3

Anonymous Authentication Protocols for Vehicular Ad Hoc Networks: An Overview

Hu Xiong, Zhi Guan, Jianbin Hu and Zhong Chen
Key Laboratory of Network and Software Security Assurance of the Ministry of Education, Institute of Software, School of Electronics Engineering and Computer Science, Peking University
P. R. China

1. Introduction

According to car crash statistics, over six million motor vehicle crashes occur on U.S. highways each year. More than 42,000 people are killed in these accidents which injure three million others, and cost more than $230 billion each year. Astonishingly, five people die every hour in these crashes in the United States which is about one death every 12 minutes IVI (2001). In order to alleviate the threats of these crashes and improve the driving experience, car manufactures and the telecommunication industry have made great efforts to equip each vehicle with wireless devices that allow vehicles to communicate with each other as well as with the roadside infrastructure located in critical points of the road, such as intersections or construction sites. Misener (2005); VII (2011). Technologies built on 802.11p and IEEE 1609 standards, 5.9 GHz Dedicated Short Range Communications (DSRC) protocols [1] DSRC (1999), are proposed to support these advanced vehicle safety applications such as secure and effective vehicle-to-vehicle (V2V) (also known as Inter-Vehicle Communica- tion (IVC)) and vehicle-to-infrastructure (V2I) communications, which are also known as Vehicle Safety Communications (VSC) technologies. As shown in Fig. 1, the wireless communication devices installed on vehicles, also known as onboard units (OBUs), and the roadside units (RSUs), form a self-organized Vehicular Ad Hoc Network (VANET) Lin (2008); Sun (2007). 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. Thus, an increasing interest has been raised recently on the VANETs-based applications Bishop (2000), aiming to improve driving safety and traffic management by the method of providing drivers and passengers with Internet access.

Due to the open broadcasting of wireless communications and the high-speed mobility of the vehicles, extensive research efforts have been launched by academic institutions and industrial research labs several years ago to investigate key issues in VANETs, especially

[1] The United States Federal Communications Commission (FCC) has allocated in the USA 75MHz of spectrum in the 5.9GHz band for DSRC and the European Telecommunications Standards Institute (ETSI) has allocated in the Europe 30 MHz of spectrum in the 5.9GHz band for Intelligent Transportation Systems in October 1999 and August 2008, respectively

security and privacy preservation for mobile vehicles Calandriello *et al.* (2007); Chen *et al.* (2011); Daza *et al.* (2009); Hubaux *et al.* (2004); Kamat *et al.* (2006); Kounga *et al.* (2009); Li *et al.* (2008); Lin *et al.* (2007; 2008a;b); Lu *et al.* (2008; 2009; 2010); Mak *et al.* (2005); Plöβl & Federrath (2008); Raya & Hubaux (2005; 2007); Sun *et al.* (2007; 2010a;b); Wasef *et al.* (2010); Wang *et al.* (2008); Wu *et al.* (2010); Xu *et al.* (2007); Xi *et al.* (2007; 2008); Xiong *et al.* (2010a;b); Zhang *et al.* (2008a;b). Obviously, any malicious behaviors of user, such as injecting beacons 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.

It is natural to observe that achieving privacy and liability simultaneously is conflicting goal. On one aspect, a well-meaning OBU is willing to offer as much local information as possible to RSUs and other OBUs to create a safer driving environment so long as its locations cannot be tracked. And on the other, a misbehaving OBU may abuse the privacy protection mechanism to avoid legal responsibility when it involved in a dispute involving safety messages [2]attempts. Therefore, the *conditional privacy-preserving authentication* should be fulfilled in VANETs where a trusted authority can reveal the real identity of targeted OBU in case of a traffic event dispute, even though the OBU itself is not traceable by the public.

This chapter surveys the literature on privacy issues in VANETs from different perspectives, and thus provides researchers with a better understanding of this primitive. This chapter does not propose or advocate any specific anonymous authentication mechanisms. Even though some sections might point out vulnerabilities in certain classes of authentication protocols, our purpose is not to criticize, but to draw attention to these problems so that they might be solved.

The remainder of this chapter is organized as follows. Section 2 presents attack model, security requirements and related VANETs network architecture. All previous privacy-preserving protocols for VANETs are classified in Section 3, together with the basic cryptographic primitives. An example of Ring-signature based anonymous authentication protocol based on bilinear pairing are given in Section 4. Section 5 discusses how to use the taxonomies. Section 6 concludes the paper by stating some possible future research directions.

2. Motivation

2.1 Attack model

According to Lin (2008); Lin *et al.* (2007); Raya & Hubaux (2005; 2007); Sun *et al.* (2007), several possible security attacks in VANETs have been defined and listed as follows:

- Fake information attack: The adversary may diffuse bogus messages to affect the behavior of others. For instance, in order to divert traffic from a given road, one may send a fake traffic jam message to the others.
- Message replay attack: The adversary replays the valid messages sent by a legitimate user some time before in order to disturb the traffic.

[2] A safety message reports on the state of the sender vehicle, e.g., its location, speed, heading, etc.

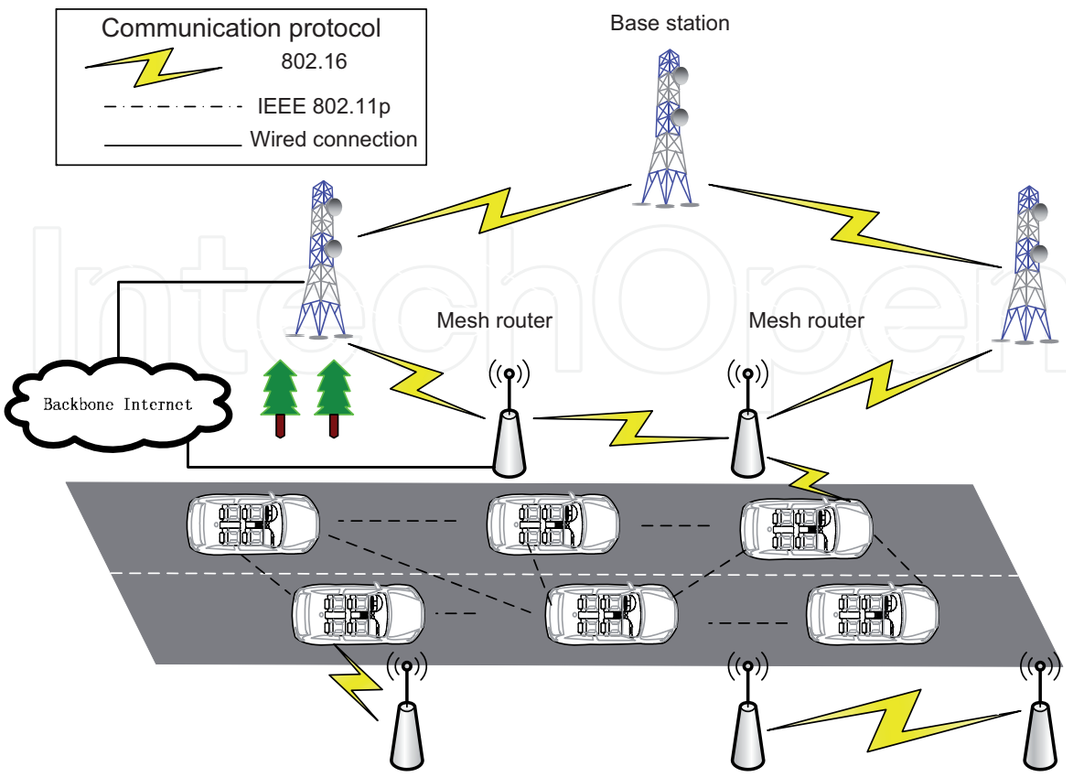


Fig. 1. Vehicular Ad Hoc Networks

- Message modification attack: A message is altered during or after transmission. The adversary may wish to change the source or content of the message in terms of the position and/or time information that had been sent and saved in its device notably in the case of an accident.
- Impersonation attack: The adversary may pretend to be another vehicle or even an RSU by using false identities to fool the others.
- RSU preemption/replication attack: An RSU may be compromised such that the adversary can relocate the compromised RSU to launch any malicious attack, such as broadcasting fake traffic information. Moreover, the adversary may illegally interrupt and manipulate traffic lights which is controlled by the corrupted RSU to get a better traffic condition
- Denial of service (DoS) attack: The adversary injects irrelevant jamming and aggressive dummy messages to take up the channels and consume the computational resources of the other nodes, such as RF interference or jamming or layer 2 packet flooding.
- Movement tracking: Since wireless communication is on an openly shared medium, an adversary can easily eavesdrop on any traffic. After the adversary intercepts a significant amount of messages in a certain region, the adversary may trace a vehicle in terms of its physical position and moving patterns simply through information analysis. Assuming that the attacker does not make use of cameras, physical pursuit, or onboard tracking devices to reveal the identity of his target; otherwise, the tracking problem becomes simpler but also more expensive and limited to few specific targets.

