An Intelligent Traffic System with the help of a secure VANET

[1]Deepu Mathew, [2]Hia Anns Roy,
[1]M.tech,Student, [2]Asst.Professor Computer science
[1]Computer Science,
[1]SJCET Palai, Kottaym, India

Abstract : A vehicular ad hoc network(VANET) system used in modern transportation system that improves the road safety and other efficiency parameters. In this technology it uses cars as node in a network to develop a mobile network. In vanet, the distance between cars around 100 to 300 meters and only those ones are allowed to connect together. The broadcast of messages by vehicles are in an open-access environment. It makes several critical security issues. A mishandling of this information may cause several critical issues like traffic accident and other traffic problems. So authentication of vehicles is necessary to improve the safety in vanet. During authentication a vehicles confidentiality-related data, such as identity of user and information about locations must be kept private.There are different types of authentication schemes are available and preserving the privacy related data of ve-hicles are different in different authentication schemes. A new authentication scheme with the help of dynamic generated tokens are proposed in this method. It increases the overall security of the system

IndexTerms **–VANET,RSU**

I. INTRODUCTION

Everything is becoming wireless. The fascination of mobility, accessibility and flexibility makes wireless technologies the dominant method of transferring all sorts of information. Satellite televisions, cellular phones and wireless Internet are well-known applications of wireless technologies. This work presents a promising wireless application and introduces a tiny contribution to its research community. Wireless research field is growing faster than any other one. It serves a wide range of applications under different topologies every one of which comes with some new specialized protocols. In this research, we will present an introduction to a wireless technology that is expected to be adopted by both governments and manufacturers in the very near future. It directly affects car accidents and the sales of one of the largest markets. It is the technology of building a robust network between mobile vehicles; i.e. let vehicles talk to each other. This promising technology is literally called Vehicular Ad-Hoc Networks (VANETs). In this research, an introduction to the technology of VANETs will be presented as well as a new contribution with a new dynamic token concept for increasing the security in VANET.

II. LITERATURE SURVEY

In the last few years, many privacy preserving authentication methods have been proposed such as pseudonym based methods , group signature-based schemes, ID-based schemes, symmetric cryptography-based methods.

A. M.Raya, P.Papadimitratos, and J.P. Hubaux,Securing vehicular communications,IEEE Wireless Commununication

Raya et al. [2] introduce a hardware security module (HSM) or a Temper Proof Device (TPD) that is used to protected the cryptographic stuff stored in a vehicles OBU. Among the vehicle on-board equipment, there should be two hardware modules needed for security, namely the Event Data Recorder (EDR) and the Tamper-Proof Device (TPD).Whereas the EDR only provides tamper-proof storage, the TPD also possesses cryptographic processing capabilities.The EDR will be responsible for recording the vehicles critical data, such as position, speed, time, etc., during emergency events, similar to an airplanes black box. These data will help in accident reconstruction and the attribution of liability. EDRs are already installed in many road vehicles, especially trucks. These can be ex-tended to record also the safety messages received during critical event.This scheme suffer from the storage and communication overhead of pseudonymous certificates. Usage of Certification Revoca-tion List(CRL) is a major drawback of this method. When revoking a vehicle, all the certicates issued to that vehicle needed to be included in the CRL whose size grows exponentially. Therefore, there is an extra overhead included in the distribution, storage and checking of CRL.

B. M.Rayaand, JP.Hubaux, Securing vehicular adhoc networks,J.Comput. Se-cur., vol. 15, no. 1, pp. 3968, 2007

Message authenticity is compulsory to defend VANETs from outsiders, as well as bad insiders. But since safety messages will not contain any responsive information, condentiality is not mandatory .As a result, the transferring of safety messages in a VANET requires authentication but not encryption. Digital signatures are a good methods in the VANET setting, because safety related messages are normally standalone, and should be transform to receivers as fast as possible.A work by Raya and Hubaux [1], in which they described the safety and privacy requirements for VANET and suggest one of the initial pseudonym-based schemes, many other

authors have followed their work and proposed a lot of pseudonym based and group signature-based schemes. The pseudonyms-based schemes are implemented by using Public Key Infrastructure (PKI). PKI based certicates are attached with the message that are signed with the equivalent private keys. Each certicate contains a pseudo identity. The relation between the pseudo identity and the certicate is known to the issuing authority, called certication authority (CA).

