A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks

Chun-Ta Li , Min-Shiang Hwang , Yen-Ping Chu

Roll no: 201001004
International Institute of Information Technology, Hyderabad 500 032, India
E-mail: saumya.choudhary@students.iiit.ac.in
Center for Security, Theory and Algorithmic Research

Roll no: 201001115
International Institute of Information Technology, Hyderabad 500 032, India
E-mail: surya.baghrecha@students.iiit.ac.in
Center for Security, Theory and Algorithmic Research

Roll no: 201001126
International Institute of Information Technology, Hyderabad 500 032, India
E-mail: saumya.dwivedi@students.iiit.ac.in
Center for Security, Theory and Algorithmic Research

Abstract:

Security and privacy preservation are key issues in Vehicular Ad Hoc Networks. In this proposal, Chun Ta Li's paper has been reviewed and modifications suggested to increase efficiency of such communication networks while preserving privacy and message authentication. Some of the attacks identified also have corresponding solutions proposed along with it. The proposed scheme is based on a secure elliptic curve digital signature algorithm approach as compared to Li's non-interactive ID-based scheme.

Keywords:

Anonymous communication protocol, ad hoc networks, ECDSA, privacy, mutual authentication, key establishment,Vehicular ad hoc networks

Introduction:

The wireless communication devices installed on vehicles, also known as on-board units (OBUs), and the roadside units (RSUs), form a self-organized Vehicular Ad Hoc Network (VANET). Furthermore, the RSUs are connected to the backbone network via the high speed network connections. In this way, VANETs inherently provide a way to collect traffic and road information from vehicles, and to deliver road services including warnings and traffic information to users in the vehicles.

Security and efficiency are the two most concerned issues when dealing with such type of networks. Obviously, any malicious behaviors of user, such as injecting messages with false information, modifying and replaying the previously disseminated messages, could be fatal to the other users. Thus, identifying the message issuer is mandatory to reduce the risk of such attacks. Meanwhile, in order to protect the user-related private information, such as the driver's name, the license plate, speed, position, and travelling routes along with their relationship, authentication in VANETs should be privacy-preserving.

Hence, a safe protocol must protect against fake information attack, message replay attack, message modification attack, Impersonation attack, RSU preemption/replication attack and denial of service attack.

Many researchers including Chun Ta li has addressed most of the issues raised in VANET communication. However, by some research, we found that their suggested protocol violates the anonymity property. Also, although they claim that their scheme is efficient in its

implementation on mobile vehicles in comparison to other related proposals, but we found that there are methods which are more efficient and yet preserve anonymity.

The following section lists the works of various other researchers and their proposed algorithm. In next section we propose our modification to the authentication scheme followed by sections on performance analysis and comparison with other schemes. This is followed by references.

RELATED WORK:

PKI: A public-key infrastructure (PKI) satisfies security requirements like authenticity and data integrity proposed by Parno and Perrig. Pseudonymous PKI provides privacy through the use of multiple certificates or pseudonyms obtained from the infrastructure. These pseudonyms do not contain any direct identity information of the vehicle. To appear anonymous to other vehicles and adversaries, a vehicle may use each pseudonym for signing a small number of messages so that only a limited number of its messages may be linked to one another. Each such pseudonym must be certified by the CA. Therefore, in pseudonymous PKI, vehicles need to communicate frequently with the infrastructure to obtain new sets of pseudonyms, resulting in communication overhead.

TACK Scheme:TACK's Temporary anonymous Certificate keys where vehicle communicate with CA through regional authority they store updated revocation information from group manager and grant short lived keys only when they are not revoked by gm(group manager). Both requires extensive communication to eliminate this autonomous certificate scheme (A vehicle generates initial set of master credentials and later it generates without using involvement of CA)

PKI+ user generates public key n their certificates without using CA. Ca is only required only for initial registration phase where it gets master certificate n pubkey n also for updated parameters after each revocation.

In **PKI++** , all non-revoked vehicles are not forced out of the group at every revocation event. Revocation is achieved by publishing revocation lists. Thus, a non-revoked vehicle without the latest revocation list can still authenticate its messages, though it may accept messages from some revoked vehicles. PKI++ also ensures backward unlinkability of revoked vehicles. Thus, compared to PKI+, revocation in PKI++ is made less costly, albeit at the expense of additional storage and computation overhead.

Ring signature scheme introduced by Rivest, Shamir and Tauman Rivest et al. (2001), offers two main properties: anonymity and spontaneity. In practice, anonymity in a ring signature means 1-out-of-n signer verifiability, which enables the signer to keep anonymous in these “rings" of diverse signers. This scheme allows a real signer to form a ring arbitrarily while allowing a set of authorities to revoke the anonymity of the real signer. . However, this protocol suffers larger communication overhead than that of other protocols because the length of ring signature depends on the size of the ring.

In **Chum’s blind signature scheme**, there are two main participants, namely: the user and the signer, respectively. The user first generates a message m and the signer will generate the digital signature on message m for the user by using signer’s private key and the signer will be unable to know the content of signed message and it can be implemented based on existing well-known digital signature schemes. However it is subjected to the RSA blinding attack through which it is possible to be tricked into decrypting a message by blind signing another message.