2.2 Security requirements

To countermeasure and mitigate the potential threats in the aforementioned attack models, a security system for safety messaging in a VANET should satisfy the following requirements.

1. *Efficient anonymous authentication of safety messages*: The security system should provide an *efficient* and *anonymous* message authentication mechanism. First of all, all accepted messages should be delivered unaltered, and the origin of the messages should be authenticated to guard against impersonation attacks. Meanwhile, from the point of vehicle owners, it may not be acceptable to leak personal information, including identity and location, to unauthorized observers while authenticating messages. Therefore, providing a secure yet anonymous message authentication is critical to the applicability of VANETs. Furthermore, considering the limited storage and computation resource of OBUs, the authentication scheme should have low overheads for safety message verification and storage.
2. *Efficient tracking of the source of a disputed safety message*: An important and challenging issue in these conditions is enabling 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 inside attacks, but also have reasonable overheads for the revealing the identity of a message sender.
3. *Threshold authentication* Chen *et al.* (2011); Daza *et al.* (2009); Kounga *et al.* (2009); Wu *et al.* (2010): A message is viewed as trustworthy only after it has been endorsed by at least n vehicles, where n is a threshold. The threshold mechanism is a *priori* countermeasure that improves the confidence of other vehicles in a message. In addition, the threshold in the proposed scheme should be adaptive, that is to say, the sender can dynamically change the threshold according to the traffic context and scenarios.
4. *Confidentiality* Kamat *et al.* (2006); Li *et al.* (2008); Plöβl & Federrath (2008); Wang *et al.* (2008) Some research teams pointed out that the privacy of the communication content should be protected against unauthorized observers. While confidentiality of communicating message can be negligible in most cases, it is e.g. crucial for services subject to costs. Besides application data administrative messages like routing protocol information or messages containing cryptographic material, the cryptographic information held by participants or centralized instances should also be protected against unauthorized access.

2.3 Network model

Similar to previous work Calandriello *et al.* (2007); Chen *et al.* (2011); Daza *et al.* (2009); Hubaux *et al.* (2004); Kamat *et al.* (2006); Kounga *et al.* (2009); Li *et al.* (2008); Lin *et al.* (2007; 2008a;b); Lu *et al.* (2008; 2009; 2010); Mak *et al.* (2005); Plöβl & Federrath (2008); Raya & Hubaux (2005; 2007); Sun *et al.* (2007; 2010a;b); Wasef *et al.* (2010); Wang *et al.* (2008); Wu *et al.* (2010); Xu *et al.* (2007); Xi *et al.* (2007; 2008); Xiong *et al.* (2010a;b); Zhang *et al.* (2008a;b), the security system should include at least three types of entities: the top Trusted authority (TA), the immobile RSUs at the roadside, and the moving vehicles equipped with on-board units (OBUs).

- OBU: A vehicle can not join the VANETs unless it registers its own public system parameters and corresponding private key to the TA. The secret information such as

private keys to be used generates the need for a tamper-proof device in each vehicle. According to existing works, only the authorized parties can access to this tamper-proof device. OBUs are mobile and moving most of the time. When the OBUs are on the road, they regularly broadcast routine safety messages, such as position, current time, direction, speed, traffic conditions, traffic events. The information system on each vehicle aggregates and diffuses these messages to enable drivers form a better awareness of their environment (Fig. 2). The assumed communication protocol between neighboring OBUs (IVC) or between an OBU and a RSU (V2I) is 5.9 GHz Dedicated Short Range Communication (DSRC) DSRC (1999) IEEE 802.11p.

- RSU: The RSUs, which are subordinated by the TA, form a wireless multi-hop mesh network (mesh mode in WiMax) aiming to extend the wireless coverage and increase the network robustness and throughput. Some of these RSUs are connected to the backbone networks with wired connections or to the WiMax base stations with wireless connections. Vehicles and passengers can gain access to the Internet for a short moment when passing through any of the RSUs by communicating with it. Thus, the RSUs should be able to perform fast handoff in order to support basic Internet services such as e-mail and TCP applications. We remark that the handoff process should be predictive when the moving pattern and speed of the vehicle are given. In addition, the RSUs should work as gateways which also support the 802.11p protocol and can transform the safety messages broadcasted by the vehicles into IP packets. With the support from RSUs, the workload of the vehicles is reduced. Otherwise, the vehicles need to send multiple copies of safety messages in different formats: one to the other vehicles with 802.11p, and one to the base stations with 802.16e. Different from the vehicles, we assume that RSUs have neither computation and energy constraints nor buffer size constraints.
- TA: The TA is in charge of the registration of all RSUs and OBUs each vehicle is equipped with. The TA can reveal the real identity of a safety message sender by incorporating with its subordinate RSUs. To the end, the TA requires ample computation and storage capability, and the TA cannot be compromised and is fully trusted by all parties in the system.

The network dynamics are characterized by quasi-permanent mobility, high speed, and (in most cases) short connection times between neighboring vehicles or between a vehicle and a roadside infrastructure network access point.

3. Taxonomy of privacy-preserving authentication protocol for VANETs

3.1 RSU-based approach

Zhang *et al*.Zhang *et al.* (2008a;b) presented a novel RSU-aided message authentication scheme (RSUB), in which the RSUs are responsible for validating the authenticity of messages sent from vehicles and for sending the results back to peer vehicles. Compared to the solutions without support from RSUs, this kind of schemes enables lower computation and communication overheads for each vehicle. Independently, Lu *et al*. Lu *et al.* (2008) introduced another anonymous authentication protocol for VANETs based on generating on-the-fly short-lived anonymous keys for the communication between vehicles and RSUs. These keys enable fast anonymous authentication and conditional privacy. All of these schemes employ RSUs to assist vehicles in authenticating messages. To keep a centralized certificate issuer from