C. R.Lu, X.Lin, H.Zhu, P.-H.Ho, and X.Shen,ECPP:Efcient conditional pri-vacy preservation protocol for secure vehicular communications, in Proc. IEEE INFOCOM, Apr. 2008, pp. 1229123

Lu et al. [5] propose a conditional privacy preserving approach. A vehicle wants to get short-time pseudonym keys from RSU and therefore, this method requires pervasive operation of RSUs. A major drawback of this system is that the trusted authority needs to frequently distribute the RSUs with updated CRL. In this work introduce an efficient conditional privacy preservation (ECPP) protocol in vehicular adhoc networks (VANETs) to address the issue on anonymous authentication for safety messages with authority trace-ability. The proposed protocol is characterized by the generation of on-the-fly short-time anonymous keys between On-Board Units (OBUs) and Roadside Units (RSUs), which can provide fast anonymous authentication and privacy tracking while minimizing the required storage for short-time anonymous keys.

D. D. Y. W. Liu, J. K. Liu, Y. Mu, W. Susilo, and D. S. Wong, Revocable ring signature, J. Comput. Sci. Technol., vol. 22, no. 6, pp. 785794, Nov. 2007

Group signature allows the anonymity of a real signer in a group to be revoked by a trusted party called group manager. It also gives the group manager the absolute power of controlling the for-mation of the group. Ring signature, on the other hand, does not allow anyone to revoke the signer anonymity, while allowing the real signer to form a group (also known as a ring) arbitrarily without being controlled by any other party. In this paper, propose a new variant for ring signature, called Revocable Ring Signature. The signature allows a real signer to form a ring arbitrarily while allowing a set of authorities to revoke the anonymity of the real signer. This new variant inherits the desirable properties from both group signature and ring signature in such a way that the real signer will be responsible for what it has signed as the anonymity is revocable by authorities while the real signer still has the freedom on ring formation. We provide a formal security model for revocable ring sig-nature and propose an efficient construction which is proven secure under our security model.: Data sharing has never been easier with the advances of cloud computing, and an accurate analysis on the shared data provides an array of benefits to both the society and individuals. Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. Yet the costly certificate verification in the tra-ditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. Identity-based (id-based) ring signature, which eliminates the process of certificate verification, can be used instead. In this paper, we further enhance the security of id-based ring signature by providing forward security: if a secret key of any user has been compromised, all previous generated signatures that include this user still remain valid. This property is especially important to any large scale data sharing system, as it is impossible to ask all data owners to re authenticate their data even if a secret key of one single user has been compromised.

E. L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, A scalable robust authentication protocol for secure vehicular communications, IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 16061617, May 2010

Existing authentication protocols to secure vehicular ad hoc networks (VANETs) raise challenges such as certificate distribution and revocation, avoidance of computation and communication bottle-necks, and reduction of the strong reliance on tamper-proof devices. This paper efficiently copes with these challenges with a decentralized group-authentication protocol in the sense that the group is maintained by each roadside unit (RSU) rather than by a centralized authority, as in most existing protocols that are employing group signatures. In our proposal, we employ each RSU to maintain and manage an on-the-fly group within its communication range. Vehicles entering the group can anonymously broadcast vehicle-to-vehicle (V2V) messages, which can be instantly verified by the vehicles in the same group (and neighboring groups). Later, if the message is found to be false, a third party can be invoked to disclose the identity of the message originator. Our protocol efficiently exploits the specific features of vehicular mobility, physical road limitations, and properly distributed RSUs. Our design leads to a robust VANET since, if some RSUs occasionally collapse, only the vehicles that are driving in those collapsed areas will be affected. Due to the numerous RSUs sharing load to maintain the system, performance does not significantly degrade when more vehicles join the VANET; hence, the system is scalable.

F. X. Lin, X. Sun, P.-H. Ho, and X. Shen, GSIS: A secure and privacy preserv-ing protocol for vehicular communications, IEEE Trans. Veh. Technol, vol. 56, no. 6, pp. 34423456, Nov.2007

In this paper, first identify some unique design requirements in the aspects of security and pri-vacy preservation for communications between different communication devices in Vehicular Ad Hoc Networks (VANETs). Then propose a novel secure and privacy preserving protocol based on Group Signature and Identity-based Signature techniques, called GSIS. The work demonstrate that the proposed protocol can not only guarantee the requirements of security and privacy, but also pro-vide desired traceability of each vehicle in the case where the identity of the message sender has to be revealed by the authority for any dispute event. of VANETs in spite of its ultimate importance. In this paper, we are committed to tackle the problem of security assurance and

conditional privacy preserva-tion in vehicular communication applications. To the best of our knowledge, this is the first study that deals with the issues of both security and conditional privacy in VANETs through a cryptographic approach. We introduce a novel security and privacy preserving protocol for VANETs, called GSIS, by integrating the techniques of Group Signature and Identity based Signature . The security prob-lems are divided into the following two aspects: security and privacy preservation between OBUs and OBUs, as well as that between OBUs and RSUs, in light of their different design requirements.In the first aspect, group signature is used to secure the communication between OBUs and OBUs, where messages can be securely and anonymously signed by the senders while the identities of the senders can be recovered by the authorities. In the second aspect, a signature scheme using Identity-based cryptography (IBC) is adopted at RSUs to digitally sign each message launched by RSUs to ensure its authenticity, where the signature overhead can be greatly reduced. OBUs installed in emergency vehicles will be treated the same as RSUs since it is unnecessary to protect the privacy of both RSUs and OBUs installed in emergency vehicles.