Proposed Scheme:

We are proposing solutions/different method of implementation for the following issues in Li’s paper:

1) **Violation of Anonymity property**
As per the paper, before a vehicular ad hoc network is deployed, we need the aid of a trusted third party TTP only at the initial network formation. Consider the scenario that a vehicular node wants to be able to dynamically access available services in VANETs.
[Pre-Deployment Phase] Whenever a new vehicle wants to join the network(Vi), Vi will perform the following phase with TTP. First, V i must personally go to registration center and provide his/her identification information to the center for registration. Then, the TTP of the registration center presents a set of node parameters and sends them to Vi through a secret channel, including V i’s identity VIDi; the identity of the roadway section rl; the group’s secret key HtSK shared among all nodes in the network; Vi’s secret key VKi. It is also assumed that the vehicle secret key VKi and group secret key HtSK is undisclosed.

However, it *may happen that the attack is internal and a malicious group member can obtain the VIDi of some other member by using group secret key HtSK to XOR the message broadcasted by Vi during communication.*

Moreover, if two malicious group members, Va and Vb, share their secret keys, VKa and VKb, they can break the system by computing (VKa- VKb). The whole equation, when known and unknown quantities are separated comes of form df = k3 * Ø (n). Accordingly they can figure out Ø(n) by setting k3 to a proper value. This *makes the secret keys in the system insecur*e. Thus, the system is broken.

2) **More processing delay for authentication at sender and receiver.**
Due to more number of complex computations during authentication phase, the processing delay is quite large. To overcome this, we *propose a scheme 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 the schemes used in Li's paper(blind signature and digital signature algorithm).

3) **Computational and Communicational overheads** List of revoked vehicles must be continuously updated and broadcasted to all nodes, this leads to computational complexities.

Proposal Description:

Following modifications are proposed to the authentication phase of Li's paper that is the pre-deployment phase(when the vehicles and RSU are given IDs):

1) The vehicles shall register themselves with transport authorities. This will be an offline process generating the necessary information for vehicular nodes and the service providers to form a secure VANET environment.(similar to TTP process in the aforementioned paper)

2) After vehicle registration, the transport authority shall deploy RSUs at each road section. The RSU should also be registered with the TA and its public key shall be conveyed to all the registered vehicles.

3) When a vehicle's range reaches an RSU, the vehicle sends a request to the RSU to provide a temporary identity. After verifying the vehicle's credential, the RSU will generate the temporary ID for the vehicle and use it for generating and sending transfer messages.

4) During the message transfer phase, this temporary ID is used as the identity of the vehicle instead of the real vehicle identity(in this way the anonymity of the vehicle is preserved). Even if the VID gets disclosed and becomes known to a group member, the temporary id is only valid in a particular range. Also each temporary ID is associated with

a timestamp, hence they generally expire after establishing one successful connection.

5) There are generally two type of scenarios. First case is when the destination is within the range of both source and RSU and the other when destination is not within the range of source but is within the range of RSU. In the second scenario, we have to use intermediate vehicle to achieve communication process by broadcasting message from the corresponding RSU.
The rest 3 scenarios proposed in Li's paper can remain the same, using this temporary id as the replacement for VID.

Analysis of Proposed scheme and Comparison:

1)In terms of computational costs, computation is decreased in the authentication phase by reducing the number of asymmetric operations. 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. 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.

2) The above proposed scheme also satisfies the anonymity property. hence, it is more secure than all of the other proposed protocols..

3) 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.

4)Communication Computational costs: 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.

5) The proposed protocol as well as Li's paper do implement conditional

privacy-preserving authentication. It enables a trusted third party (such as police officers) to retrieve a vehicle's real identity from its pseudo identity. If this feature is not provided, anonymous authentication can only prevent an outside attack, but cannot deal with an inside one. Furthermore, the system should not only provide safety message traceability to prevent insider attacks, but also have reasonable overheads for revealing the identity of a message sender.

References:

1) http://dspace.nitrkl.ac.in/dspace/bitstream/2080/1606/1/mavan.pdf
2) http://eprint.iacr.org/2010/028.pdf
3) http://cdn.intechopen.com/pdfs/32070/InTech-Anonymous_authentication_protocols_for_vehicular_ad_hoc_networks_an_overview.pdf
4) Chun-Ta Li, Min-Shiang Hwang, Yen-Ping Chu: A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. Computer Communications 31(12): 2803-2814 (2008)
5) Anup Kumar Bhattacharya, Abhijit Das, Dipanwita Roy Chowdhury, Arvind Iyer and Debojyoti Bhattacharya, Autonomous certification with list-based revocation for secure V2V communication, 8th International Conference on Information Systems Security (ICISS 2012), Lecture Notes in Computer Science, Vol. 7671, Springer-Verlag, pp 208-222, Dec 15-19, Guwahati, India.
6) http://en.wikipedia.org/wiki/Blind_signature
7) http://en.wikipedia.org/wiki/VANET