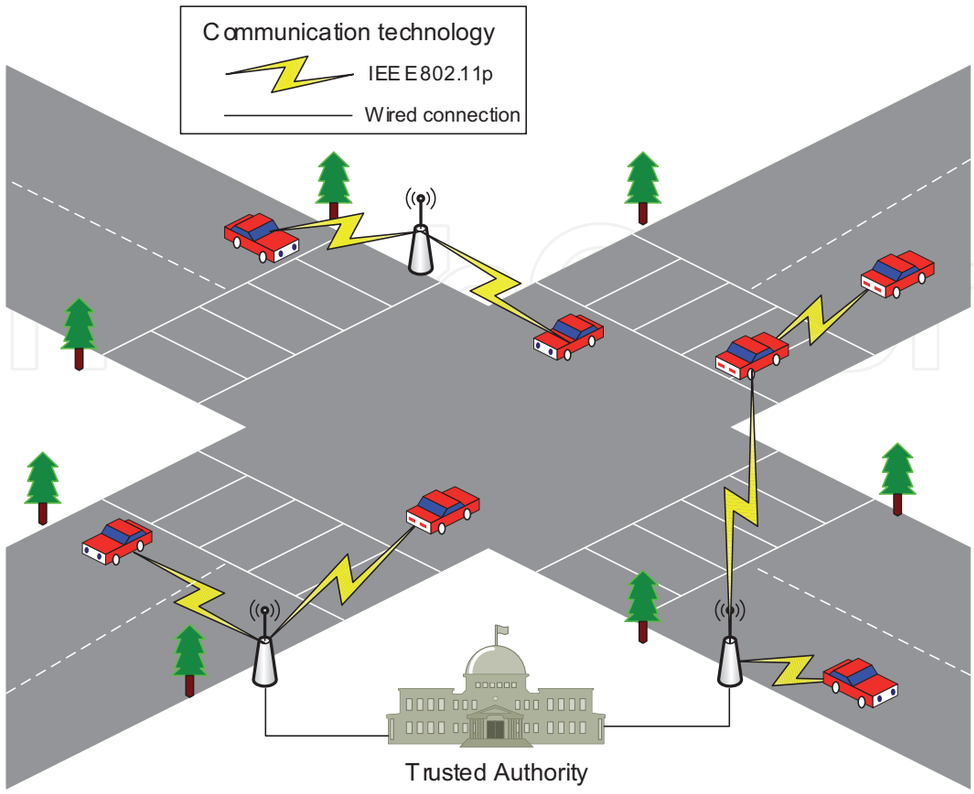


Fig. 2. VANETs Architecture

being a bottleneck, an RSU is allowed to issue certificates for the vehicles. However, it brings a privacy risk when an RSU is compromised by the adversaries. Once the service records of an RSU are leaked, it is easy for the adversary to link the pseudonymous certificates that a vehicle has obtained from the compromised RSU. In particular, when the number of compromised RSUs increases, it possibly provides a solution for the adversaries to revert the mobile trace of the target vehicles. However, relying on the roadside infrastructure for safety message authentication is a precarious solution: while these messages enable critical assisted driving features the roadside infrastructure will likely offer only partial coverage (for example during the deployment stage, for economic considerations, or simply due to physical damage).

3.2 Group-oriented signature-based approach

3.2.1 Group signature-based scheme

In Chaum & Hevst (1991), Chaum and Heyst proposed a new type of signature scheme for a group of entities, called group signatures. Such a scheme allows a group member to sign a message on the group's behalf such that everybody can verify the signature but no one can find out which group member provided it. However, there is a trusted third party, called the group manager, who can reveal the identity of the originator of a signature in the case of later dispute. This act is referred to as "opening" a signature or also as revocation of a signer's anonymity. The group manager can either be a single entity or a number of coalitions of several entities (e.g., group members). Dozens of group signature schemes Boneh *et al.*

(2004); Boneh & Shacham (2004); Chaum & Hevst (1991); Nakanishi & Funabiki (2005) have been proposed since 1991 due to its attractive features.

Lin *et al*. Lin *et al.* (2007; 2008a); Sun *et al.* (2007) proposed the group signature based (GSB) protocol, based on the efficient group signature Boneh *et al.* (2004). With GSB, each vehicle stores only a private key and a group public key. Messages are signed using the group signature scheme without revealing any identity information to the public. Thus privacy is preserved while the trusted authority is able to expose the identity of a sender. However, the time for safety message verification grows linearly with the number of revoked vehicles in the revocation list in the entire network. Hence, each vehicle has to spend additional time on safety message verification. Furthermore, when the number of revoked vehicles in the revocation list is larger than some threshold, the protocol requires every remaining vehicle to calculate a new private key and group public key based on the exhaustive list of revoked vehicles whenever a vehicle is revoked. Lin *et al*. Lin *et al.* (2007; 2008a); Sun *et al.* (2007) do not explore solutions to effectively updated the system parameters for the participating to vehicles in a timely, reliable and scalable fashion. This issue is not explored and represents an important obstacle to the success of this scheme.

3.2.2 Ring signature-based scheme

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. Spontaneity is a property which makes the distinction between ring signatures and group signatures Boneh *et al.* (2004); Chaum & Hevst (1991). Different from group signatures which allow the anonymity of a real signer in a group can be revoked by a group manager, the ring signature only gives the group manager the absolute power to control the formation of the group, and does not allow anyone to revoke the signer anonymity, while allowing the real signer to form a ring arbitrarily without being controlled by any other party. Since Rivest *el al.*'s scheme, many ring signature schemes have been proposed Abe *et al.* (2002); Bresson *et al.* (2002); Dodis *et al.* (2004); Wong *et al.* (2003); Xiong *et al.* (2009; 2011). In 2007, Liu *et al.* Liu *et al.* (2007) have introduced a new variant for the ring signature, called revocable ring signature. 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. In other words, the real signer will be responsible for what has signed as the anonymity is revocable by authorities while the real signer still has full freedom on ring formation.

To address the scalability concern in Lin *et al.* (2007), Xiong *et al.* Xiong *et al.* (2010a) proposed a spontaneous protocol based on the revocable ring signature Liu *et al.* (2007), which allows the vehicle to generate the message without requiring online assistance from the RSUs or the other vehicles. In this solution, the remaining vehicles are not required to update their system parameters regardless of the number of revoked vehicles. 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. Furthermore, Xi *et al.* Xi *et al.* (2007; 2008) also introduced a random key-set-based authentication protocol to preserve the vehicle’s privacy based on ring signature. However, this solution only provides unconditional anonymity without an effective and efficient mechanism to reveal message sender’s identities when necessary.

3.2.3 *k*-TAA-based scheme

In a *k*-times anonymous authentication (*k*-TAA) system Teranisi *et al.* (2004), participants are a group manager (GM), a number of application providers (AP) and a group of users. The GM registers users into the group and each AP independently announces the number of times a user can access his application. A registered user can then be anonymously authenticated by APs within their allowed numbers of times (*k* times) and without the need to contact the GM. Dishonest users can be traced by anyone while no one, even the GM or APs, can identify honest users or link two authentication executions performed by the same user. Finally no one, even the GM, is able to successfully impersonate an honest user to an AP. In *dynamic k*-TAA Nguyen & Safavi-Naini (2005), APs have more control over granting and revoking access to their services and so have the required control on their clients.

Sun *et al.* Sun & Fang (2009); Sun *et al.* (2010c) proposed a new misbehavior defense technique leveraging the idea of dynamic revocation, to provide a means of limiting the impact of misbehavior by adjusting it to an acceptable level during the vulnerable period existing in the automatic revocation technique based on *dynamic k*-TAA. However, the downside of Sun *et al.*'s scheme is obviously the lack of capability to trace misbehaving users.

3.3 Pseudonyms-based approach

3.3.1 Basic scheme

Raya *et al*.Raya & Hubaux (2005; 2007) introduced the large number of anonymous key based (LAB) protocol. Their key idea is to install on each OBU a large number of private keys and their corresponding anonymous certificates. To sign each launched message, a vehicle randomly selects one of its anonymous certificates and uses its corresponding private key. The other vehicles use the public key of the sender enclosed with the anonymous certificate to authenticate the source of the message. These anonymous certificates are generated by employing the pseudo-identity of the vehicles, instead of taking any real identity information of the drivers. Each certificate has a short life time to meet the drivers'privacy requirement. Although LAB protocol can effectively meet the conditional privacy requirement, it is inefficient and may become a scalability bottleneck. The reason is that a sufficient numbers of certificates must be issued to each vehicle to maintain anonymity over a significant period of time. (Raya *et al*.Raya & Hubaux (2005; 2007) suggest using *large pseudo* certificates for each vehicle). As a result, the certificate database to be searched by the TRC in order to match a compromised certificate to its owner's identity is huge. In addition, the protocols of Raya & Hubaux (2007) are extended for providing confidentiality in specific scenarios of VANET implementations in Wang *et al.* (2008).

