the AS through the manufacturer or a secure channel. The AS computes the secure key set (Private secure key){PSKi, i = 1, . . . , n} based on the hash-chain method (e.g., h2(x) = h(h(x))) and sends this key set to the LE. secure key set that is stored in the security hardware and it does not need to store any authentication information of the user. Moreover, each PSKi has a short lifetime for robust security. Therefore, each trustful vehicle performs the key update procedure with the LE when the key lifetime is going to end. We can see that the new PSK (e.g., PSK2) cannot be inferred from the old PSK (e.g., PSK1) since the key generation scheme has a one-way feature of the hash function **Normal vehicle registration:** Other vehicles need to perform the normal vehicle registration procedure with the AS through the manufacturer or a secure behavior when the vehicle left the car factory. This initial registration procedure is only performed once. Each and every car provided with its own id and password to proceed with the login procedure whenever

it needed to start the communication. Vehicles needed to be authenticated. In addition, the registered user cannot impersonate to another valid user successfully when the user obtain the above parameters. This is because the user does not know the AS's secret key to be shared.

a) *Step 1)* Useri → AS: A user sends the public identification IDi and his chosen password PW*i* to the AS via the manufacturer or a secure channel.

b) *Step 2)* After receiving the user's ID and password, the AS computes the folloing secret authentication parameters for the user: $Ai = h(IDi||x)$, $Bi = h2(IDi||x) = h(Ai)$, $Ci = h(PWi) \oplus Bi$, and $Di = PSK \oplus Ai$. The objective of *Ai* is to build the relation between the user's ID and AS. Moreover, the objective of *Ci* is to build the relation among user's password, ID, and AS. Therefore, the user only keys in the correct personal information (i.e., ID*i* and PW*i*) in the login procedure. Otherwise, the OBU*i* rejects this login request.

c) *Step 3)* AS→ Useri: The AS stores the parameters (i.e., ID*i*, *Bi*, *Ci*, *Di*, *h*( )) in the OBU's security hardware via the manufacturer or a secure channel.

Note that the AS does not need to store the user's verification information (e.g., the user's password). Therefore, an adversary cannot obtain the information to launch a stolen verified attack.

In addition, the registered user cannot impersonate to another valid user successfully when the user obtains the above parameters. This is because the user does not know the AS's secret key named 'x'.

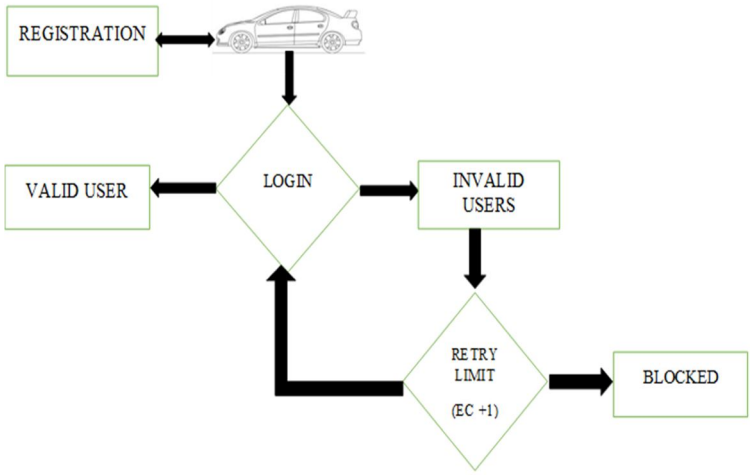

Fig 1.2 REGISTRATION

C. *Login Procedure*

The login procedure is the initial step. The OBU unit is fixed inside the vehicle it is a hardware device and with help of OBU the user can get authentication request to the authentication server (AS) or Law executor (LE). The OBU will detect an error event immediately if the user has malicious intentions. The user gives ID and password to authentication server as initial step if the user is valid then the user allowed to enter general authentication if the user already not registered then if he provide invalid ID or password then the user is blocked initially again if the user tries to enter then the request is rejected. The login procedure is the first checkpoint. The OBU will detect an error event immediately if the user has malicious intentions. The steps of the login procedure are listed.