G. Comparison of Different methods

Pseudonym scheme and group signature methods are the two main schemes in the area of privacy preserved authentication in VANET. The work done by Raya and Hubaux [4] is the first work pro-poses the pseudonym based scheme. This work use Public key infrastructure scheme.CA. Raya et al. [2] come up with more improvements by introducing a hardware security module (HSM) or a Temper Proof Device (TPD) that is used to protect the cryptographic content stored in a vehicles OBU. This work is more efficient than their previous works. Usage of HSM and TPD increases the efficiency of the system. But the system is suffered in the case that there is more overhead involved in the distribution and storage of pseudonym certificates. Certificate Revocation List usage is another major drawback of this system. Zhang et al[3] introduced realistic TPD in place of an ideal TPD which overcome the disadvantages of work done by CA. Raya et al. [2]. The usage of realistic TPD improves the overall working of the system. The scheme also offers conditional anonymity. The time required to update the CRL is one of the main problem faced by the works done in this area. The work by Sun et al. [4] reduces the CRL by proposing hash chains and uses a proxy re-signature scheme in order to get better the time required to renew the CRL. The work by Lu et al. [5] , the concept of short-time pseudonym keys requirement have some disadvantages that is the trustworthy authority needs to regularly issue the RSUs with updated CRL.Hierarchical pseudonymous-based approach that requires vehicle to get principal pseudonym from the CA and secondary pseudonyms from the RSU. But this system a pervasive use of RSUs is needed. In the case group signature based methods in all works the vehicles real identity is concealed among a group of vehicles. The approach in uses the RSUs to work as group managers in order to supervise and maintain the vehicles. In this work the main concept is that a group manager who have the central control to manage and maintain vehicles. The pervasive RSU deployment is need in this case but it can have a depressing impact on the overall performance. The scheme in the work by Liu et al. provides conditional anonymity but suffers from the delivery of revocation list information to all the vehicles.

III. PROPOSED SYSTEM

A. SYSTEM ARCHITECTURE

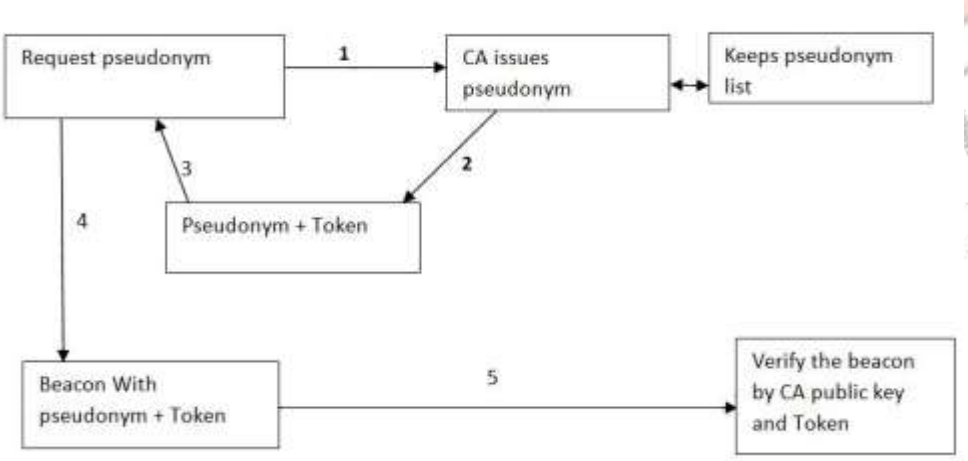

Fig1. System Architecture

The proposed system named “An Intelligent Traffic System with the help of a secure VANET” improves the security of the existing methods. In this method, introduce the concept of a dynamic token which used to authenticate the user. As the name implies the tokens are changed during a given interval of time. So users with newest tokens are considered as a genuine user. In old methods when a user is blocked by the certificate authority, in this method the blocked user never gets the newly created tokens. So when he comes with the old token other users can know as he is a blocked one or not a genuine user. So the dynamically generated token improves the overall security of the system.

The central part of the system is the certificate authority .Generation of pseudonyms is used to verify the user authenticity without disclosure the personal details. So privacy is preserved with the help of pseudonym. RSA cryptographic method is improves the

security of the system. The data is encrypted using RSA and transferring of encrypted data leads to better security. The communication between vehicles and other modules using such encrypted mechanism.

B. MODULES

1. Certificate Authority
   Certificate Authority is the central component of this system. The vehicles who wish to send messages through this VANET system first send request to the CA to generate the pseudonyms for keeping the privacy. The initiator vehicle first generates the public/private key pair using RSA. The vehicles send a request to the CA to generate the pseudonyms. The request contains the unique id and public key of the vehicle. The CA receive the request from the vehicles and check their unique id. Then check whether the car is already revoked or not. If it is not revoked the create a list of pseudonyms and sign the pseudonym with its private key. And the certificate Authority also responsible for creating the tokens.The tokens is created and sends to cars in certain time interval. When misbehavior is occurring then the vehicles are put into a revoked list. Revoked vehicles can't perform any action in the network.
2. Vehicular Module
   The vehicles broadcast the messages. The message contains the pseudonym and the message and the token. On the receiver side the vehicle checks the pseudonym and the tokens. So only those who have the correct pseudonym and tokens are become a genuine.
3. Road Side Unit(RSU)
   Road Side Units are responsible for passing the messages. It act as a by passer of message between vehicles.When vehicles moves outside the range the RSU is pass the messages.

C. IMPLEMENTATION

The proposed system use three methods,

1. Pseudonym generation
2. Token generation
3. Attaching Token with pseudonym

Pseudonym generation

The pseudonym concept is used or more security.During authentication, a vehicles privacy-related data, such as identity and location information, must be kept private.Before sending the messages between vehicles, the sender vehicle first request a pseudonym. CA(Certificate Authority) module is responsible for generating the pseudonym.

Pseudo code for pseudonym generation algorithm

```
Begin
   t= timestamp
   for i=1 to K
   begin
     Generate random n
   p=n // t
   pSigned=signCA(p)
   p[i]=pSigned // p
   t=t+200
   End for
End
```

Token generation

For more security a new concept "Dynamic Token" is introduced.As the name implies the token is changed within a time period.Token is a symmetric key and the generated key is send to all vehicles.

Psedocode for Token Generation Algorithm

```
token = new GenerateKey().generateKey();
generator = KeyGenerator.getInstance("DES");
generator.init(new SecureRandom());
key = generator.generateKey();
return key;
```

Attaching Token with pseudonym

The above algorithm is used to generate the pseudonym.In this system set the value of K as 10. So 10 different pseudonym are generated.Each pseudonym is signed by the CA.This sign is used to verify that the use is an authorized one.The vehicles used the pseudonym when they try to send the messages.At receiver side the receiver vehicle is check the pseudonym by verifying the signature of the CA.By using this concept during authentication, a vehicles privacy-related data, such as identity and location information, be kept private.

IV. RESULT AND CONCLUSION

ADVANTAGES OVER EXISTING METHODS

1. Reduces the cryptography overhead.
2. Tokens are used to avoid certificate concept in existing method.
3. In existing method,certificate become static.
4. Dynamic token increase security and easy to find blocked cars.
5. In Existing method the blocking needs more steps.
6. In proposed method blocking is simple an blocked vehicles never get the new token.

In VANET, the broadcast of messages by vehicles are in an open-access environment. It makes several critical security issues. A mishandling of this information may cause several critical issues like traffic accident and other traffic problems. So authentication of vehicles is necessary to improve the safety in VANET. In this project, proposed a method to improve the authentication mechanism in VANET. During the authentication time the vehicles privacy related information kept secret. A dynamic token which is created by a CA(Certificate Authority) is used to authenticate between vehicles. So the dynamic token changes during the time period which provides more security to the system. It reduces the cryptography overhead of existing methods.

REFERENCES

[1] M. Raya ,P. Papadimitratos,J.P. Hubaux} Securing vehicular communications,IEEE Wireless Commun,vol.13,no.5,pp.815,Oct2006.

[2] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, C. Hu ,Distributed aggregate privacy-preserving authentication in VANETs, IEEE Trans. Intell. Transp. Syst.,vol. 18, no. 3, pp. 516526, Mar. 2017.

[3] R.Lu, X.Lin, H.Zhu, P.H.Ho, X.Shen,,ECPP:Efcient conditional privacy preservation protocol for secure vehicular communications, in Proc. IEEE INFOCOM, Apr.2008, pp. 1229123.

[4] A. Shamir, Identity-based cryptosystems and signature schemes, in Advances in Cryptology. Berlin, Germany: Springer, 1984, pp. 4753.

[5] L. Zhang, Q. Wu, A. Solanas,J. Domingo-Ferre, A scalable robust authentication protocol for secure vehicular communications, IEEE Trans. Veh. Technol., vol.59, no. 4, pp. 16061617, May 2010.

[6] D. Y. W. Liu, J. K. Liu, Y. Mu, W. Susilo, D. S. Wong, Revocable ring signature,J. Comput. Sci. Technol., vol. 22, no. 6, pp. 785794, Nov. 2007.