3.3.2 TESLA-based scheme

TESLA is an efficient and message-loss tolerant protocol for broadcast authentication with low communication and computation overhead Perrig *et al.* (2002a). It is widely used in areas of sensor networks Perrig *et al.* (2002b). It uses one-way hash chain where the chain elements are the secret keys to compute message authentication code (MAC). With TESLA, a sender sends data packets at a predefined schedule, which has been known in advance to the receivers as well as the commitment to a hash chain as a key commitment. Each hash chain element as a MAC key corresponds to a certain time interval. For each packet, the sender attaches a

MAC tag to it. This MAC tag is derived using the next corresponding MAC key in the hash chain based on negotiated key disclosure delay schedule between the sender and the receiver. Obviously, upon receiving the packet, the receiver canąt verify the authenticity of the packet yet. After key disclosure delay, the sender discloses MAC key, and then the receiver is able to authenticate the message after verifying the released MAC key is indeed the corresponding element of the chain. One requirement for TESLA scheme is the loose synchronization among the nodes. The disadvantage is the delayed message authentication.

Lin *et al*. Lin *et al.* (2008b) developed the 'time-efficient and secure vehicular communication' scheme (TSVC) based on the Timed Efficient Stream Loss-tolerant Authentication (TESLA) standard (RFC 4082) Perrig *et al.* (2002a). With TSVC, a vehicle first broadcasts a commitment of hash chain to its neighbors and then uses the elements of the hash chain to generate a message authentication code (MAC) with which other neighbors can authenticate this vehicles' following messages. Because of the fast speed of MAC verification, the computation overhead of TSVC is reduced significantly. However, TSVC also requires a huge set of anonymous public/private key pairs as well as their corresponding public key certificates to be preloaded in each vehicle. Furthermore, TSVC may not be robust when the traffic becomes extremely dynamic as a vehicle should broadcast its key chain commitment much more frequently.

3.3.3 Proxy re-signature-based scheme

Proxy re-signature schemes, introduced by Blaze, Bleumer, and Strauss Blaze *et al.* (1998), and formalized later by Ateniese and Hohenberger Ateniese & Hohenberger (2005), allow a semi-trusted proxy to transform a delegateeąśs signature into a delegatorąśs signature on the same message by using some additional information. Proxy re-signature can be used to implement anonymizable signatures in which outgoing messages are first signed by specific users. Before releasing them to the outside world, a proxy translates signatures into ones that verify under a system's public key so as to conceal the original issuer's identity and the internal structure of the organization. Recently, Libert et al. Libert & Vergnaud (2008) have introduced the first *multi-hop unidirectional* proxy re-signature scheme wherein the proxy can only translate signatures in one direction and messages can be resigned a polynomial number of times.

The size of the certificate revocation list (CRL) and the checking cost are two important performance metrics for the revocation mechanism in VANETs. Unfortunately, the pseudonymous authentication schemes are prone to generating a huge CRL, whereas the checking cost in the group-signature-based schemes is unacceptable for the vehicles with limited computation power. Since the CRL is usually transmitted by vehicle-to-vehicle communication, the quick increase of the CRL in the pseudonymous authentication schemes brings large communication cost. Moreover, the larger the CRL size, the longer the transmission delay to all vehicles, and during this period, the misbehaving vehicles can compromise VANETs continually. Sun et al. Sun *et al.* (2010a;b) proposed an efficient authentication protocol which supports RSU-aided distribution certificate service that allows a vehicle to update its certificate set from an RSU on the road based on the proxy re-signature Libert & Vergnaud (2008). In their scheme, the vehicle only needs to request the re-signature keys from an RSU and re-sign numbers of the certificates issued by the TA to be the same as those issued by the RSU itself, and thus significantly reduces the revocation cost and the

certificate updating overhead. However, their scheme also rely on the RSUs which only cover partial high-way or city roads during the deployment stage.

3.3.4 Confidentiality-oriented scheme

The need for confidentiality in specific scenarios of VANET implementations has also been discussed in recent works Kamat *et al.* (2006); Li *et al.* (2008); Plöβl & Federrath (2008); Wang *et al.* (2008). Specifically in Wang *et al.* (2008), the protocols of Raya & Hubaux (2007) are extended: session keys for pairs of vehicles are established by using the Diffie-Hellman key agreement protocol while group session keys are established using the key transfer approach. These keys are used for both message authentication and confidentiality Wang *et al.* (2008). A lightweight authenticated key establishment scheme with privacy preservation and confidentiality to secure the communications in VANET is proposed by Li *et al.* Li *et al.* (2008). Meantime, two security frameworks for VANETs to provide authentication, confidentiality, non-repudiation and message integrity have also been proposed by Plöβl & Federrath (2008) and Kamat *et al.* (2006) independently. Nevertheless, all of these works Kamat *et al.* (2006); Li *et al.* (2008); Plöβl & Federrath (2008); Wang *et al.* (2008) suffer from the same criticism in LAB, in other words, each OBU has to take a large storage space to store a huge number of anonymous key pairs.

3.4 *Priori*-based approach

By taking strict punitive action, a *posteriori* countermeasures can exclude some rational attackers, but they are ineffective against irrational attackers such as terrorists. Even for rational attackers, damage has already occurred when punitive action is taken. To reduce the damage to a bare minimum, the *priori* countermeasures have been proposed to prevent the generation of fake messages. In this approach, a message is not considered valid unless it has been endorsed by a number of vehicles above a certain threshold.

3.4.1 Basic scheme

Most recently, Kounga *et al.* Kounga *et al.* (2009) proposed a solution that permits vehicles to verify the reliability of information received from anonymous origins. In this solution, each vehicle can generate the public/private key pairs by itself. However, the assumption in this solution is very restricted in that additional hardware is needed on the OBU. However, Chen and Ng Chen & Ng (2010) showd that the Kounga *et al.*'s scheme does not achieve the goals of authenticity of a message, privacy of drivers and vehicles, reliability of distributed information, and revocation of illegitimate vehicles.

After that, a proposal is also presented following the *priori* protection paradigm based on threshold signature by Daza *et al.* Daza *et al.* (2009). Nevertheless, to obtain the anonymity, this protocol assumes that the OBU installed on the vehicle can be removable and multi OBUs could alternatively be used with the same vehicle (like several cards can be used within a cell phone in the same time). Thus, this assumption may enable malicious adversary to mount the so-called Sybil attack: vehicles using different anonymous key pairs from corresponding OBUs can sign multiple messages to pretend that these messages were sent by different vehicles. Since multi OBUs can be installed on the same vehicle, no one can find out whether all of these signatures come from the same vehicle or not.