1) *Useri→OBUi:* When a user wants to access the service, he/she inputs ID*i* and *PWi* to the OBUi.

2) The OBUi checks the ID*i* and verifies whether h(PWi) ⊕ Ci is equal to *Bi*, where *Bi* and *Ci* are obtained from the initial registration procedure. If the information is correct, the OBUi performs the general authentication procedure. **h(PWi) ⊕ Ci** has to be equal to *Bi*. If the values are not equal then the user inputs the wrong ID*i* or PW*i*, resulting in the login request will be rejected.

D. *Key Revocation Procedure*

The mechanism of key revocation is based on timer which treats as the lifetime of the key. The authentication state of a mistrust vehicle becomes trustfully and obtains an authorized parameter (i.e., *PSK*) when the vehicle performs the authentication procedure

successfully. Then, the authentication state in the hello message is changed to trust and the secure hardware sets up a timer to count down. When the lifetime of the key is over, the state of the vehicle is changed to mistrust. Certainly, our scheme is easy to integrate with other key revocation schemes (e.g., token-based mechanism). In fact, the system can ask the trustful vehicle to perform the key update procedure on the hour (or several hours) for reducing the compromised probability. The key update procedure is performed when the key lifetime of the TV will terminate. The TV extends its state of trustfulness after it finishes the key update procedure.

E. General Authentication Method

The OBU performs the general authentication procedure after the user completes the login procedure. Note that the OBU never uses the real identity of the user to perform the authentication procedure so nobody can obtain the user's real identity (i.e., ID*i*) via the intercepted

message. The OBU generates a random number $N1$ and calculates the message $M1$ as $h(Bi) \oplus N1$ then it computes with alias entity of the user identity and generate M2. The OBU sends an authentication request to the LE. The LE returns the authentication reply message) to the OBU. In this time, this OBU becomes trustful and obtains an authorized parameter when it is authenticated successfully. Thus, the other mistrustful OBUs can be authenticated by it without necessarily finding an LE.

Trust-worthy Authentication Procedure based on the concept of transitive trust relationships to improve the performance of the authentication procedure. The state of a mistrustful OBU becomes trustful and then obtains an authorized parameter (i.e., PSK) when the OBU is authenticated successfully. Then, the trustful OBU plays the role of LE temporarily to assist with the authentication procedure of a mistrustful OBU. In this procedure, the trustful vehicle performs the authentication procedure and works as an LE. Note that it still does not need to store the authentication information of the user. Hence, our scheme only has a few storage spaces. Then, the steps of the general authentication and the trust extended authentication procedures are the same. As a result, all vehicles in a VANET can complete the authentication procedure quickly.

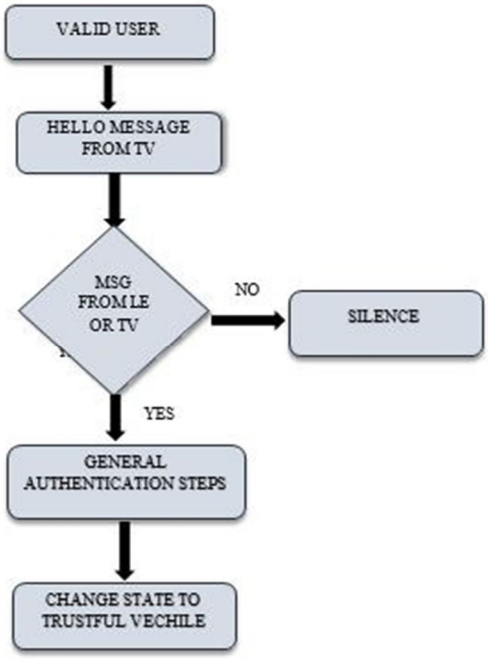

Fig 1.2 Malicious vehicle

F. Password Changing

The password change procedure is optional, to provide high security .The procedure is invoked when a user wants to change his password. It can be completed without any assistance from the AS since the security hardware of the OBU stores the parameters. The user provided with ID and password if need to change the password hashing and XOR operation are performed and the password gets updated. The new password is also updated in the Authentication server (AS) for further authentication to be proceeded.

