World Congress on Information and Communication Technologies
11 – 14 December 2011, Mumbai, India

A Secure and Efficient Message Authentication Protocol for VANETs with Privacy Preservation

Bharati Mishra[1], Saroj Kumar Panigrahy[2], Tarini Charan Tripathy[3], Debasish Jena[4], and Sanjay Kumar Jena[5]

[1,4]*International Institute of Information Technology Bhubaneswar, Odisha, India*
[2,5]*National Institute of Technology Rourkela, Odisha, India*
[3]*Kalam Institute of Technology, Berhampur, Odisha, India*
bharati@iiit-bh.ac.in, skp.nitrkl@gmail.com, tarinitripathy@yahoo.com, dr.djena@gmail.com, skjena@nitrkl.ac.in

Abstract

In this paper, a secure and efficient protocol for vehicular ad hoc networks has been proposed that ensures both message authentication and privacy preservation. As safety related message may contain life critical information, it is a necessity that the sender as well as the message are authentic. The proposed scheme is based on a secure elliptic curve digital signature algorithm approach. The proposed scheme supports conditional privacy, where the user's location can be revealed at the willingness of the user. Apart from this, the scheme is secure against attacks like DoS, Sybil and Grey/Black Hole attacks. From the comparison with previously proposed schemes, it is found that the proposed scheme as based on elliptic curve discrete logarithmic problem, outperforms existing algorithms based on integer factoring and discrete logarithmic problem.

Index Terms

VANETs, Authenticity, Privacy, Anonymity, ECDSA.

1. Introduction

Vehicular Ad hoc Networks (VANET) can be defined as a form of Mobile Ad hoc Networks (MANET) to provide communications among nearby vehicles and between vehicles and nearby fixed roadside equipments. In other words, VANET is a technology that uses moving vehicles as nodes in a network to create a mobile network. It turns every participating vehicle into a wireless router or node, allowing vehicles approximately 100 to 300 metres of each other to connect and, in turn, create a network with a wide range. As vehicles fall out of the signal range and drop out of the network, other vehicles can join in, connecting vehicles to one another so that a mobile Internet is created. In order to join the network each vehicle passes through a series of registration and authentication phases.

VANETs are a promising approach for facilitating intelligent transportation system (ITS) that includes road safety, traffic management, and infotainment dissemination for drivers and passengers. Security is a fundamental issue for promising applications in such networks. Due to extraordinarily high mobility of vehicles in a vehicular network, frequent handover requests will be a norm, which initiates the demand for an effective and fast authentication scheme that can maintain the service continuity in presence of the frequent handover events. This imposes the need for a strong message authentication technique that guarantees authentication as well as integrity. Also, VANETs are highly vulnerable to privacy threats. In a VANET, an adversary can easily monitor any target vehicle, track its location and extract information that is confidential and private to that vehicle. Therefore, another important security requirement of VANETs is to preserve the privacy of the participating nodes. Thus, the ultimate goal of the security solutions for VANETs is to provide security services, such as authentication, confidentiality, integrity, privacy, anonymity, and availability, to the users. Apart from these, VANETs are prone to some specific attacks such as the Denial of Service (DoS) attacks, Sybil attacks, Grey Hole attacks, Black Hole attacks and so on.

The proposed scheme is based on elliptic curve digital signature algorithm (ECDSA) which generates secure signatures that are to be used by the participating nodes. The vehicles are provided with temporary identities that are generated using secure cryptographic techniques. These temporary identities are used during any sort of communication, thereby preserving privacy and provide anonymity to the user. This scheme facilitates methods to prevent Sybil attacks and presents techniques to detect DoS attacks, Grey Hole attacks and Black Hole attacks.

The remaining sections of this paper is organized as follows. Section 2 provides the related works for secure VANET exist in literature. The proposed scheme for a secure and efficient VANET is discussed in Section 3. Section 4 describes the performance issues of the proposed scheme. Finally, Section 5 discusses the concluding remarks.

2. Existing Works Related to Secure VANETs

The basic objective of a secure VANET is to facilitate secure communication in an adversary environment. For instance, if two parties, A and B, want to safely communicate over an active network, they would definitely want to make sure that the data they correspond between themselves should remain private and authenticity of the data should be maintained. There have been a numerous studies performed by researchers to achieve these security goal and provide a safe and friendly environment to the users of the vehicular network. These papers are based on the various types of cryptosystems available.