	Anonymous authentication	Traceability	Confidentiality	GSBS	RSUS	*Priori* -based	PBS
Zhang *et al.* (2008a;b)	✓	✓			✓		
Lu *et al.* (2008)	✓	✓			✓		
Lin *et al.* (2007; 2008a)	✓	✓		✓			
Sun *et al.* (2007)	✓	✓		✓			
Xiong *et al.* (2010a)	✓	✓		✓			
Xi *et al.* (2007; 2008)	✓			✓			
Sun & Fang (2009)	✓			✓			
Sun *et al.* (2010c)	✓			✓			
Raya & Hubaux (2005; 2007)	✓	✓					✓
Lin *et al.* (2008b)	✓	✓					✓
Sun *et al.* (2010a;b)	✓	✓		✓			✓
Li *et al.* (2008)	✓	✓	✓				✓
Plöβl & Federrath (2008)	✓	✓	✓				✓
Kamat *et al.* (2006)	✓	✓	✓				✓
Wang *et al.* (2008)	✓	✓	✓				✓
Kounga *et al.* (2009)[3]						✓	
Daza *et al.* (2009)	✓	✓				✓	
Wu *et al.* (2010)	✓	✓		✓		✓	

GSBS: Group-oriented signature based scheme; RSUS: RSU based scheme; PBS: Pseudonyms-based scheme

Table 1. Summary of related protocols

3.4.2 Group signature-based scheme

A linkable group signature Nakanishi *et al.* (1999) is a variant of group signatures. In a linkable group signature, it is easy to distinguish the group signatures produced by the same signer, even though the signer is anonymous. Linkable group signatures can thwart the Sybil attack but are not compatible with vehicle privacy due to the linkability of signer identities, i.e., the various message endorsements signed by a certain vehicle can be linked. Wu *et al.* Wu *et al.* (2010) proposed a novel protocol based on linkable group signature, which is equipped with both *priori* and *posteriori* countermeasures. However, they face the same adverse conditions in GSB protocol in which the verification time grows linearly with the number of revoked vehicles and every remaining vehicle need to update its private key and group public key when the number of revoked vehicles is larger than some threshold.

4. An example of ring-signature based anonymous authentication protocols

In order to be self-contained, we give an example of Ring-signature based authentication protocol along with the notion of bilinear pairing Xiong *et al.* (2010a) as follows.

4.1 Bilinear pairing

Note that the publication of an identity based encryption scheme Boneh & Franklin (2001) built on bilinear pairings has triggered a real upsurge in the popularity of pairings among

cryptographers. Following Boneh and Franklin, a lot of cryptosystems based on pairings have been proposed which would be hard to construct using more conventional cryptographic primitives. At this moment, pairing-based cryptography is a highly active field of research, with several hundreds of publications.

Let $\mathbb{G}_1$ denote an additive group of prime order q and $\mathbb{G}_2$ be a multiplicative group of the same order. Let P be a generator of $\mathbb{G}_1$, and $\hat{e}$ be a bilinear map such that $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ with the following properties:

1. Bilinearity: For all $P, Q \in \mathbb{G}_1$, and $a, b \in \mathbb{Z}_q$, $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.
2. Non-degeneracy: $\hat{e}(P, P) \neq 1_{\mathbb{G}_2}$
3. Computability: It is efficient to compute $\hat{e}(P, Q)$ for all $P, Q \in \mathbb{G}_1$

4.2 Ring-signature based

4.2.1 System initialization

Firstly, as described in section 2.3, we assume each vehicle is equipped with a tamper-proof device, which is secure against any compromise attempt in any circumstance. With the tamper-proof device on vehicles, an adversary cannot extract any data stored in the device including key material, data, and codes. We assume that there is a trusted Transportation Regulation Center (TRC) which is in charge of checking the vehicle's identity, and generating and pre-distributing the private keys of the vehicles. Prior to the network deployment, the TRC sets up the system parameters for each OBU as follows:

- Let $\mathbb{G}_1, \mathbb{G}_2$ be two cyclic groups of same order q. Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be a bilinear map.
- The TRC first randomly chooses $x_{TRC} \in_R \mathbb{Z}_q$ as its private key, and computes $y_{TRC} = x_{TRC}P$ as its public key. The TRC also chooses a secure cryptographic hash function $\mathcal{H} : \{0,1\}^* \rightarrow \mathbb{Z}_q$.
- Each vehicle V_i with real identity RID_i generates its public/private key pair as follows:
  - The vehicle V_i first chooses $x_i \in_R \mathbb{Z}_q$ as its private key, and computes $y_i = x_iP$ as its public key.
  - V_i randomly selects an integer $t_i \in_R \mathbb{Z}_q$ to determine the verification information of y_i: $a_i = \mathcal{H}(t_iP \parallel RID_i)$ and $b_i = (t_i + x_i \cdot a_i)$. Then V_i sends $\{y_i, RID_i, a_i, b_i\}$ to TRC.
  - After receiving $\{y_i, RID_i, a_i, b_i\}$, TRC checks whether the following equation holds:

$$a_i \stackrel{?}{=} \mathcal{H}((b_iP - a_iy_i) \parallel RID_i)$$

    If it holds, then $\{y_i, RID_i\}$ is identified as the valid public key and identity. Otherwise, it will be rejected. In the end, the TRC stores the (y_i, RID_i) in its records.
- Each vehicle is preloaded with the public parameters $\{\mathbb{G}_1, \mathbb{G}_2, q, y_{TRC}, \mathcal{H}\}$. In addition, the tamper-proof device of each vehicle is preloaded with its private/public key pairs (x_i, y_i) and corresponding anonymous certificates (these certificates are generated by taking the vehicle's pseudo-identity ID_i). Finally, the vehicle will preload the revocation list (RL) from the TRC.

4.2.2 OBU safety message generation

Vehicle V_π signs the message M before sending it out. Suppose $S = \{y_1, \cdots, y_n\}$ is the set of public keys collected by vehicle V_π and it defines the ring of unrevoked public keys. Note that the public key set S, collected and stored temporarily by V_π, is dynamic. We assume that all public keys y_i, $1 \leq i \leq n$ and their corresponding private keys x_i's are generated by TRC, and π ($1 \leq \pi \leq n$) is the index of the actual message sender. In other words, as V_π travels through the road network, the set of public keys collected by it keeps changing over time. Otherwise, a unique set of public keys used by a vehicle may enable the adversary to infer its traveling trajectory. The signature generation algorithm $Sig(S, x_\pi, y_{TRC}, M)$ is carried out as follows.

1. Randomly select $r \in_R \mathbb{Z}_q$ and compute $R = rP$.
2. For y_{TRC}, compute $E_{TRC} = \hat{e}(y_\pi, y_{TRC})^r$.
3. Generate a non-interactive proof $SPK(1)$ as follows: $SPK\{\alpha : \{E_{TRC} = \hat{e}(R, y_{TRC})^\alpha\} \bigwedge \{\bigvee_{i \in [1,n]} y_i = \alpha P\}\}(M)$. The signature σ of M with respect to S and y_{TRC} is (R, E_{TRC}) and the transcript of $SPK(1)$.

For clear presentation, we divide $SPK(1)$ into two components:

$$SPK\{\alpha : E_{TRC} = \hat{e}(R, y_{TRC})^\alpha\}(M), \tag{1a}$$

$$SPK\{\alpha : \bigvee_{i \in [1,n]} y_i = \alpha P\}(M). \tag{1b}$$

To generate a transcript of $SPK(1a)$, given E_{TRC}, R, y_{TRC}, the actual message sender indexed by π proves the knowledge of x_π such that $E_{TRC} = \hat{e}(R, y_{TRC})^{x_\pi}$ by releasing (s, c) as the transcript such that

$$c = \mathcal{H}(y_{TRC} \parallel R \parallel E_{TRC} \parallel \hat{e}(R, y_{TRC})^s E_{TRC}^c \parallel M)$$

This can be done by randomly picking $l \in_R \mathbb{Z}_q$ and computing

$$c = \mathcal{H}(y_{TRC} \parallel R \parallel E_{TRC} \parallel \hat{e}(R, y_{TRC})^l \parallel M)$$

and then setting $s = l - cx_\pi \bmod q$.

