ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Issue 4, April 2016

An Identity based Batch Verification Scheme For Authentication Provision in VANETs

T.S Sadham Hussain
M.E.,Computer Science and Engineering,
Mohamed Sathak Engineering college,
Kilaklarai. Tamilnadu, India.
Sadham10@gmail.com

Mr. M.Mohammed Sithik M.E
Assistant Professor, Computer Science and Engineering,
Mohamed Sathak Engineering college,
Kilaklarai. Tamilnadu, India.
sithikbe@gmail.com

Abstract— **In recent days the usage of Vehicular ad hoc networks are increased to improve traffic safety and efficiency. In VANETs, better communication efficiency can be achieved by sacrificing security and vice versa. But VANETs cannot get started without either of them. However, during communication user privacy is an important and practical concern to the deployment of VANET. For that many existing security protocols were suffered from the downloading or latest revocation list from a concerned authority and it cannot allow trustworthiness of message when the message is authenticated. In the existing paper they proposed with A Threshold Anonymous Authentication Protocol for VANETs that proposed a new group signature scheme to achieve threshold authentication and efficient traceability. It used more number of key to provide a secure communication and it also increased the authentication process too long. In this paper we are going to propose an efficient batch signature verification scheme for communications between vehicles and RSUs and vehicle 2 vehicles. Since identity-based cryptography is employed in generating private keys for pseudo identities, certificates are not needed and thus transmission overhead can be significantly reduced. Then we also implement an Identity-based Batch Verification (IBV) scheme for VANETs. In our proposed paper we are going to use Cramer–Shoup cryptosystem algorithm for encryption purposes.**

Keywords—VANET; Authentication; batchVerification;

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) are Implemented using the principles of mobile ad hoc networks (MANETs) - the spontaneous creation of a wireless Local network for data exchange - to the domain of vehicles. They became as a very important part of intelligent transportation systems (ITS). VANETs supports a wide range of applications from simple one hop information dissemination of, e.g., cooperative awareness messages (CAMs) to multi-hop dissemination of messages over vast distances. The concepts that are interest to mobile ad hoc networks (MANETs) are of interest in VANETs, but the working mechanisms differs in some cases such as Rather than moving at random, vehicles tend to move in an organized fashion. The interactions with the tower like equipment can likewise be characterized fairly accurately. Also most of the on board units in vehicles are restricted in their range of motion.

Example applications of VANETs are:

- *Electronic brake lights*, which allow a driver (or an autonomous car or truck) to react to vehicles braking even though they might be obscured (e.g., by other vehicles)
- *Platooning*, which allows vehicles too closely (down to a few inches) follow a leading vehicle by wirelessly receiving acceleration and steering information, thus forming electronically coupled "road trains".
- *Traffic information systems*, which use VANET communication to provide up-to-the minute obstacle reports to a vehicle's satellite navigation system

The term VANET sounds similar with the more generic term inter-vehicle communication (IVC), although the focus remains on the aspect of spontaneous networking, much less on the use of infrastructure like Road Side Units (RSUs) or cellular networks. VANETs which use vehicles as mobile nodes are a subclass of mobile ad hoc networks (MANETs) to provide communications among nearby vehicles and between vehicles and nearby roadside equipment but apparently differ from other networks by their own characteristics. Specifically, the nodes (vehicles) in VANETs are limited to road topology while moving, so if the road information is available, we are able to predict the future position of a vehicle; what is more, vehicles can afford significant computing, communication, and sensing capabilities as well as providing continuous transmission power themselves to support these functions.

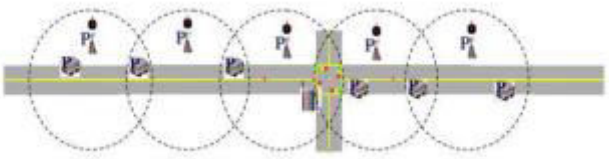

Fig. 1.1 RSU Grouping

In-vehicle communication, which is more and more necessary and important in VANETs research, refers to the in-vehicle domain. In-vehicle communication system can detect a

vehicle's performance and especially driver's fatigue and drowsiness, which is critical for driver and public safety.

Vehicle-to-vehicle (V2V) communication can provide a data exchange platform for the drivers to share information and warning messages, so as to expand driver assistance.

Vehicle-to-road infrastructure (V2I) communication is another useful research field in VANETs. V2I communication enables real-time traffic/weather updates for drivers and provides environmental sensing and monitoring.