Table 1 NOTATIONS

Symbols	Description
X	Secret key protected by AS
PSK	Secured key preshared between AS and LE
⊕	Xor operator
Idi	Public identification of entity
PWi	Password of entity
‖	Combination of strings

IV. CONCLUSION

The security of vehicular ad hoc networks plays a vital role in protecting the valid users. Authentication provides core stone service by protecting the user at initial step. Hence efficient authentication named DECENTRALIZED LIGHT WEIGHT AUTHENTICATION scheme protects valid user in VANETs from malicious attack. Based on trust relation concept authentication in dynamic environment is improved and provides less storage space. REGISTARTION PROCEDURE is implemented which makes the vehicle to register initially with authentication server. The valid users are checked at the login phase. Hence security provided from initial step. In future the other modules are implemented to improve the authentication procedure and extend the security by adding intrusion detection technique.

REFERENCES

[1] J.-F. Lee, C.-S. Wang, and M.-C. Chuang, “Fast and reliable emergency message dissemination mechanism in vehicular ad hoc networks,” in Proc. IEEE Wireless Commun. Netw. Conf., Apr. 2010, pp. 1–6. M. Raya and J. P. Hubaux, “Securing vehicular ad hoc networks,” J. Comput. Security, vol. 15, no. 1, pp. 39–68, 2007.
[2] M. Nekovee and B. B. Bogason, “Reliable and efficient information dissemination in intermittently connected vehicular ad hoc networks,” in Proc. IEEE Vehicular Technol. Conf., Apr. 2007, pp. 2486–2490.
[3] Dedicated Short Range Communications (DSRC) [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html
[4] M. Nekovee and B. B. Bogason, “Reliable and efficient information dissemination in intermittently connected vehicular ad hoc networks,” in Proc. IEEE Vehicular Technol. Conf., Apr. 2007, pp. 2486–2490.
[5] M. Raya and J. P. Hubaux, “Securing vehicular ad hoc networks,” J. Comput. Security, vol. 15, no. 1, pp. 39–68, 2007.
[6] J. Freudiger, M. Raya, and M. Feleghhazi, “Mix zones for location privacy in vehicular networks,” in Proc. First Int. Workshop Wireless Netw. Intell. Transp. Syst., Aug. 2007, pp. 1–7.
[7] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, “AMOEBA: Robust location privacy scheme for VANET,” IEEE J. Selected Areas Commun., vol. 25, no. 8, pp. 1569–1589, Oct. 2007.
[8] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, “RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks,” in Proc. IEEE Int. Conf. Commun., May 2008, pp. 1451–1457.
[9] M.-C. Chuang and J.-F. Lee, “TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks,” in Proc. IEEE Int. Conf. Consumer Electron., Commun. Netw., Apr. 2011, pp. 1758–1761.
[10] K. Sampigethava, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, “CARAVAN: Providing location privacy for vANET,” in Proc. ACM VANET, Sep. 2006, pp. 1–15.
[11] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, “An efficient identitybased batch verification scheme for vehicular sensor networks,” in Proc. IEEE INFOCOM, Apr. 2008, pp. 246–250.
[12] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, “ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications,” in Proc. IEEE INFOCOM, Apr. 2008, pp. 1229–1237.
[13] H. Zhu, R. Lu, X. Shen, and X. Lin, “Security in service-oriented vehicular networks,” IEEE Wireless Commun., vol. 16, no. 4, pp. 16–22, Aug. 2009
[14] C.-C. Lee, T.-H. Lin, and R.-X. Chang, “A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards,” Expert Syst. Appl., vol. 38, pp. 13863–13870, Oct. 2011.
[15] T. H. Chen, H. C. Hsiang, and W. K. Shih, “Security enhancement on an improvement on two remote user authentication schemes using smart cards,” Future Generation Comput. Syst., vol. 27, pp. 377–380, Apr. 2011.
[16] X. Li, Y. Xiong, J. Ma, and W. Wang, “An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards,” J. Netw. Comput. Appl., vol. 35, pp. 763–769, Mar. 2012.