To generate the transcript of $SPK(1b)$, given S, the actual message sender indexed by π, for some $1 \leq \pi \leq n$, proves the knowledge of x_π out of n discrete logarithms x_i, where $y_i = x_i P$, for $1 \leq i \leq n$, without revealing the value of π. This can be done by releasing $(s_1, \cdots, s_n, c_1, \cdots, c_n)$ as the transcript such that $c_0 = \sum_{i=1}^n c_i \bmod q$ and

$$c_0 = \mathcal{H}(S \parallel s_1 P + c_1 y_1 \parallel \cdots \parallel s_n P + c_n y_n \parallel M).$$

To generate this transcript, the actual message sender first picks randomly $l \in_R \mathbb{Z}_q$ and $s_i, c_i \in_R \mathbb{Z}_q$ for $1 \leq i \leq n, i \neq \pi$, then computes
$c_0 = \mathcal{H}(S \parallel s_1 P + c_1 y_1 \parallel \cdots \parallel s_{\pi-1} P + c_{\pi-1} y_{\pi-1} \parallel lP \parallel s_{\pi+1} P + c_{\pi+1} y_{\pi+1} \parallel \cdots \parallel s_n P + c_n y_n \parallel M)$

Payload	Timestamp	Signature	Public Key Sets
100 bytes	4 bytes	40n+60 bytes	20n bytes

Table 2. Message Format for OBU

and finds c_π such that $c_0 = c_1 + \cdots + c_n \bmod q$. Finally the actual message sender sets $s_\pi = l - c_\pi x_\pi \bmod q$.

Now we combine the constructions of $SPK(1a)$ and $SPK(1b)$ together. First, the actual message sender randomly picks $l_1, l_2 \in_R \mathbb{Z}_q$ and $s_i, c_i \in_R \mathbb{Z}_q$ for $1 \leq i \leq n$, $i \neq \pi$, then computes

$$c = \mathcal{H}(S \parallel y_{TRC} \parallel R \parallel E_{TRC} \parallel \hat{e}(R, y_{TRC})^{l_1} \parallel s_1 P + c_1 y_1 \parallel \cdots \parallel s_{\pi-1} P + c_{\pi-1} y_{\pi-1} \parallel l_2 P \parallel s_{\pi+1} P + c_{\pi+1} y_{\pi+1} \parallel \cdots \parallel s_n P + c_n y_n \parallel M).$$

After that, the actual message sender sets $s = l_1 - c x_\pi \bmod q$, finds c_π such that $c = c_1 + \cdots + c_n \bmod q$, and sets $s_\pi = l_2 - c_\pi x_\pi \bmod q$. The transcript of $SPK(1)$ is therefore $(s, s_1, \cdots, s_n, c_1, \cdots, c_n)$.

According to DoT (2006), the payload of a safety message is 100 bytes. The first two fields are signed by the vehicle, by which the “signature" field can be derived. A timestamp is used to prevent the message replay attack. The last field is the public key sets, which records the public key pairs employed by the OBU. The format of messages in our protocol is defined in Table 2.

4.2.3 Message verification

Once a message is received, the receiving vehicle first checks if the $RL \bigcap S \stackrel{?}{=} \emptyset$. If so, the receiver performs signature verification by verifying of $SPK(1)$ as follows:

$$\sum_{i=1}^{n} c_i \stackrel{?}{=} \mathcal{H}(S \parallel y_{TRC} \parallel R \parallel E_{TRC} \parallel \hat{e}(R, y_{TRC})^s E_{TRC}^{\sum_{i=1}^{n} c_i} \parallel s_1 P + c_1 y_1 \parallel \cdots \parallel s_n P + c_n y_n \parallel$$

After that, the receiving vehicle updates its own public key set by randomly choosing public keys from S.

4.2.4 OBU fast tracing

A membership tracing operation is performed when solving a dispute, where the real ID of the signature generator is desired. The TRC first checks the validity of the signature and then uses its private key x_{TRC} and determines if

$$E_{TRC} \stackrel{?}{=} \hat{e}(y_i, R)^{x_{TRC}}$$

for some i, $1 \leq i \leq n$.

If the equation holds at, say when $i = \pi$, then the TRC looks up the record (y_π, RID_π) to find the corresponding identity RID_π meaning that vehicle with identity RID_π is the actual

message generator. The TRC then broadcasts the (y_π, RID_π) to all OBUs and each OBU adds the y_π into his local revocation list (RL).

4.2.5 Message verification

Once a message is received, the receiving vehicle V_j, one of the group G_{GNO}, uses his group's shared secret key κ_{GNO} to do the following with ciphertext (C_1, C_2):

1. Recover the session key $k_s \leftarrow b_1/(b_0)^{\kappa_{GNO}}$.
2. Decrypt $D_{k_s}(C_2) = M\|\sigma\|GNO$ with the session key k_s, where $D_{k_s}(\cdot)$ denotes a symmetric decryption with key k_s and $\sigma = (c, s_1, s_2, s_3, s_4, T_1, T_2, T_3)$.
3. Check whether $c \in \{0,1\}^k$, and $s_1 \in_R \pm\{0,1\}^{\epsilon(\gamma_2+k)+1}$, $s_2 \in_R \pm\{0,1\}^{\epsilon(\lambda_2+k)+1}$, $s_3 \in_R \pm\{0,1\}^{\epsilon(\lambda_1+2l_p+k+1)+1}$, and $s_4 \in_R \pm\{0,1\}^{\epsilon(2l_p+k)+1}$ and $T_1, T_2, T_3 \in \mathbb{Z}_n$.
4. Accept the signature if and only if $c = \mathcal{H}(g\|h\|y\|a_0\|a\|T_1\|T_2\|T_3\|d_1'\|d_2'\|d_3'\|d_4'\|M\|C_1)$ where d_1', d_2', d_3', d_4' are computed by the following equations: $d_1' = a_0^c T_1^{s_1 - c2^{\gamma_1}} / (a^{s_2 - c2^{\lambda_1}} y^{s_3}) \mod n$, $d_2' = T_2^{s_1 - c2^{\gamma_1}} / g^{s_3} \mod n$, $d_3' = T_2^c g^{s_4} \mod n$, $d_4' = T_3^c g^{s_1 - c2^{\gamma_1}} h^{s_4} \mod n$.

4.2.6 OBU fast tracing

A membership tracing operation is performed when solving a dispute, where the real ID_i of the signature generator is desired. The MM first decrypts (T_1, T_2) in a decrypted C_2 message to find the membership certificate A_i as follows:

1. Recover $A_i = T_1/T_2^x$.
2. Prove that $log_g y = log_{T_2}(T_1/A_i \mod n)$.

Then the MM looks up the record (A_i, ID_i) to find the corresponding identity ID_i meaning that vehicle with identity ID_i is the actual message generator. The MM then broadcasts the (A_i, ID_i) to all OBUs and each OBU adds the ID_i into his local revocation list (RL).

5. Using the taxonomies

In designing the above taxonomies, we selected those components and approach of existing mechanisms that, in our opinion, offer critical information regarding design philosophy and security properties. How can these taxonomies be used?

- *A map of anonymous authentication protocols for VANETs*. For novice researchers, these taxonomies offer a comprehensive overview for a quick introduction to this field. Experienced researchers can use and extend these taxonomies to structure and organize their knowledge in the field.
- *Exploring new strategies*. Besides the existing mechanisms, the taxonomy explored a few strategies seen rarely in the wild and some novel methods.
- *Understanding solution constrains*. The taxonomy highlights common constraints and weaknesses for each class of mechanisms. Understanding these problems will focus research efforts on solving them.
- *Identifying unexplored research areas*. Examining the effectiveness of different mechanism classes achieving different security properties will highlight unexplored venues for research.

6. Conclusion

The anonymous authentication protocols for VANETs can be constructed based on a multitude of cryptographic primitives, which obscures a global view of this field. This chapter is an attempt to cut through the obscurity and structure the knowledge in this field. The proposed taxonomies are intended to help the community think about the constrains of existing works and the possible countermeasures.

7. Acknowledgements

This work is partially supported by National Natural Science Foundation of China under Grant No. 61003230, China Postdoctoral Science Foundation under Grant No. 20100480130, Chongqing Key Lab of Computer Network and Communication Technology under Grant No. CY-CNCL-2010-01 and National Research Foundation for the Doctoral Program of Higher Education of China under Grant No. 200806140010.