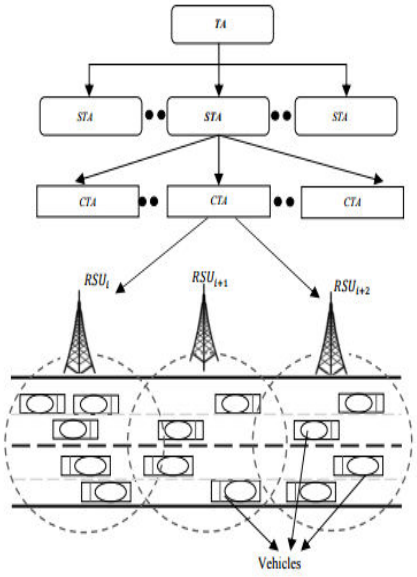

Fig 1.2 Architecture of VANET

Vehicle-to-broadband cloud (V2B) communication means that vehicles may communicate via wireless broadband mechanisms such as 3G/4G. A broadband cloud may include more traffic information and monitoring data as well as infotainment, this type of communication will be useful for active driver assistance and vehicle tracking.

II. MODELS AND DESIGN GOALS

In this section, we formalize the system model, security model, and identify our design goals.

A. System Model

Our system model is composed of the following parties: the central authority (CA), the tracing manager (TM), many RSUs, and many OBUs, as shown in Fig. 2. The CA is responsible for authenticating the public keys of RSUs. After authentication, the CA will issue the corresponding public key certificates. The TM is responsible for authenticating the public keys of OBUs. After authentication, the TM will issue the corresponding public key certificates. The TM is also able to reveal the real identity of the sender who broadcasts a false/in-dispute message in the network. RSUs are densely distributed along the road, and designed to manage a group of OBUs within their communication range. Especially, every RSU will issue every OBU within its communication range a group certificate that is used together with OBU's private key to sign the broadcasted message in the corresponding group. Each vehicle is equipped with an OBU, and the OBU can request group certificates from RSUs and communicate with each other based on the dedicated short-range communications protocol . The OBU accepts one message if and only if there are enough number of valid signatures on the message. The number could be adjusted in case the OBU desires. Note that RSUs won't issue the group certificate to the OBU which has existed in the revocation list managed by the TM.

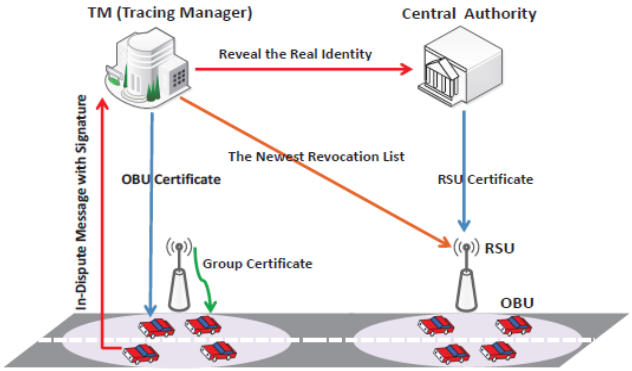

Fig 2.1 Existing Architecture

B. Security Model

We assume that the CA and TM are fully trusted, while RSUs are honest-but-curious. That is, RSUs will faithfully follow the proposed protocol, but could launch passive attacks to get secret information as much as possible. Specifically, RSUs will try to get the vehicle's trace or the real identities of the signers of broadcasted messages by colluding malicious OBUs, but they won't modify the communication data among them and OBUs, and won't collude with other OBUs. Honest OBUs accept one message if and only if there are enough number of OBUs broadcasting valid signatures on the same message. Each OBU has its own "enough number" (threshold value). Moreover, the signatures on broadcasted messages won't be revealed by others except the TM. To obtain privileges of the road, malicious OBUs may try to broadcast false messages or many signatures on the same message without being detected.

C. Design Goals

Our design goal is to develop an efficient threshold anonymous authentication protocol for VANETs. It has the following desirable properties. *Dynamic threshold:* The OBU can change the threshold at any time.

Distinguishability of message origin: Anyone can check whether two different signatures on the same message are generated by the same signer.

Efficient revocation: The TM is able to reveal the signer's identity of any one signature with constant computation and communication cost. Furthermore, the OBU does not need to retrieve the newest revocation list from the remote CA or TM.

Unforgeability: Only the OBU holding the group certificate from one RSU can generate valid signature on behalf of the group that is maintained by the RSU.