2.1. Protocols for Message Authentication and Privacy Preservation

Message authentication with privacy preservation is a very active topic for securing VANETs. The idea of Identity-based anonymity approaches is to make vehicles not identifiable. According to Rongxing [1], there are two basic models for identity-based anonymity approaches: one is huge anonymous keys based (HAB) [2], [1], [3], the other is group signature technique based (GSB) [4], [5]. Both of them can address the security requirements well, such as authentication, non-repudiation, identity revocation, and conditional anonymity. In the group-signature-based schemes, utilizing group signatures [6], any public entity will not reveal the originator identity of a routine traffic message [7], [8]. However, one limitation is that the cost for signing and verifying messages is far more than adopting the traditional public-key based signature. To reduce these overheads, A. Wasef et al. [9] propose the Hybrid scheme, wherein a vehicle can issue a certificate for itself by using a group key and then signing its messages using the public-key-based signature. In such a way, the average overhead of message authentication can decrease. This scheme achieves a tradeoff between the group-signature-based scheme and traditional PKI-based schemes.

However, due to the limited bandwidth of wireless communication and the high-speed mobility of vehicles, it is difficult to distribute a large certificate revocation list (CRL) to all vehicles in a timely fashion. To decrease the CRL size, Bellur [7] suggests segmenting a country into a number of geographic regions and assigning region-specific certificates with a validity period to a vehicle. Lu et al. [1] develop the efficient conditional privacy preservation (ECPP) protocol, which is the first protocol to support legitimate vehicles updating short time Pseudonymous certificates from the RSUs frequently.

2.1.1. Scheme Based on Blind Signature and One-Way Hash Function. The scheme by Chun-Ta Li et al. [10] not only accomplishes V2V and V2I authentication and key establishment for communication between members, but also integrates blind signature techniques into the scheme in allowing mobile vehicles to anonymously interact with the services of roadside infrastructure. According to the security threats and privacy issues into consideration, the scheme claims to maintain essential requirements.

2.1.2. Message Authentication Scheme Based on ECDSA. ECDSA is a variant of the Digital Signature Algorithm (DSA) that operates on elliptic curve groups [11]. S. S. Manvi et al. in [12], proposed an efficient message authentication scheme that is based on elliptic curve digital signature algorithm (ECDSA). The authors of the paper have claimed to overcome some inherent drawbacks of existing authenticating and security schemes like: more processing delay for authentication at sender and receiver, computational and communicational overheads, storage requirements, etc.

2.2. Inherent Drawbacks of Existing Schemes

The existing schemes are efficient and reliable. The researchers have also proved their claims to be true and up to mark. Each of these papers have significant contributions to the security of VANETs. Some of these inherent drawbacks of the existing schemes are listed below:

- More processing delay for authentication at sender and receiver.
- Computational and Communicational overheads. List of revoked vehicles must be continuously updated and broadcasted to all nodes, this leads to computational complexities.
- Storage/memory requirements for storing the updated revocation lists as well as each pseudonym need to be certified and stored.

Motivated by this, a protocol has been proposed that takes the advantages of the existing schemes and improves them so as to achieve authentication, conditional privacy and security against attacks. The scheme provides data integrity, data origin authentication, non-repudiation, reliability and efficiency. It is based on ECDSA as a 160-bit key in ECC is as secured as 1024-bit key in RSA and, ECC is faster and occupies less memory space. Also it guarantees security as ECDLP is more secure as compared to its counterparts IFP and DLP.

3. Proposed Scheme for Secure VANET

3.1. System Model

Some design decisions were made in the course of building the system model. These decisions were made after taking into consideration both practical implementation and performance issues.

Let us consider a VANET composed of a large number of vehicles $V = \{V_1, V_2, ...\}$ and a spot of roadside units (RSUs) $R = \{R_1, R_2, ...\}$, as shown in Figure 4.1 [13]. In the VANET, each vehicle $V_i \epsilon V$ has a unique nonzero identifier and moves from one place to another either along a fixed route (e.g., bus) or by choosing a dynamical path (e.g., taxi), while each RSU $R_j \epsilon R$ is placed at some critical locations L_j in the area. The communications between vehicle and vehicle are bidirectional, i.e., two vehicles within the transmission range T_V can communicate with each other. However, since RSU's transmission range T_R is larger than T_V, the communication between vehicle and RSU is not entirely bidirectional. Assume that the distance between vehicle V_i and RSU R_j is $D = |V_i - R_j|$. When $T_V < D \leq T_R$, only V_i can detect the existence of R_j; when $0 \leq D \leq T_V$, V_i and R_j can communicate with each other.