8. Nomenclature

Notations	Descriptions
TA:	**T**rusted **A**uthority
OBU:	**O**n**B**oard **U**nit
RSU:	**R**oad**S**ide **U**nit
VANETs:	**V**ehicular **A**d Hoc **Net**works
DSRC:	**D**edicated **S**hort **R**ange **C**ommunications
V2V:	**V**ehicle-to-**V**ehicle
IVC:	**I**nter-**V**ehicle **C**ommunication
FCC:	**F**ederal **C**ommunications **C**ommission
ETSI:	**E**uropean **T**elecommunications **S**tandards **I**nstitute
VSC:	**V**ehicle **S**afety **C**ommunications
DoS:	**D**enial **o**f **s**ervice
TESLA:	**T**imed **E**fficient **S**tream **L**oss-tolerant **A**uthentication
MAC:	**M**essage **A**uthentication **C**ode
CRL:	**C**ertificate **R**evocation **L**ist
TSVC:	**T**ime-efficient and **S**ecure **V**ehicular **C**ommunication

Table 3. Notations

9. References

M. Abe, M. Ohkubo, K. Suzuki. (2002). 1-out-of-n signatures from a variety of keys, In *Proc. ASIACRYPT 2002*, New Zealand, Lecture Notes in Computer Science, 2501, Springer-Verlag, pp.415 432.

G. Ateniese, S. Hohenberger. (2005). Proxy Re-Signatures: New Definitions, Algorithms, and Applications, In: *ACM Conference on Computer and Communications Security (CCS 2005)*, pp. 310-319.

R. Bishop. (2000). A survey of intelligent vehicle applications worldwide, in *Proceedings of the IEEE Intelligent Vehicles Symposium 2000*, Dearborn, MI, USA, Oct. pp. 25-30.

M. Blaze, G. Bleumer, M.Strauss. (1998). Divertible Protocols and Atomic Proxy Cryptography, In: *Nyberg, K. (ed.) EUROCRYPT 1998*, LNCS 1403, pp. 127-144. Springer.

D. Boneh and M. K. Franklin. (2001). Identity-Based Encryption from the Weil Pairing, in: *CRYPTO 2001*, LNCS 2139, pp. 213-229. Springer. SIAM Journal of Computing, Vol. 32, No. 3, pp. 586-615, 2003.

D. Boneh, X. Boyen, H. Shacham. (2004). Short group signatures, In: Franklin, M.K. (ed.) CRYPTO 2004. vol 3152 of LNCS, pp. 227-242, Springer, Heidelberg.

D. Boneh and H. Shacham. (2004). Group signatures with verifier-local revocation, in *Proc. ACM CCS' 04*, pp. 168-177.

E. Bresson, J. Stern, M. Szydlo. (2002). Threshold ring signatures and applications to ad-hoc groups, In *Proc. CRYPTO 2002*, USA, Lecture Notes in Computer Science, 2442, Springer-Verlag, pp.465 480.

G. Calandriello, P. Papadimitratos, J.-P. Hubaux, A. Lioy. (2007). Efficient and robust pseudonymous authentication in VANET, *Vehicular Ad Hoc Networks* pp. 19-28.

D. Chaum, E. van Hevst. (1991). Group Signature, In *EUROCRYPT 1991*,volume 547 of LNCS, pp. 257-265.

L. Chen and S. Ng. (2010). Comments on "Proving Reliability of Anonymous Information in VANETs" by Kounga *et al*., IEEE Transactions on Vehicular Technology, Vol. 59, No. 3, pp. 1503-1505.

L. Chen, S.-L. Ng and G. Wang. (2011). Threshold anonymous announcement in VANETs. IEEE Journal on Selected Areas in Communications, Vol. 29, No. 3, pp. 605-615.

V. Daza, J. Domingo-Ferrer, F. Sebé, and A. Viejo. (2009). Trustworthy Privacy-Preserving Car-Generated Announcements in Vehicular Ad Hoc Networks", *IEEE Transactions on Vehicular Technology*, vol. 58, no. 4, pp. 1876-1886.

Y. Dodis, A. Kiayias, A. Nicolosi, V. Shoup. (2004). Anonymous identification in ad doc groups, In *Proc. EUROCRYPT 2004*, Switzerland, LNCS 3027, Springer-Verlag, pp.609 626, Full version: http://www.cs.nyu.edu/ nico-lo-si/pa-pers/

U.S. Department of Transportation. (2006). National Highway Traffic Safety Administration, *Vehicle Safety Communications Project*, Final Report. Appendix H: WAVE/DSRC Security.

Dedicated Short Range Communications (5.9 GHz DSRC), Available: http://www.leearmstrong.com/DSRC/DSRCHomeset.htm

J.P. Hubaux, S. Capkun, L. Jun. (2004). The Security and Privacy of Smart Vehicles, *IEEE Security & Privacy Magazine*, Vol. 2, No. 3, pp. 49-55.

Saving Lives Through Advanced Vehicle Safety Technology: Intelligent Vehicle Initiative Final Report. [Online]. Available: http://www.itsdocs.fhwa.dot.gov/JPODOCS/REPTS_PR/14153_files/ivi.pdf

P. Kamat, A. Baliga, W. Trappe. (2006). An Identity-Based Security Framework For VANETs, *VANETąŕ06*, pp. 94-95.

G. Kounga, T. Walter, and S. Lachmund. (2009). Proving Reliability of Anonymous Information in VANETs, *IEEE Transactions on Vehicular Technology*, vol. 58, no. 6, pp. 2977-2989.

C.-T. Li, M.-S. Hwang, Y.-P. Chu. (2008). A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks, *Computer Communications*, Vol. 31, pp. 2803-2814.

B. Libert, D. Vergnaud. (2008). Multi-Use Unidirectional Proxy Re-Signatures, *ACM Conference on Computer and Communications Security (CCS 2008)*, Alexandria, Virginia, USA.

D. Y. W. Liu, J. K. Liu, Y. Mu, W. Susilo, D.S. Wong. (2007). Revocable Ring Signature, *J. Comput. Sci. Technol.* 22(6): pp. 785-794.

X. Lin. (2008). Secure and Privacy-Preserving Vehicular Communications, PhD thesis, University of Waterloo, Waterloo, Ontario, Canada.

X. Lin, X. Sun, P.-H. Ho and X. Shen. (2007). GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications, *IEEE Transactions on Vehicular Technology*, vol. 56(6), pp. 3442-3456, 2007.

X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho and X. Shen. (2008a). Security in Vehicular Ad Hoc Networks, *IEEE Communications Magazine*, vol. 46, no. 4, pp. 88-95, 2008.

X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho and X. Shen. (2008b). TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving, *IEEE Transactions on Wireless Communications*, vol. 7, no. 12, pp. 4987-4998.

R. Lu, X. Lin, H. Zhu, P.-H. Ho and X. Shen. (2008). ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications, *The 27th IEEE International Conference on Computer Communications (INFOCOM 2008)*, Phoenix, Arizona, USA.

R. Lu, X. Lin, H. Zhu, and X. Shen. (2009). SPARK: A New VANET-based Smart Parking Scheme for Large Parking Lots, *The 28th IEEE International Conference on Computer Communications (INFOCOM 2009)*, Rio de Janeiro, Brazil.

R. Lu, X. Lin, and X. Shen. (2010). SPRING: A Social-based Privacy-preserving Packet Forwarding Protocol for Vehicular Delay Tolerant Networks, *The 29th IEEE International Conference on Computer Communications (INFOCOM 2010)*, San Diego, California, USA.

T. K. Mak, K. P. Laberteaux and R. Sengupta. (2005). A Multi-Channel VANET Providing Concurrent Safety and Commercial Services, in *Proceedings of 2nd ACM International Workshop on Vehicular Ad Hoc Networks*, Cologne, Germany, Sep. pp. 1-9.