Anonymity: Only the TM can reveal the signer's identity. In other words, even RSUs, they cannot reveal any OBU's location if the OBU is not in their own communication range. *Traceability:* Any OBU cannot generate any valid signature which is traced back to other OBU.

III. EXISTING SYSTEM

Recently many research efforts have been dedicated to design anonymous authentication for VANET. However, these existing anonymous authentication protocols for VANET either suffer from the heavy workload of downloading the newest revocation list from a remote authority. So here we proposed a new protocol to solve the above said problems in VANET. WE proposed a Threshold Anonymous Authentication Protocol for VANETs that is a decentralized group model which used a new group signature scheme to achieve threshold authentication. This group signature scheme reduces the work burden of generation of group certificates for OBUs and it can easily retrieve the revocation list from the authority.

A group signature scheme is composed of the following five algorithms: SETUP, CERTGEN, SIGN, VERIFY, and OPEN. Then generated group signatures are verified and traced correctly with the help of our proposed group signature scheme. In case of an OBU requesting a group certificate which is not in a revocation list in the sense, RSU generate the group certificate for the OBUs. By using our proposed protocol an OBU is released by the RSU when the heavy work burden is encountered by an OBU. From this we can say our proposed protocol is efficient for revocation.

Dsadvantages

- It generates more number of key which increases the memory space
- Presence of certificate authority increases the probability of attacks.

IV. SYSTEM ARCHITECTURE

Authentication is the act of confirming the truth of an attribute of a single piece of data (a datum) claimed true by an entity. In contrast with identification which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity. It might involve confirming the identity of a person by validating their identity documents, verifying the validity of a Website with a digital certificate, tracing the age of an artifact by carbon dating, or ensuring that a product is what its packaging and labeling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification.

Authentication has relevance to multiple fields. In art, antiques, and anthropology, a common problem is verifying that a given artifact was produced by a certain person or was produced in a certain place or period of history. In computer science, verifying a person's identity is often required to secure access to confidential data or systems. The ways in which someone may be authenticated fall into three categories, based on what are known as the factors of authentication: something the user knows, something the user has, and something the user is. Each authentication factor covers a range of elements used to authenticate or verify a person's identity prior to being granted access, approving a transaction request, signing a document or other work product, granting authority to others, and establishing a chain of authority. Security research has determined that for a positive authentication, elements from at least two, and preferably all three, factors should be verified. The three factors (classes) and some of elements of each factor are:

The knowledge factors: Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN), challenge response (the user must answer a question, or pattern)

The ownership factors: Something the user has (e.g., wrist band, ID card, security token, cell phone with built-in hardware token, software token, or cell phone holding a software token)

The inherence factors: Something the user is or does (e.g., fingerprint, retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature, face, voice, unique bio-electric signals, or other biometric identifier).

The process of *authorization* is distinct from that of authentication. Whereas authentication is the process of verifying that "you are who you say you are", authorization is the process of verifying that "you are permitted to do what you are trying to do". Authorization thus presupposes authentication.

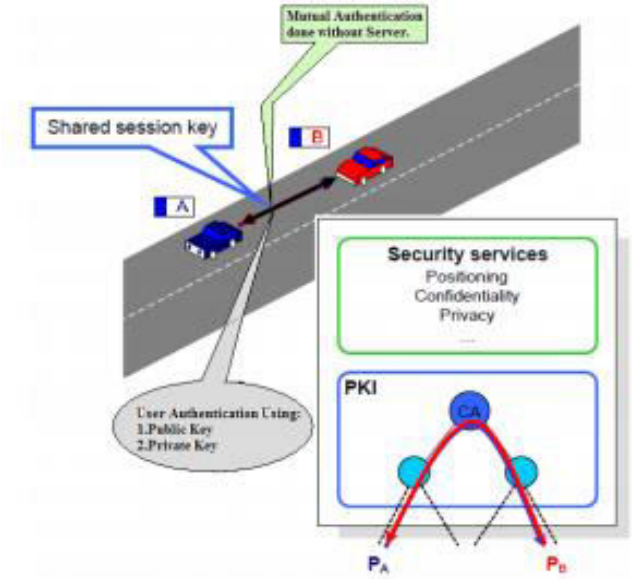

Fig 4.1 Authentication in VANET

In cryptography, a cryptosystem is called a "threshold cryptosystem", if in order to decrypt an encrypted message; several parties (more than some threshold number) must cooperate in the decryption protocol. The message is encrypted using a public key and the corresponding private key is shared among the participating parties. Threshold versions of encryption schemes can be built for many public

encryption schemes. The natural goal of such schemes is to be as secure as the original scheme. The most common application is in the storage of secrets in multiple locations to prevent the capture of the cipher text and the subsequent performance of cryptanalysis on that cipher text. Most often the secrets that are "split" are the secret key material of a public key cryptography key pair or the cipher text of stored password hashes.

Certificate Authority

In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made by the private key that corresponds to the certified public key. In this model of trust relationships, a CA is a trusted third party – trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. Many public-key infrastructure (PKI) schemes feature CAs.

Trusted certificates are typically used to make secure connections to a server over the Internet. A certificate is required in order to avoid the case that a malicious party which happens to be on the path to the target server pretends to be the target. Such a scenario is commonly referred to as a man-in-the-middle attack. The client uses the CA certificate to verify the CA signature on the server certificate, as part of the checks before establishing a secure connection. Usually, client software—for example, browsers—includes a set of trusted CA certificates. That makes sense in as much as users need to trust their client software: A malicious or compromised client can skip any security check and still fool its users into believing otherwise.

The problem of assuring correctness of match between data and entity when the data are presented to the CA (perhaps over an electronic network), and when the credentials of the person/company/program asking for a certificate are likewise presented, is difficult. This is why commercial CAs often uses a combination of authentication techniques including leveraging government bureaus, the payment infrastructure, third parties' databases and services, and custom heuristics. In some enterprise systems, local forms of authentication such as Kerberos can be used to obtain a certificate which can in turn be used by external relying parties. Notaries are required in some cases to personally know the party whose signature is being notarized; this is a higher standard than is reached by many CAs.

- A signature, contract or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form.
- A contract relating to such transaction may not be denied legal effect, validity or enforceability solely because an electronic signature or electronic record was used in its formation.

An authority revocation list (ARL) is a form of CRL containing certificates issued to certificate authorities, contrary to CRLs which contain revoked end-entity certificates. If the CA can be subverted, then the security of the entire system is lost, potentially subverting all the entities that trust the compromised CA.

V. PROPOSED SYSTEM

Our major design goal of this proposed system is to develop an efficient authentication protocol for VANETs. In the existing protocol, we separate the whole VANET into several small groups by RSUs who are response to generate group certificates for OBUs. To avoid the generation of certificates in this paper we propose a batch verification scheme. It avoids generation time of certificates. We introduce an efficient batch signature verification scheme for communications between vehicles and RSUs and v2v since identity-based cryptography is employed in generating private keys for pseudo identities, certificates are not needed and thus transmission overhead can be significantly reduced. We implement Identity-based Batch Verification (IBV) scheme for VANETs in the application we are going to use Cramer–Shoup cryptosystem algorithm.

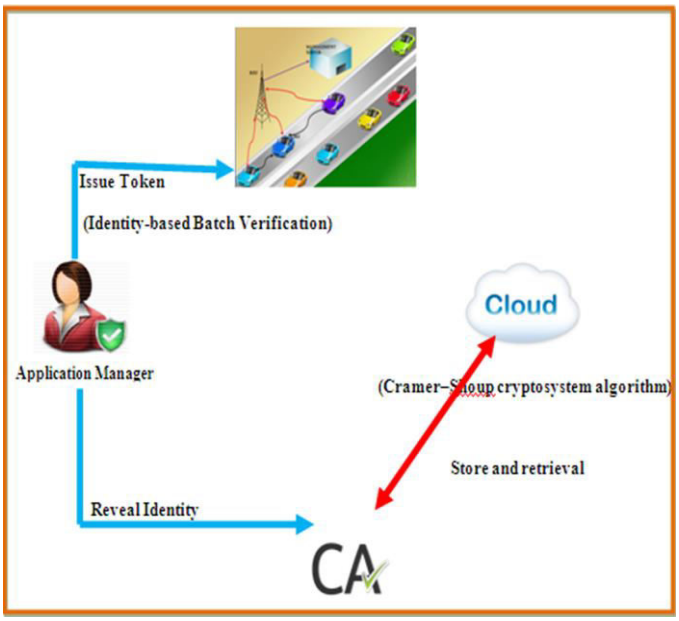

Fig 5.1 proposed system Architecture

The Cramer–Shoup system is an asymmetric key encryption algorithm, and was the first efficient scheme. Cramer–Shoup algorithm consists of three algorithms: the key generator, the encryption algorithm, and the decryption algorithm. Cramer–Shoup may be used in a hybrid cryptosystem to improve efficiency on long messages. If anyone of the cluster OBU comes for batch verification that corresponding batch token is received from the group for batch verification. This token is verified with the help of an Identity-based Batch Verification it allow those vehicles only otherwise discard it.

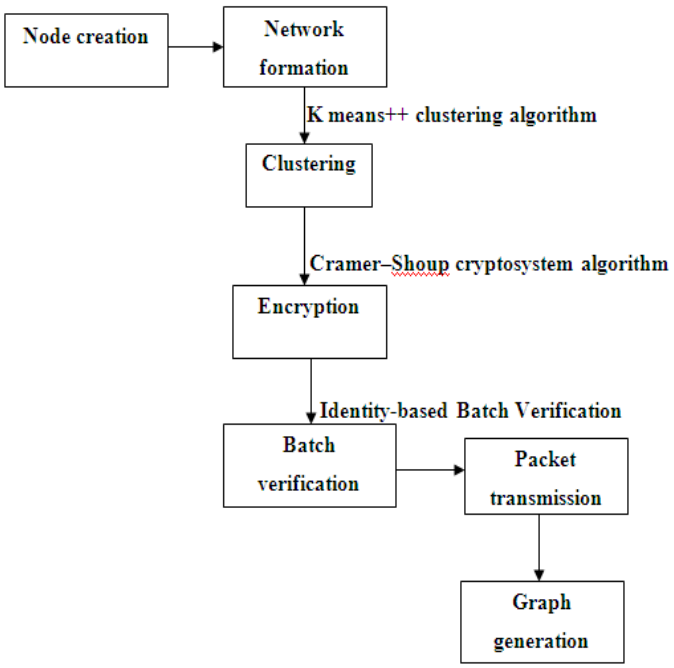

Fig 5.2 Data flow diagram

The above figure shows how data has been transferred from one module to another module, it explains the data flow from the node creation to graph generation,.

Advantages

- It reduced transmission overhead
- Our proposed system reduces the transmission time
- Cramer-Shoup suitable for long messages.

VI. SECURITY ANALYSIS

In this section, we analyze the security properties of our proposed protocol one by one.

A. Dynamic Threshold & Distinguishability of Message Origin

It is easy to see that the proposed protocol allows the OBU to set the threshold value as it wants. On the other hand, by using comparing $\sigma 9$ in the signature, the OBU can easily check whether two signatures on the same message are generated by the same signer or not.

B. Efficient Revocation

In the proposed protocol, we separate the whole VANET into several small groups by RSUs who are response to generate group certificates for OBUs. Only if the OBU requesting a group certificate is not in the revocation list, the RSU would generate the group certificate for the OBU. With the help of RSUs, OBUs can be released from the heavy workload of obtaining revocation list from the remote CA. On the other hand, algorithm OPEN allows the TM to trace the real identity of the signer for any signature on a bad message by only costing two exponentiations, one multiplication, and one division in G2. Hence, our protocol satisfies efficient revocation.

C. Unforgeability, Anonymity and Traceability

It is easy to verify that our proposed protocol satisfies unforgeability, anonymity and traceability by using the following Theorem.

Theorem: The proposed group signature scheme satisfies unforgeability.

Proof: We show that if there exists an adversary *A* breaking the unforgeability of our proposed group signature scheme, then we can build an algorithm *B* solving some hard problem by invoking *A* in a black-box manner. There are two cases in the forger. One is that the group member's private key corresponding to the forgery is unknown to *B*. The other is that the group member's private key is known to *B*. Note that in both cases, *A* cannot query the group certificate.

VII. RELATED WORKS

There have been many works dedicated to design efficient threshold anonymous authentication schemes.

In this section, we will focus only on research that makes use of decentralized group model or threshold authentication method. for more comprehensive and excellent surveys. With the aim to release the CA from the heavy workload of generating group certificate, and free the OBU from obtaining revocation list from remote CA, Lu et al. presented an efficient conditional privacy preservation protocol for secure vehicular communications, named ECPP. In ECPP, each vehicle should obtain a short-time anonymous certificate from an RSU when it is in the communication range of the RSU. However, in order to avoid the link ability of the messages, the OBU should frequently interact with RSUs. It is because that the short lived anonymous certificate should be sent and forwarded to verifiers for validating messages from the anonymous OBU.

Some schemes also apply the decentralized group model. However, in order to achieve anonymity, these two schemes require that a large set of anonymous certificates (public key) should be preloaded in each vehicle.

To avoid the frequent interaction between OBUs and RSUs, and the large preloaded set of anonymous certificates (public key), Zhang et al. proposed a new anonymous authentication in the decentralized group model by using group signature and signcryption . However, the scheme in does not support threshold authentication. Actually, the use of the threshold authentication method to achieve some assurance of trueness on the received traffic information is a common approach in many works.

The threshold value in the threshold authentication method may be fixed by the system or dynamic according to user's willing. One key issue to use the threshold authentication method is the distinguishability of message origin. That is, two signatures on the same message by the same signer should be linkable by anyone. Some schemes in give efficient solutions for this problem. Some advanced cryptographic techniques, such as message-linkable group signature, direct anonymous attestation, one-time anonymous authentication are used in these two schemes. However, these two schemes cannot satisfy efficient revocation. In particular,

to reveal the signer's identity, the scheme in should perform n pairing operations, where n is the number of vehicles in the system; while the scheme can reveal the signer's identity by using two signatures but not single one signature. Furthermore, OBUs in these two schemes should download the revocation list from the remote CA.

VIII. Conclusion

Commonly, an important requirement of a group signature scheme demands that honestly-generated signatures can be verified and traced correctly. In our proposed system we implemented a new encryption technique to reduce a transmission overhead and we provide a batch verification scheme for group identity verification. In the proposed protocol, we separate the whole VANET into several small groups by RSUs which contains number of onboard units. The groups of OBUs are termed as clusters. The cluster is formed with the help of k means++ clusters. K means++ cluster is developed from the drawback associated with k means algorithm. Then the batch verification is done with the help of Identity-based Batch Verification. Before starting batch verification process we should encrypt a message. So, we used Cramer–Shoup cryptosystem algorithm. Finally our simulation result shows that our proposed approach improves scalability and reduced transmission overhead.

In our future work, we will further improve the effectiveness of the broker-less in VANET**.** It reduces the presence of third party and improves encryption more efficient and provides improved security.

References

1. S. Dietzel, E. Schoch, B. K¨onings, M. Weber, and F. Kargl, "Resilient secure aggregation for vehicular networks," IEEE Network, vol. 24, no. 1, pp. 26–31, 2010. [Online]. Available: http://dx.doi.org/10.1109/MNET.2010.5395780.
2. Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," IEEE T. Vehicular Technology, vol. 59, no. 7, pp. 3589–3603, 2010. [Online]. Available: http://dx.doi.org/10.1109/TVT.2010.2051468.
3. X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc
4. networks," IEEE T. Vehicular Technology, vol. 62, no. 7, pp. 3339–3348, 2013. [Online]. Available: http://dx.doi.org/10.1109/TVT.2013.2257188.
5. Q. Wu, J. Domingo-Ferrer, and U´ . Gonza´lez-Nicola´s, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," IEEE T. Vehicular Technology, vol. 59, no. 2, pp. 559–573, 2010. [Online]. Available: http://dx.doi.org/10.1109/TVT.2009.2034669.
6. L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEE T. Vehicular Technology, vol. 59, no. 4, pp. 1606–1617, 2010. [Online]. Available: http://dx.doi.org/10.1109/TVT.2009.2038222.
7. L. Chen, S. Ng, and G. Wang, "Threshold anonymous announcement in vanets," IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp. 605–615, 2011. [Online]. Available: http://dx.doi.org/10.1109/JSAC.2011.110310.
8. J. Camenisch, S. Hohenberger, and M. Ø. Pedersen, "Batch verification of short signatures," J. Cryptology, vol. 25, no. 4, pp. 723–747, 2012. [Online]. Available: http://dx.doi.org/10.1007/s00145-011-9108-z.
9. J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 9, pp. 1227–1239, 2010. [Online]. Available: http://doi.ieeecomputersociety.org/10.1109/TPDS.2010.14.
10. V. Daza, J. Domingo-Ferrer, F. Seb´e, and A. Viejo, "Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks," IEEE T. Vehicular Technology, vol. 58, no. 4, pp. 1876–1886, 2009. [Online]. Available: http://dx.doi.org/10.1109/TVT.2008.2002581.
11. M. Raya, A. Aziz, and J. Hubaux, "Efficient secure aggregation in vanets," in Proceedings of the Third International Workshop on Vehicular Ad Hoc Networks, VANET 2006, Los Angeles, CA, USA, September 29, 2007, 2006, pp. 67–75. [Online]. Available: http://doi.acm.org/10.1145/1161064.1161076.