3.2. The Proposed Protocol

In this section, an RSU aided message authentication scheme has been proposed which shall also provide conditional privacy preservation. When a vehicle shall come in the range of an RSU, it shall request the RSU for a temporary ID known as pseudo ID which will be valid till the vehicle moves to another RSU's range. This pseudo ID will be used by the sender vehicle for its identity instead of its actual identity. When the vehicle wants to send a message, the vehicle shall sign the message with its private key using ECDSA signature and append its temporary ID in place of sender address. The vehicle which receives the message shall query the RSU for the public key of the sender vehicle and provides the sender's pseudo ID in the request. The RSU shall find out the actual ID from the pseudo ID and broadcast the corresponding public key of the sender vehicle. The interested vehicles shall verify the sender vehicles signature and thus authenticate the message but the sender's identity remains anonymous to the receiving vehicles.

Notations that are used throughout this proposed scheme are summarized in Table 1 and the details of the proposed scheme are described in the following subsections.

3.2.1. Vehicle Registration with Trusted Authority. Before VANET setup, interested vehicles shall register themselves with transport authorities. This will be an offline process. The vehicle owner shall provide its identity, address and proof for the same. After verification, the transport authority shall ask the owner to provide the key pool to be registered. The vehicle owner shall generate a pool of ECDSA public-private key pairs using following algorithm.

A vehicle A's key pair is associated with a particular set of EC domain parameters $D = (q, F_R, a, b, G, n, h)$.

Table 1. Notations Used Through The Proposed Scheme

Symbols Used	Description
Q_i, d_i	Public and Private key of i^{th} vehicle
TID_i	Temporary ID of i^{th} vehicle
VID_i	Actual ID of i^{th} vehicle
S	Source
D	Destination
RSU_{Pr}	Private key of RSU
$H(m)$	A cryptographic hash function on message m
$\oplus$	Exclusive-Or operation
T_D	Timestamp, that Destination attaches
T_S	Timestamp, that Source attaches
$a\|\|b$	Concatenation of a and b
TID_S, TID_I, TID_D	Temporary ID of Source, Intermediate and Destination vehicles resp.
D	Elliptic curve domain parameter
M_i	Message sent in i^{th} iteration
ACK_j	Acknowledgement in j^{th} iteration

This association is assured cryptographically i.e. through certificates.

- ▷ Select a random or pseudorandom integer d in the interval $[1, n-1]$.
- ▷ Compute $Q_A = d * G$.
- ▷ A's public key is Q_A and private key is d.
- ▷ For different values of d, different Q_A values are generated which shall form the pool of public keys for vehicle A.

Vehicle A shall register these public keys against its ID which is VID_A. These public keys have a certain validity period. After the validity period expires, A must renew the public key pool by generating and registering a fresh set of public keys. The transport authority then issues certificates authenticating the public keys. For this it signs the certificates with its private key. Any third party can validate these certificates using the public key of the TA.

3.2.2. RSU Installation Phase. After vehicle registered, the transport authority shall deploy RSUs at each road section. It shall upload the details of the entire vehicle registered till date to the RSU. In turn the RSU also will be registered with the TA and its public key shall be conveyed to all the registered vehicles.

Temporary Identity Acquisition Phase. When a vehicle's range reaches an RSU, the vehicle sends a request to the RSU to provide a temporary identity. It also sends its identity and public key certificate which it shall use in further communication. The RSU shall validate the identity and the certificate for the public key. Then it shall generate a temporary identity for the vehicle and send it in the reply.

$$TID_I = VID_I \oplus (RSU_{Pr}) \quad (1)$$

Message Transfer Phase. The message transfer performed by the vehicles in a VANET can be broadly categorized into two types.

A. Broadcast of Message.

- **Step I: Signing the Messages**
  When the vehicle wants to send a message first it needs to sign the message with its private key corresponding to the public key it has conveyed to the RSU. It shall not send its true identity. Instead it shall use its temporary identity TID.
- **Step II: Public Key Look Up**
  The vehicle which receives the message and the signature shall enquire the nearby RSU for the public key corresponding to the TID_I. The RSU shall calculate VID_I from the TID_I as follows:

$$VID_I = TID_I \oplus (RSU_{Pr}) \tag{2}$$

  Then it shall retrieve the public key for the VID_I and broadcast it. The interested vehicles shall use the public key for verification of the message received.
- **Step III: Message Signature Verification**
  The vehicles after receiving the public key, shall verify the signature on the message using ECDSA signature verification method discussed earlier.

B. Personalized Message Transfer. The whole process is divided into two steps, such as: Firstly, checking of the presence of destination vehicle in the range of RSU, and secondly, the communication process. There may arise 2 cases in the above said communication process.
a. Destination is within the range of both source and RSU.
b. Destination is not within the range of source but is within the range of RSU.

1. Checking of the presence of destination vehicle in the range of RSU. In this step the source vehicle checks whether the destination vehicle is present in the range of RSU or not.

- **Step 1:** The source vehicle sends the temporary identity (TID_S) assigned to it and temporary identity of destination vehicle(TID_D) to the RSU within its range.
- **Step 2:** After getting the temporary identities, the concerned RSU checks its own database to confirm whether the destination vehicle is present within it's range or not.
- **Step 3:** If the destination vehicle is present within the range of RSU, then that RSU sends a positive acknowledgement (ACK) to the source vehicle; otherwise it sends a negative acknowledgement (NACK).
- **Step 4:** If negative acknowledgement comes from RSU, then the communication process stops. If there is positive acknowledgement from RSU, then the communication process begins.

2. Communication Process. Prior communication process starts, there are some computations done by source vehicle. Source vehicle first selects a random number 'a'. It computes $C = (Q_D^2)^{H(T_S)*d_S}$ where Q_D is the public key of destination and d_S is the private key of the source. T_S is the timestamp generated by the source vehicle. Then it computes $C \oplus a$. According to the position of presence of destination vehicle there are two cases. Both of the cases will be discussed separately.

Case I: Destination is within the range of both source and RSU. In this case, the destination vehicle is present in the range of both source and RSU.

- **Step 5:** The source vehicle sends the TID_S, TID_D, T_S, $C \oplus a$ to destination vehicle. Then C is calculated by the source vehicle before.
- **Step 6:** At first the destination vehicle checks whether the received temporary destination id is his own or not. If it doesnot match then the message is dropped. If it matches then the destination vehicle computes $C' = (Q_S^2)^{H(T_S)\oplus d_D}$ where Q_S and d_D are public key of source and private key of destination respectively. After computing C', it recovers the random number 'a' by computing $C \oplus a \oplus C'$. Then it will select a random number 'b'. Then it computes $K = H(a||b||0)$.
- **Step 7:** The destination vehicle sends TID_D, TID_S, T_D, $C' \oplus (b||k)$ to the source vehicle.
- **Step 8:** The source vehicle has previously computed C. Now the source vehicle recovers b and K by computing $C' \oplus (b||K) \oplus C$. Then the source vehicle compute $k' = H(a||b||0)$. Then it compare K with k'. If both are equal to each other then the destination vehicle is proved as authenticated and mutual authentication get established between source and destination.
- **Step 9:** After authenticating each other message transfer starts between source and destination. The source vehicle sends TID_S, TID_D, T_S, $C \oplus M_i$ to the destination vehicle where M_i is the message transferred at ith iteration. The destination vehicle recovers the message M_i by computing $C' \oplus M_i \oplus C$.
- **Step 10:** After recovering the message the destination vehicle send an acknowledgement to the source vehicle. So it sends TID_S, TID_D, T_D, $C' \oplus ACK_j$ to the source vehicle. The source vehicle recovers ACK_j by computing $C' \oplus ACK_j \oplus C$.

Case II: Destination is not within the range of source but is within the range of RSU. In this case the destination vehicle is not present in the range of source but it is present in the range of RSU. The detail process is shown in the figure 7 and explained in various steps.

- **Step 5:** As the destination vehicle is not present in the range of source vehicle, the source vehicle sends TID_S, TID_D, T_S, $C \oplus a$ to all the vehicles that are

present in the range of source. The C is calculated by the source vehicle before.

- **Step 6:** In this step, all the intermediate vehicles who got the message from the source vehicle checks that whether the destination vehicle is present in their range. Any of them who finds the destination in his range, forwards TID_S, TID_V, TID_D, T_S, $C \oplus a$ to the destination vehicle.
- **Step 7:** At first the destination vehicle checks whether the received temporary destination id is his own or not. If it doesn't match then the message is dropped. If it matches then the destination vehicle computes $C' = (Q_S^2)^{H(T_S)*d_D}$ where Q_S and d_D are public key of source and private key of destination respectively. After computing C', it recovers the random number 'a' by computing $C \oplus a \oplus C'$. Then it will select a random number 'b'. Then it computes $K = H(a||b||0)$.
- **Step 8:** The destination vehicle sends TID_D, TID_I, TID_S, T_D, $C' \oplus (b||k)$ to the intermediate vehicle.
- **Step 9:** The intermediate vehicle forwards TID_D, TID_I, TID_S, T_D, $C' \oplus (b||k)$ to the source vehicle.
- **Step 10:** The source vehicle has previously computed C. Now the source vehicle recovers b and K by computing $C' \oplus (b||K) \oplus C$. Then the source vehicle compute $k' = H(a||b||0)$. Then it compare K with k'. If both are equal to each other then the destination vehicle is proved as authenticated and mutual authentication get established between source and destination.
- **Step 11:** After authenticating each other message transfer starts between source and destination. The source vehicle sends TID_S, TID_D, T_S, $C \oplus M_i$ to the destination vehicle where M_i is the message transferred at ith iteration.
- **Step 12:** The intermediate vehicle forwards TID_S, TID_I, TID_D, T_S, $C \oplus M_i$ to the source vehicle. The destination vehicle recovers the message M_i by computing $C' \oplus M_i \oplus C$.
- **Step 13:** After recovering the message the destination vehicle send an acknowledgement to the intermediate vehicle. So it sends TID_D, TID_I, TID_S, T_D, $C' \oplus ACK_j$ to the destination vehicle.
- **Step 14:** The intermediate vehicle forwards TID_D, TID_I, TID_S, T_D, $C' \oplus ACK_j$ to the source vehicle. The source vehicle recovers ACK_j by computing $C' \oplus ACK_j \oplus C$.

Finally, after completing all these above given steps of the proposed protocol, each vehicle in a VANET can now be guaranteed a much more secure driving as well as communicating environment, with assured privacy preservation.

4. Performance Analysis

In this section, the performance of the proposed scheme is evaluated and compared with other related works in terms of computational costs. In [14], He et al. proposed an authorized anonymous ID-based scheme. The security of their scheme is based on blind signature and RSA cryptosystem. Later, in [15], Yang et al. proposed a secure scheme for providing anonymous communications in wireless systems without using asymmetric cryptosystems. The results of a comparison of efficiency between the proposed scheme, Chun-Ta Li et al.'s scheme [10], Yang et al.'s scheme [15] and He et al.'s scheme [14] are shown in Table 2. For evaluation of performance, some computational parameters are defined as follows.

Table 2. Efficiency comparisons between the proposed scheme and other related schemes

Parameter	Proposed Scheme	Chun-Ta-Li's scheme [10]	Yang et al.'s scheme [15]	He et al.'s scheme [14]
T_{asym}	2	5	0	6
T_{sym}	0	0	8	2
T_{exp}	0	0	17	0
T_{hash}	4	9	0	5
T_{xor}	9	9	4	0
Total computation costs	200 T_{sym}	500 T_{sym}	1028 T_{sym}	602 T_{sym}

- T_{exp} — denotes the time for the modular exponentiation.
- T_{hash} — denotes the time for the hashing operation.
- T_{sym} — denotes the time for the symmetric encryption/decryption operation.
- T_{asym} — denotes the time for the asymmetric encryption/decryption operation.
- T_{xor} — denotes the time for the XOR ($\oplus$) operation.

For instance, a symmetric encryption/decryption is at least 100 times faster than an asymmetric encryption/decryption in software and an exponential operation is approximately equal to 60 symmetric encryptions/decryptions. Moreover, it requires 0.0005s to perform a one-way hashing operation and 0.0087s to perform a symmetric encryption/decryption.

4.1. Computational Overhead

From Table 2, the proposed protocol outperforms the other three existing protocols. The computational costs of the one-way hash function and the XOR ($\oplus$) operations is ignored since these two kinds of operations are quite lighter in terms of load than that of a symmetric encryption/decryption.

4.2. Communication Overhead

Any two communicating nodes in the service phases of the proposed scheme require two communication rounds to accomplish mutual authentication and message integrity. Note that two rounds is the minimum number needed for any

authenticated communication scheme with mutual authentication to fulfill its goal. As a result, the proposed scheme is highly efficient in limited computation and communication resource environments to access the dynamic and remote information systems.

4.3. Storage Overhead

In the authorization phase, the proposed scheme achieves low storage overheads because the service provider (that is the RSU in this scheme) does not need to maintain authorized credential per user at all point of time and each credential is still secure against malicious attacks. In addition, each user only needs to store its own credential like its certificate $Cert_i$ and its private key. While the other service phases are running, for involved participants, including the vehicular node and the roadside unit only need to maintain one credential $Cert_i$ and two random numbers (a, b) for each currently in-use credential and thus the storage overhead of MAPWPP scheme is much less compared to other related schemes.

5. Conclusion

In this paper, attempts have been made to design a secure and efficient communication scheme for VANETs. Here a novel RSU involved communication scheme is proposed. As ECDLP is used for encryption, hence the protocols require less computational power, memory and communication bandwidth giving it clear edge over the traditional crypto-algorithm. By comparison with other related schemes, the proposed scheme not only provides the advantage of user privacy preservation but also maintains good and sought after properties (e.g. low computational cost). Hence, a vehicular node can anonymously interact with other vehicular node and nobody can learn information about the user (e.g. location/user identification/transaction privacy). As the schemes are based on ECDLP, they achieve the same security with fewer bits key as compared to their counterpart like IFP and DLP based schemes.

References

[1] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, april 2008, pp. 1229 –1237.

[2] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *Wireless Communications, IEEE*, vol. 13, no. 5, pp. 8 –15, october 2006.

[3] Y. Jiang, M. Shi, X. Shen, and C. Lin, "Bat: A robust signature scheme for vehicular networks using binary authentication tree," *Wireless Communications, IEEE Transactions on*, vol. 8, no. 4, pp. 1974 –1983, april 2009.

[4] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "Gsis: A secure and privacy-preserving protocol for vehicular communications," *Vehicular Technology, IEEE Transactions on*, vol. 56, no. 6, pp. 3442 –3456, nov. 2007.

[5] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," in *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*, ser. VANET '07. New York, NY, USA: ACM, 2007, pp. 19–28. [Online]. Available: http://doi.acm.org/10.1145/1287748.1287752

[6] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *Proceedings of the 11th ACM conference on Computer and communications security*, ser. CCS '04. New York, NY, USA: ACM, 2004, pp. 168–177. [Online]. Available: http://doi.acm.org/10.1145/1030083.1030106

[7] B. Bellur, "Certificate assignment strategies for a pki-based security architecture in a vehicular network," in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, 30 2008-dec. 4 2008, pp. 1 –6.

[8] C. Jung, C. Sur, Y. Park, and K. Rhee, "A robust conditional privacy preserving authentication protocol in vanet," in *Proceeding of MobiSec*, June 2009, pp. 35–35.

[9] A. Wasef, Y. Jiang, and X. Shen, "Dcs: An efficient distributed-certificate-service scheme for vehicular networks," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 2, pp. 533 –549, feb. 2010.

[10] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Computer Communications*, vol. 31, no. 12, pp. 2803 – 2814, 2008, mobility Protocols for ITS/VANET.

[11] B. S. M. Aydos and C. K. Koc, "An elliptic curve cryptography based authentication and key agreement protocol for wireless communication," *2nd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications*, pp. 1–12, October 1998.

[12] S. Manvi, M. Kakkasageri, and D. Adiga, "Message authentication in vehicular ad hoc networks: Ecdsa based approach," in *Future Computer and Communication, 2009. ICFCC 2009. International Conference on*, april 2009, pp. 16 –20.

[13] X. Lin and H.-H. Chen, "A secure and efficient rsu-aided bundle forwarding protocol for vehicular delay tolerant networks," *Wirel. Commun. Mob. Comput.*, vol. 11, pp. 187–195, February 2011. [Online]. Available: http://dx.doi.org/10.1002/wcm.935

[14] Q. He, D. Wu, and P. Khosla, "The quest for personal control over mobile location privacy," *Communications Magazine, IEEE*, vol. 42, no. 5, pp. 130 – 136, may 2004.

[15] C.-C. Yang, Y.-L. Tang, R.-C. Wang, and H.-W. Yang, "A secure and efficient authentication protocol for anonymous channel in wireless communications," *Applied Mathematics and Computation*, vol. 169, pp. 1431–1439, 2005.