J. A. Misener. (2005). Vehicle-infrastructure integration (VII) and safety, *Intellimotion*, Vol. 11, No. 2, pp. 1-3.

T. Nakanishi, T. Fujiwara, and H. Watanabe. (1999). A linkable group signature and its application to secret voting, Transactions of Information Processing Society of Japan, vol. 40, no. 7, pp. 3085-3096.

T. Nakanishi and N. Funabiki. (2005). Verifer-local revocation group signature schemes with backward unlinkability from bilinear maps, in *Proc. ASIACRYPT' 05*, LNCS, vol. 3788, pp. 533-548.

L. Nguyen, R. Safavi-Naini. (2005). Dynamic *k*-times anonymous authentication, in *ACNS 2005*, LNCS 3531, pp. 318-333.

A. Perrig, R. Canetti, J. D. Tygar, D. Song. (2002). The TESLA Broadcast Authentication Protocol, RSA CryptoBytes, vol. 5, no. 2, pp. 2-13.

A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar. (2002). Spins: security protocols for sensor networks, Wireless Networks, vol. 8, no. 11, pp. 521-534.

K. Plöβl, H. Federrath. (2008). A privacy aware and efficient security infrastructure for vehicular ad hoc networks, *Computer Standards & Interfaces*, Vol. 30, pp. 390-397.

M. Raya, J. P. Hubaux, (2005). The security of vehicular ad hoc networks, *3rd ACM workshop on Security of ad hoc and sensor networks*, pp. 11-21.

M. Raya and J. P. Hubaux. (2007). Securing Vehicular Ad Hoc Networks, *Journal of Computer Security*, Special Issue on Security of Ad Hoc and Sensor Networks, Vol. 15, Nr. 1, pp. 39-68.

R. L. Rivest, A. Shamir, Y. Tauman. (2001). How to Leak a Secret, In *AsiaCrypt 2001*, volume 2248 of LNCS, pp. 552-565.

X. Sun, X. Lin, P. Ho. (2007). Secure Vehicular Communications Based on Group Signature and ID-Based Signature Scheme, *International Communications Conference (ICC 2007)*, Glasgow, Scotland, June 24-28.

X. Sun. (2007). Anonymous, secure and efficient vehicular communications, Master thesis, University of Waterloo, Waterloo, Ontario, Canada.

J. Sun, Y. Fang. (2009). Defense against misbehavior in anonymous vehicular ad hoc networks, Ad Hoc Networks (Special Issue on Privacy and Security in Wireless Sensor and Ad Hoc Networks), Vol. 7, No. 8, pp. 1515-1525.

Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su. (2010). A Secure and Efficient Revocation Scheme for Anonymous Vehicular Communications, *International Communications Conference (ICC 2010)*, Cape Town, South Africa.

Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su. (2010). An Efficient Pseudonymous Authentication Scheme With Strong Privacy Preservation for Vehicular Communications, *IEEE Transactions on Vehicular Technology*, Vol. 59, No. 7, pp. 3589-3603.

J. Sun, C. Zhang, Y. Zhang, Y. Fang. (2010). An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks, IEEE Transactions on Parallel and Distributed Systems, Vol. 21, No. 9, pp. 1227-1239.

I. Teranisi, J. Furukawa, and K. Sako. (2004). *k*-Times Anonymous Authentication, in *ASIACRYPT 2004*, Springer-Verlag, LNCS 3329, pp. 308-322.

Vehicle infrastructure integration. U.S. Department of Transportation, [Online]. Available: http://www.its.dot.gov/index.htm

A. Wasef, Y. Jiang, and X. Shen. (2010). DCS: An efficient distributed certificate service scheme for vehicular networks, IEEE Transactions on Vehicular Technology, vol. 59, no. 2, pp. 533-549.

G. Wang. (2004). Security Analysis of Several Group Signature Schemes. [Online]. Available: http://eprint.iacr.org/2003/194

N. W. Wang, Y. M. Huang, and W. M. Chen. (2008). A novel secure communication scheme in vehicular ad hoc networks, *Computer Communications*, Vol. 31, pp. 2827-2837.

D. S. Wong, K. Fung, J. Liu, V. Wei. (2003). On the RS-code construction of ring signature schemes and a threshold setting of RST, In *Proc. 5th Int. Conference on Infoation and Communication Security (ICICS 2003)*, China, Lecture Notes in Computer Science, 2836, Springer-Verlag, pp.34 46.

Q. Wu, J. Domingo-Ferrer, and Úrsula González-Nicolás. (2010). Balanced Trustworthiness, Safety, and Privacy in Vehicle-to-Vehicle Communications, *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 559-573.

Q. Xu, T. Mak, J. Ko and R. Sengupta. (2007). Medium Access Control Protocol Design for Vehicle-Vehicle Safety Messages, *IEEE Transactions on Vehicular Technology*, Vol. 56, No. 2, pp. 499-518.

Y. Xi, K. Sha, W. Shi, L. Scnwiebert, and T. Zhang. (2007). Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks, *Eighth International Symposium on Autonomous Decentralized Systems (ISADS'07)*, pp. 344-351.

Y. Xi, W. Shi, L. Schwiebert. (2008). Mobile anonymity of dynamic groups in vehicular networks, *Security and Communication Networks*, Vol. 1, No.3, pp. 219-231.

H. Xiong, Z. Qin, F. Li. (2011). Identity-based Ring Signature Scheme based on quadratic residues, High Technology Letters, Vol. 15, No.1, pp. 94-100.

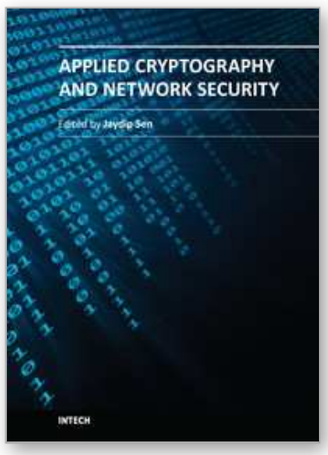
H. Xiong, K. Beznosov, Z. Qin, M. Ripeanu. (2010). Efficient and Spontaneous Privacy-Preserving Protocol for Secure Vehicular Communication, *International Communications Conference (ICC 2010)*, Cape Town, South Africa.

H. Xiong, Z. Qin, F. Li. (2010). Secure Vehicle-to-roadside communication protocol using certificate-based cryptosystem, IETE Technical Review, Vol 27, No 3, pp. 214-219.

H. Xiong, Z. Qin, F. Li. (2011). A Certificateless Proxy Ring Signature Scheme with Provable Security, International Journal of Network Security, Vol.12, No.2, pp.113-127.

C. Zhang, X. Lin, R. Lu and P.-H. Ho. (2008). RAISE: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks. IEEE International Conference on Communications (ICC'08), Beijing, China.

C. Zhang, X. Lin, R. Lu, P.-H. Ho and X. Shen. (2008). An Efficient Message Authentication Scheme for Vehicular Communications, *IEEE Transactions on Vehicular Technology*, vol. 57, no. 6, pp. 3357-3368.



Applied Cryptography and Network Security

Edited by Dr. Jaydip Sen

ISBN 978-953-51-0218-2
Hard cover, 376 pages
Publisher InTech
Published online 14, March, 2012
Published in print edition March, 2012

Cryptography will continue to play important roles in developing of new security solutions which will be in great demand with the advent of high-speed next-generation communication systems and networks. This book discusses some of the critical security challenges faced by today's computing world and provides insights to possible mechanisms to defend against these attacks. The book contains sixteen chapters which deal with security and privacy issues in computing and communication networks, quantum cryptography and the evolutionary concepts of cryptography and their applications like chaos-based cryptography and DNA cryptography. It will be useful for researchers, engineers, graduate and doctoral students working in cryptography and security related areas. It will also be useful for faculty members of graduate schools and universities.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen