Safety and Privacy in Vehicular Communications

Josep Domingo-Ferrer and Qianhong Wu

Universitat Rovira i Virgili,
UNESCO Chair in Data Privacy,
Dept. of Computer Engineering and Mathematics,
Av. Països Catalans 26, E-43007 Tarragona, Catalonia
{josep.domingo,qianhong.wu}@urv.cat

Abstract. Vehicular *ad hoc* networks (VANETs) will improve traffic safety and efficiency provided that car-to-car communication stays trustworthy. Therefore, it is crucial to ensure that the information conveyed by vehicle-generated messages is reliable. A sensible option is to request that the content of a message originated by a certain vehicle be endorsed by nearby peer vehicles. However, neither message generation nor message endorsement should entail any privacy loss on the part of vehicles co-operating in it. This chapter surveys the available solutions to this security-privacy tension and analyzes their limitations. A new privacy-preserving system is sketched which guarantees message authentication through both *a priori* and *a posteriori* countermeasures.

Keywords: Vehicular *ad hoc* networks, Privacy, Trust, Car-to-car messages.

1 Introduction

According to recent technology forecasts [5], vehicles will be equipped with radio interfaces in the near future and vehicle-to-vehicle (V2V) communications will be available in vehicles by 2011. The IEEE 802.11p task group is working on the Dedicated Short Range Communications (DSRC) standard which aims at enhancing the 802.11 protocol to support wireless data communications for vehicles and the road-side infrastructure [39]. Car manufacturers and telecommunication industry gear up to equip each car with devices known as On-Board Units (OBUs) that allow vehicles to communicate with each other, as well as to supply Road-Side Units (RSUs) to improve safety, traffic efficiency, driver assistance, and transportation regulation. The RSUs are expected to be located in the critical points of the road, such as traffic lights at road intersections. The OBUs and RSUs form a self-organized network called a vehicular *ad hoc* network (VANET), emerging as the first commercial instantiation of the mobile *ad hoc* networking (MANET) technology.

VANETs allow nodes including vehicles or road-side infrastructure units to communicate with each other over single or multiple hops. In other words, nodes will act both as end points and routers. Vehicular networking protocols allow vehicles to broadcast messages to other vehicles in the vicinity. It is suggested

C. Bettini et al. (Eds.): Privacy in Location-Based Applications, LNCS 5599, pp. 173–189, 2009.

that each vehicle periodically send messages over a single hop every 300ms within a distance of 10s travel time (which means a distance range between 10m and 300m)[35]. This mechanism can be used to improve safety and optimize traffic. However, malicious vehicles can also make use of this mechanism by sending fraudulent messages for their own profit or just to jeopardize the traffic system. Hence, the system must be designed to ensure that the transmission comes from a trusted source and has not been tampered with since transmission.

Another critical concern in VANETs is the privacy or anonymity of the driver (or the vehicle, for that matter). As noted in [10], a lot can be inferred about the driver if the whereabouts and the driving pattern of a car can be tracked. It is indeed possible for attackers to trace vehicles by using cameras or physical tracking, but such physical attacks can only trace specific targets and are much more expensive than monitoring the communication in VANETs. Hence, most studies focus on thwarting the latter attacks.

1.1 VANET Architecture

Since in VANETs vehicles periodically report their state information including their location-related information to other vehicles, it is natural to require the vehicles to be equipped with hardware allowing position information collection. Such type of hardware includes GPS or DGPS receivers, which additionally allow clock synchronization. These positioning systems are increasingly available in high-end vehicles. Sensors are another type of devices enabling vehicles to collect their state information including speed, temperature, direction, etc. These devices turn vehicles into potential information sources in view of improving traffic safety and efficiency.

Among the vehicle onboard equipment, some hardware modules are required to guarantee that the information collected has not been altered when sending it to other vehicles [34]. Typically, there are two modules, namely the Event Data Recorder (EDR) and the Tamper-Proof Device (TPD). The EDR only provides tamper-proof storage while the TPD also possesses cryptographic processing capabilities. The EDR is responsible for recording the critical data of the vehicle (such as position, speed, time, etc.) during emergency events, similar to the black box of an airplane. These data will help in accident reconstruction and liability attribution. Hence, if some investigation is later carried out, these messages can be extracted and used as evidences. EDRs are already installed in many road vehicles, *e.g.* trucks. TPD provides the ability to verify and sign messages. Compared with general CPUs, a TPD not only provides the ability for processing, but it also provides hardware protection so that it cannot be easily penetrated by anyone who is not authorized to do so. The TPD stores all the cryptographic material and performs cryptographic operations, especially signing and verifying safety messages. By binding secret cryptographic keys with a given vehicle, the TPD guarantees the accountability property as long as it remains inside the vehicle. However, TPDs suffer from a high cost for mass deployment and can currently only be expected in high-end vehicles.

VANETs can be viewed as a special kind of mobile *ad hoc* networks. VANET-enabled vehicles are equipped with radio interface for the purpose of forming short-range wireless *ad hoc* networks. In the United States, the Federal Communications Commission has allocated a licensed frequency band of about 75MHz in the 5.8/5.9GHz band specifically for VANETs, usually referred to as DSRC (Dedicated Short Range Communications) [39]. Similar bands have been allocated in Japan and Europe. The MAC layer protocol is either a modified version of 802.11 WLAN or the 3G protocol extended for decentralized access. The original 802.11 protocol is not suitable for VANETs due to the high mobility and highly dynamic topology. A modified version referred to as 802.11p is being developed by the IEEE group for VANETs. The 3G protocol is designed for centralized cellular networks and there have been efforts to enhance it with TDMA- and CDMA-based MAC protocols for decentralized access [27].

A difference between VANETs and generic mobile *ad hoc* networks is that centralized authorities are expected in most VANETs. A conventional transportation regulation system (without VANETs) may involve vehicle manufacturers, a transportation regulation office, the traffic police, and judges. Hence, as suggested in existing schemes [20,26], it is reasonable to assume that those conventional entities have their corresponding electronic counterparts in a VANET. Such centralized authorities are responsible for enrolling vehicles, validating their identities, and issuing electronic certificates to vehicles. The authorities also take care of regular (*e.g.*, annual) health checks of vehicles. In case of serious traffic accidents, they may be involved in collecting electronic witnesses, reconstructing accidents, and tracing drivers. By collecting vehicular communications, some authorities may play a role in optimizing traffic and relieving congestions.

In addition to the above centralized authorities, road-side infrastructure can be expected in vehicular *ad hoc* networks. These distributed road-side units are very useful in collecting vehicular communications and optimizing traffic, distributing and relaying safety-related messages, enrolling vehicles from other VANETs and so on. Depending on the designated roles of the road-side infrastructure, the existing proposals assume very diverse numbers and distributions of road-side units. Some proposals require base stations to be distributed evenly throughout the whole road network, others only at intersections, and others at region borders. Due to cost considerations, especially at the beginning it is unrealistic to require vehicles to always have wireless access to road-side base stations.

1.2 Potential Applications

VANETs have various potential applications including collision avoidance, accident investigation, driving assistance, traffic optimization, traffic regulation, vehicle-based infotainment and so on. Basically, the applications fall into three categories.

Traffic safety related applications. These applications are the main thrust behind VANETs. There are tens of thousands of deaths each year and hundreds of thousands of people get injured in traffic accidents all over the world. Safety related messages from a road-side unit to a vehicle could warn a driver when she/he enters an intersection. V2V communications can save many lives and prevent injuries. Some of the worst traffic accidents are due to many vehicles rear-ending each other after a single accident at the front of the line suddenly halts traffic. In this scenario, if a vehicle broadcasts a message about sudden braking to its neighbor vehicles and other receivers relay the message further, more drivers far behind will get an alarm signal before they see the accident and such type of serious traffic accidents could be avoided. VANETs can also provide driving assistance, *e.g.* violation warning, turn conflict warning, curve warning, lane merging warning etc., to avoid traffic accidents. Many of the accidents come from the lack of co-operation between drivers. By giving more information about the possible conflicts, many life-endangering accidents can be averted. Furthermore, given that vehicle state information and vehicular communications are accountable, VANETs can help in accident reconstruction and witness collection so that the injured and sacrificed can be compensated fairly in case of casualties.

Traffic optimization. With the increasing number of vehicles, people are experiencing more and more traffic delays during the rush hours. VANETs can greatly reduce traffic delays in several ways. Firstly, vehicles could serve as information source and transmit the traffic condition information for the vehicular network. Then transportation agencies could utilize this information to guide vehicles. This will finally relieve traffic congestion. Secondly, vehicles can also work as information collectors and collect data about weather or road surface conditions, construction zones, highway or rail intersections, emergency vehicle signal preemption, etc., and relay those data to other vehicles. Thirdly, the driving assistance provided by VANETs can also improve traffic efficiency. With that assistance, drivers can enjoy smooth and easy driving by avoiding possible conflicts. Finally, VANETs allow transportation administration authorities to manage vehicles electronically (*e.g.* speed control, permits, etc.), which is much more efficient than traditional manual administration.

Value-added services in VANETs. Since vehicles usually have sufficient computational capacity and power supply, complex protocols can be implemented to provide advanced services in VANETs. By implementing advanced electronic payment protocols [3] in VANETs, one can achieve the convenient and desirable goal of passing a toll collection station without having to reduce speed, wait in line, look for some coins and so on. As GPS systems have become available in many vehicles, it is also possible to realize location-based services in VANETs, for instance, finding the closest fuel station, restaurant, hotel, etc. Other kind of services include infotainment, vehicle-based electronic commerce and so on. All these services lead to a more comfortable driving experience and an easier life for drivers, although they are not the main purpose when designing VANETs.

1.3 Plan of the Rest of This Chapter

Section 2 describes the characteristics of the VANETs assumed in the subsequent sections. Section 3 reviews the countermeasures proposed in the literature to obtain secure and privacy-preserving VANETs. Section 4 discusses how to combine *a priori* and *a posteriori* countermeasures in order to overcome the shortcomings of proposals in the literature. Section 5 is a conclusion.

2 Characteristics of VANETs

In this section, we describe the VANET environment in which our scheme is assumed to be implemented.

2.1 Entities in a VANET

Typically, the following entities are present in a VANET:

- **Semi-trusted parties.** A conventional transportation regulation system (without VANETs) may involve vehicle manufacturers, a transportation regulation office, the traffic police, and judges. Hence, as suggested in existing schemes, it is reasonable to assume that those conventional entities have their corresponding electronic counterparts in a VANET. They all have respective secret/public key pairs. These public keys may be embedded into OBUs which are assumed to be tamper-proof. Unlike previous schemes, we adopt a weaker trust assumption that the parties cannot access the private keys of vehicles. A weaker assumption implies more robust systems against vehicle control by, say, organized criminals (for whom it will be harder to access the vehicle's private key).
- **Vehicles.** A VANET mainly consists of vehicles which periodically produce safety-related messages. OBUs and vehicles can be physically bound by embedding an OBU into each vehicle. The owner of a vehicle can also be bound to an OBU by some unique information such as a PIN or his/her unique biometric features. Ownership of a vehicle might be transferred by erasing existing personal information and recording a new one, along with a physical contract. Although the driver might not be the owner, it is the driver who fully controls the vehicle during driving. Hence, we interchangeably use the terms OBU, vehicle, owner and driver.
- **Infrastructures.** As commonly suggested, we assume that there exist centralized authorities and distributed units in a VANET. The centralized authorities can be implemented with the above semi-trusted parties. For instance, the manufacturers produce a signature to show that vehicle ownership is legally transferred to the buyer. With this signature, the vehicle can register to the administration office, and the police office and judges can co-operatively trace the vehicle. Road-side units are also part of the VANET infrastructure. Some power of the authorities can be distributed to road-side units to avoid a communication bottleneck.

- **Attackers.** Since the main security threats in VANETs are violations of public safety and vehicle privacy, we define an attacker to be an entity who wants to successfully cheat honest vehicles by spreading false information, or compromise the privacy of honest vehicles by monitoring the communications in VANETs. A group of maliciously colluding vehicles can also be viewed as an attacker who fully controls that group of vehicles. Attackers can be either internal (that is, VANET entities) or external. They can also be classified as rational or irrational: a rational attacker follows a rational strategy, in which the cost of attack should not be more than its expected benefit, whereas the strategy of an irrational attacker (*e.g.*, a suicide terrorist) cannot be predicted in those terms. Denial-of-service (DoS) is another class of attacks which has been extensively investigated and will not be dealt with here [1].

2.2 Security Requirements

In order to obtain an implementable system to enhance the trustworthiness in V2V communications by balancing public safety and vehicle privacy, we consider the following three types of security requirements:

- **Threshold authentication.** A message is viewed as trustworthy only after it has been endorsed by at least t vehicles, where t is a threshold. The threshold mechanism is an *a priori* countermeasure that improves the confidence of other vehicles in a message. In itself, the threshold does not stop malicious behavior, but makes it more difficult to succeed. Also, the authentication may provide arguments if such behavior occurs and must later be judged.
- **Anonymity.** There is anonymity if, by monitoring the communication in a VANET, message originators cannot be identified, except perhaps by designated parties. The goal is to protect the privacy of vehicles. Since message authentication requires knowledge of a public identity such as a public key or the licence plate, if no anonymity mechanism was provided, an attacker could easily trace any vehicle by monitoring the VANET communication. This would surely be undesirable for the drivers. However, it is possible for attackers to trace vehicles by using a physical approach, *e.g.*, assisted by a camera. But such physical attacks can only trace specific targets and they are much more expensive than attacks monitoring the communication in VANETs. The anonymity mechanism is intended to disable the latter attacks.
- **Revocability.** Revocability means that, if necessary, designated parties can identify the originator and the endorsers of any doubtable message. The goal here is to balance personal privacy and public safety. If anonymity is realized without any revocability mechanism, an attacker can anonymously broadcast authenticated wrong messages to fool other vehicles without fear of being caught, which may seriously compromise public safety. The revocability mechanism is an *a posteriori* countermeasure intended to fight this impunity situation.

2.3 Operational Features of VANETs

Considering the real world, we can assume semi-trusted parties to serve as centralized authorities for vehicle registration and administration. It is also possible to use some road-side units as distributed administration nodes. These administration units make centralized security infrastructures such as public key infrastructures (PKI) usable in VANETs.

The number of mobile nodes in VANETs can be extremely large. Each vehicle is allowed to broadcast messages to other vehicles in the vicinity. It is suggested that each vehicle periodically send messages over a single hop every 300ms within a range of 10s travel time [35]. This yields a minimum range of 10m and a maximum range of 300m, corresponding to the distance covered in 10s travel time. As a consequence, the vehicles are confronted with a large number of message-signature pairs to be verified. Hence, an authentication mechanism designed for VANETs must allow fast message verification.

Due to the road-bounded topology of vehicular networks, common *ad hoc* routing/forwarding strategies are well suited for data dissemination with minimal modifications. It is a reasonable assumption that the intended communication range of an emergency message be greater than the road width. Therefore, a message relayed along the direction of a road will cover all the road area up to destination. This mechanism can also be extended in case of scenarios with road junctions.

The nodes may move very fast at a relative speed up to 320km per hour (*e.g.* two vehicles driving at 160km/h crossing each other in opposite directions). The duration of the connection between mobile nodes may be very short, *e.g.*, less than three seconds. This implies that message-signature pairs should be short enough to be transmitted before the (very sporadic) communication ends.

Unlike the nodes of other types of MANETs which are limited in power and computation, the computation devices embedded in vehicles can be expected to have substantial computational capacity, storage space and power supply. This is the physical basis on which better security can be provided in VANETs.

3 Countermeasures for Securing VANETs

VANETs can improve traffic safety only if the messages sent by vehicles are trustworthy. Dealing with fraudulent messages is a thorny issue for safety engineers due to the self-organized operation of VANETs. The situation is further deteriorated by the privacy requirements of vehicles since, in a privacy-preserving setting, the message generators, *i.e.* the vehicles, are anonymous and cannot be identified when performing maliciously. A number of schemes have been proposed to reduce fraudulent messages; such proposals fall into two classes, namely *a posteriori* and *a priori*.

3.1 *A Posteriori* Countermeasures

A posteriori countermeasures consist in taking punitive action against vehicles which have been proven to have originated fraudulent messages. To be compatible with privacy preservation, these countermeasures require the presence of a trusted third party able to open the identities of dishonest vehicles. Then the identified vehicles can be removed from the system.

Cryptographic authentication technologies have been extensively exploited to offer *a posteriori* countermeasures. Some proposals use regular digital signatures [2,34,36,37] to enable tracing malicious vehicles. To make this approach work, a public key infrastructure (PKI) is suggested in VANETs [31,34,35,41]. These schemes do not provide any methods for certificate revocation. Although issues about revocation were discussed in [7,30,37], no complete solution was provided. To address the above problem in VANETs, [36] proposes three CA revocation protocols: Revocation using Compressed Certificate Revocation Lists (RC2RL), Revocation of the Tamper-Proof Device (RTPD), and Distributed Revocation Protocol (DRP). The RC2RL protocol employs a compression technique to reduce the overhead of distribution of the certificate revocation list. Instead of checking the CA status, The RTPD proposal removes revoked certificates from their corresponding certificate stores in the vehicles. To achieve this, they introduce a tamper-proof device as a vehicle key and certificate management tool. Unlike RC2RL and RTPD, a distributed CA revocation approach is suggested in DRP to determine the status of a certificate. In this case, each vehicle is equipped with an attacker detection system, which enables a vehicle to identify any compromised peer.

When multiple vehicles observe the same driving environment, to endorse the generated message they need to authenticate the same/similar message. This raises the issue of authentication of aggregated data. In [33], the authors propose ways to authenticate identical messages. Another way to deal with authentication of aggregated data is suggested in [32]. This proposal can also handle messages that are similar but not identical, and expects nodes receiving multiple messages with similar information to summarize the information in them using only syntactic aggregation.

A critical issue posed by vehicular message authentication is driver's privacy. Since the public key used to verify the authenticated messages can be linked to specific users, attackers can trace vehicles by observing vehicular communications. Hence, mechanisms must be adopted to guarantee vehicle/driver privacy when vehicles authenticate messages. Along this research line, there are two main approaches: pseudonymous mechanisms and group signatures.

In a pseudonymous mechanism, the certificate authorities produce multiple pseudonyms for each vehicle so that attackers cannot trace the vehicles producing signatures in different periods under different pseudonyms, except if the certificate authorities open the identities of the vehicles. The IEEE 1609.2 Draft Standard [22] proposes the distribution of short-lived certificates to enable vehicle privacy. In [36], the authors propose to use a set of anonymous keys that change frequently (say every couple of minutes) depending on the driving speed. Each key can be used only once and it expires after its usage; only one key can be used at a time. These keys are preloaded in the vehicle's tamper-proof device (TPD) for a long duration, *e.g.* until the next yearly checkup; the TPD takes care of all the operations related to key management and usage. Each key is certified by the issuing CA and has a short lifetime (*e.g.*, one specific week of the year). With the help of the CAs, the key can be tracked back to the real identity of the vehicle in case law enforcement necessitates this and only after obtaining a permission from a judge.

Pseudonym mechanisms have been extensively investigated from various aspects. Short-lived certificates are also suggested in [23], mainly from the perspective of how often a node should change a pseudonym and with whom it should communicate. The authors of [38] propose to use a silent period in order to hamper linkability between pseudonyms, or alternatively to create groups of vehicles and restrict vehicles in one group from hearing messages of other groups. In [19] a user can cloak information before sending it, by providing location information at a coarse granularity in terms of time and space. In [4] mix zones are studied to protect location privacy of location-based services. In [15] the integration of pseudonymity into a real VANET communication system is investigated, bringing together different aspects. Challenges include addressing concepts across layers of the protocol stack, issues in geographical routing (location service, forwarding), and cross layer information exchange, as well as problems related to implementation design and performance.

This conditional anonymity of pseudonymous authentication will help determining the liability of drivers in the case of accidents. The downside of this approach is the necessity for generation, delivery, storage, and verification of numerous of CAs for all the keys. To mitigate this heavy overhead, [7] presents an approach to enable vehicle on-board units to generate their own pseudonyms without interacting with the CAs. The mechanism is realized with the help of group signatures. In [20] a novel group signature-based security framework is proposed which relies on tamper-resistant devices (requiring password access) for preventing adversarial attacks on vehicular networks. However, they provide no concrete instantiation or experiment analysis.

In [26], the authors propose a security and privacy preserving protocol for VANETs by integrating the techniques of group signature and identity-based signature. In their proposal, they take into account security and privacy preservation between OBUs, as well as between OBUs and RSUs. In the former aspect, a group signature is employed to secure the communication between OBUs, where messages are anonymously signed by the senders while the identities of the senders can be traced by the trusted authorities if the messages are later found to be doubtable. In the latter aspect, an identity-based signature scheme is used at RSUs to sign each message generated by RSUs to ensure its authenticity. With their approach, the heavy load of certificate management can be greatly reduced.

Hubaux *et al.* [21] take a different perspective of VANET security and focus on privacy and secure positioning issues. They observe the importance of the tradeoff between liability and anonymity and also introduce Electronic License Plates (ELP) that are unique electronic identities for vehicles.

3.2 *A Priori* Countermeasures

VANETs can improve traffic safety and efficiency only if vehicular messages are correct and precise. Despite the security provided by the combination of TPDs with authenticated messages, an attacker could still manage to transmit valid messages containing false data. It is easy for an attacker to launch such an attack. For instance, putting the vehicle temperature sensor in cold water will let the OBUs generate false messages, even if the hardware sensors are tamper-proof. Also, one may note that in some cases the sender of the data may not necessarily be malicious, but his vehicle's sensors may be out of order. To rule out such cases of false data, one needs not only to verify that the sender of the data is legitimate, but also that the data are correct. Therefore some mechanisms for detection of malicious data need to be explored. We refer to such approaches as *a priori* countermeasures which attempt to prevent the generation of erroneous messages in advance.

The application of information-theoretic measures to anomaly detection was previously studied in the literature [12,14,24], but mainly in the context of the wired Internet. Most notably, [24] successfully applied the notion of relative entropy (also known as the Kullback-Leibler distance) to measure the similarity between two datasets.

Douceur [11] observes that the redundancy checks commonly built into distributed systems to mitigate the threats posed by faulty or malicious participants fail when a single adversary can present multiple distinct identities. Douceur proposes the use of *resource testing* to verify the uniqueness of online identities in a distributed computing environment. Unfortunately, this technique may fail in a VANET if an adversary has more resources than a normal node.

Location is a very important information shared in a VANET. The first proposal aimed at verifying the position data sent by vehicles is presented in [25]. In this proposal, the authors define a number of sanity checks that any vehicle can perform locally on the position information it receives from neighboring vehicles. All position information received by a vehicle is stored for some time period. This is used to perform the checks, the results of which are weighted in order to compute a trust metric for each neighboring vehicle.

A more general proposal that handles both detection and correction of malicious data is given in [17]. The authors assume that the simplest explanation of some inconsistency in the received information is most probably the correct one. The proposal works as follows. Each vehicle maintains a model of the VANET, containing information about the actual physical state of the network, based on the messages it has received. If a new message is received, the vehicle tries to incorporate the information contained therein in its existing model. If this renders the model inconsistent, then the vehicle searches for the minimal set of malicious vehicles and messages that, if removed from the model, would make the model valid again. These vehicles and messages are removed from the model, and the process continues. This approach is expected to be fully developed and combined with the other security mechanisms.

Observing the heavy overhead incurred by the above protocols to correct erroneous messages, some new proposals suggest more efficient threshold mechanisms [9,17,29,31,33] to achieve a similar goal. In these proposals, a message is trusted only if it was endorsed by a number of vehicles in the vicinity. This approach is based on the assumption that most users are honest and will not endorse any message containing false data. Another implicit assumption is the usual common sense that, the more people endorse a message, the more trustworthy it is. Among these schemes, the proposals in [9] may be the most efficient while enabling anonymity of message originators by exploiting secret sharing techniques. But their scheme does not provide anonymity revocability, which may not suit some applications in which anonymity must be revoked "for the prevention, investigation, detection and prosecution of serious criminal offences"[13].

3.3 Discussion on Existing Countermeasures

Unfortunately, neither *a posteriori* nor *a priori* countermeasures suffice on their own to secure VANETs. By taking strict punitive action, *a posteriori* countermeasures can protect against rational attackers producing bogus messages to obtain benefits or pranks. However, they are ineffective against irrational attackers such as terrorists. Even for rational attackers, damage has already occurred when punitive action is taken. It seems that *a priori* countermeasures function better in this case because they prevent damage beforehand by letting the vehicles trust only messages endorsed by a certain number of vehicles. However, although the underlying assumption that there is a majority of honest vehicles in VANETs generally holds, it cannot be guaranteed that a number of malicious vehicles greater than or equal to the threshold will never be present at specific locations. For example, this is likely to happen if some criminal organization undertakes to divert traffic from a certain area by broadcasting messages informing that a road is barred. Furthermore, for convenience of implementation, existing schemes use an even stronger assumption that the number of honest vehicles in all cases should be at least a preset threshold. But such a universally valid threshold does not exist in practice. Indeed, the threshold should somehow take the traffic density and the message scope into account: a low density of vehicles calls for a lower threshold, whereas a high density and a message relevant to the entire traffic of a city requires a sufficiently high threshold.

The situation is aggravated by the anonymity technologies used in some proposals. A system preserves anonymity when it does not require the identity of its users to be disclosed. Without anonymity, attackers can trace all the vehicles by monitoring the communication in VANETs, which in turn can enable the attackers to mount serious attacks against specific targets. Hence, anonymity is a critical concern in VANETs. However, anonymity can also weaken *a posteriori* and *a priori* countermeasures. Indeed, attackers can send fraudulent messages without fear of being caught, due to anonymity; as a result, no punitive action can be taken against them. Furthermore, some proposals provide strong anonymity, *i.e.* unlinkability. Unlinkability implies that a verifier cannot distinguish whether two signatures come from the same vehicle or two vehicles. This feature may enable malicious vehicles to mount the so-called Sybil attack: a vehicle generates a fraudulent message and then endorses the message herself by computing on it as many signatures as required by the threshold in use; since signatures are unlinkable, no one can find out that all of them come from the same vehicle. Hence, elegantly designed protocols are required to secure VANETs when incorporating anonymity. It must be noted that, among those threshold-based systems cited above which provide *a priori* protection and anonymity, [9] is the only one resistant to the Sybil attack: in that system, vehicles belong to groups, and vehicles in a group share keys (which provides vehicle anonymity because vehicles in a group are interchangeable as far as signing goes); however, for a message to be validated, endorsements from a number of different groups are needed, so a single vehicle cannot get a message sufficiently endorsed.

4 Towards a Combination of *a Priori* and *a Posteriori* Countermeasures

Our focus is to devise a context-aware threshold authentication framework with conditional privacy in VANETs, equipped with the following properties:

- It should support a threshold authentication mechanism in the sense that a vehicle can verify whether a received message has been endorsed by at least t vehicles. The threshold can be preset or dynamically changed according to the VANET context.
- It is privacy-preserving. An attacker cannot trace the vehicles who broadcast message-signature pairs. The attacker cannot tell whether the messages are endorsed by the same vehicle or not. This property prevents attackers from identifying vehicles by collecting and mining data.
- It allows revoking anonymity when necessary. As mentioned above, without an anonymity mechanism, t malicious vehicles can anonymously endorse a bogus message to cheat other vehicles. For example, a bang of criminals can divert traffic from their target area by broadcasting a message pretending that the road leading to that area is blocked by snow.

4.1 Message-Linkable Group Signatures

Group signatures have been investigated for many years [8,18]. In a group signature scheme, each group member can anonymously sign messages on behalf of the group. However, a group manager[1] can open the identity of the author of any group signature in case of dispute. Most existing group signatures provide unlinkability in the sense that no efficient algorithm can tell whether two group signatures are generated by the same group member, even if the two signatures are on the same message. Linkable group signatures [28] are a variant of group

[1] In most existing schemes, the group manager is responsible for both enrolling members and tracing signers, but some authors suggest to separate these two roles to improve security [6].

signatures. In a linkable group signature, it is easy to identify the group signatures produced by an identical signer, even if the signer is anonymous. This feature is desirable in e-voting systems where each voter can anonymously vote only once.

Group signatures are useful for securing VANETs but they are vulnerable to the Sybil attack because of unlinkability. 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. Hence, a more sophisticated notion of linkability is required in group signatures for VANETs. Motivated by this observation, we present a new primitive referred to as message-linkable group signatures (MLGS).

An MLGS scheme has the same security properties as regular group signatures except that, given two signatures on *the same message*, one can easily decide whether the two signatures are generated by the same member or by two different members, but the originator(s) stay(s) anonymous. Specifically, a message-linkable signature is an interactive protocol between a register manager, a tracing manager, a set of group members and a set of verifiers. It consists of the following polynomial-time algorithms:

- `Setup`: It is a probabilistic setup algorithm which, on input a security parameter λ, outputs the public system parameters denoted by π, including a description of the system.
- `GKGen`: It is a probabilistic group key generation algorithm which, on input the system parameters π, outputs the public-private key pairs of the register manager and the tracing manager.
- `MKGen`: It is a probabilistic member key generation algorithm which, on input the system parameters π, outputs the public-private key pairs of group members.
- `Join`: It is an interactive protocol between group members, the register manager and the tracing manager. The output of a group member is a group certificate. The output of the register manager is a list of registered group members. The output of the tracing manager is some secret tracing information to trace group signatures.
- `GSign`: It is a probabilistic algorithm which, on input the system parameters π, a message m, a private group member key and the corresponding group certificate, outputs a group signature σ of m.
- `GVerify`: It is a deterministic algorithm which, on input the system parameters π, a message m, a group signature σ and the public key of the register manager, outputs a bit 1 or 0 to represent whether σ is valid or not.
- `GTrace`: It is a deterministic algorithm which, on input the system parameters π, a message m, a *valid* group signature σ and the secret tracing information of the trace manager, outputs the identity of the group member who generated σ.

A secure MLGS scheme must be correct, unforgeable, anonymous, traceable and message-linkable. These properties are defined as follows:

- `Correctness`. It states that `GVerify` always outputs 1 if all parties honestly follow the MLGS scheme.
- `Unforgeability`. An MLGS scheme is unforgeable if any polynomial-time user who has not registered to the group has only a probability negligible in λ to produce a valid group signature.
- `Anonymity`. An MLGS scheme is anonymous if, given a valid message-signature pair from one of two group members, any polynomial-time attacker has only probability $0.5 + \varepsilon$ of guessing the correct originator of the message-signature pair, where ε is negligible in λ.
- `Traceability`. An MLGS scheme is traceable if any polynomial-time attacker has only a negligible probability in λ to produce a valid group signature such that the output of `GTrace` is not the identity of the group signature originator.
- `Message-linkability`. An MLGS scheme is message-linkable if there exists a deterministic polynomial-time algorithm which takes as input a message m and two valid group signatures σ_1 and σ_2 on m, and outputs a bit 1 or 0 to represent whether or not the two signatures were generated by the same group member.

4.2 A New Solution Based on Message-Linkable Group Signatures

Based on MLGS, we propose a general framework for threshold authentication with revocable anonymity in VANETs. In this framework, each vehicle registers to a vehicle administration office serving as a group registration manager. When t vehicles wish to endorse some message, they can independently generate an MLGS signature on that message. After validating t MLGS signatures on the message, the verifying vehicle is convinced by the authenticated message. However, if later the message is found incorrect, the police office as well as judges (serving as the tracing manager) can trace the t cheating signers. Here, we assume that an honest signer never needs to sign the same message twice. This assumption is workable by embedding a time-stamp in each message, as suggested in most authentication schemes for VANETs, if the OBU of a vehicle senses the same situation at different times.

From the security properties of MLGS schemes, it is clear that the above framework satisfies the required properties of threshold-variable authentication, anonymity and revocability in VANETs. If $t-1$ vehicles produce t signatures on the same message, then there exists a group member who has been involved in generating at least two signatures. Such an impersonation can be easily identified since the MLGS scheme is message-linkable. The construction is asymptotically optimal in complexity as the overhead is $O(t)$ in both computation and communication, regardless of the group scale. Hence, the above framework is very suitable for threshold authentication in VANETs.

5 Conclusion and Future Work

In this chapter, we have briefly reviewed the state of the art in VANETs. We have described their architecture and some of their potential applications, especially car-to-car information sharing in view of increasing traffic safety. We have justified why VANETs should be secure *and* preserve the driver's privacy. Security and privacy countermeasures proposed in the literature have been reviewed. In order to overcome the limitations of existing proposals, we have presented a framework combining both *a priori* and *a posteriori* countermeasures. The new framework offers a better balance between public safety and driver privacy in VANETs.

There are also other aspects that should receive more attention in the future. We need a more insightful consideration of the relationship between location privacy and anonymity. Anonymity mechanisms make it hard for attackers to link vehicles at specific locations with their identities. However, the location itself can leak information on vehicle identities. Also, content-based security in VANETs should be studied. Messages in VANETs contain much information about driving patterns. It is possible for attackers to extract much private information by collecting and mining vehicular communications. Finally, application-oriented security is also an open-ended line of work: more and more types of applications will appear in VANETs in the future, each bringing its own new security concerns.

Acknowledgments and Disclaimer

This work was partly supported by the Spanish Government through projects CONSOLIDER INGENIO 2010 CSD2007-0004 "ARES" and TSI2007-65406-C03-01 "E-AEGIS". The first author is partly supported as an ICREA-Acadèmia researcher by the Government of Catalonia. The authors are with the UNESCO Chair in Data Privacy, but their views do not necessarily reflect the position of UNESCO nor commit that organization.

References

1. Aad, I., Hubaux, J.-P., Knightly, R.: Denial of service resilience in ad hoc networks. In: Proceedings of ACM MobiCom, Philadelphia, PA, USA (September 2004)
2. Armknecht, F., Festag, A., Westhoff, D., Zeng, K.: Cross-layer privacy enhancement and non-repudiation in vehicular communication. In: 4th Workshop on Mobile Ad-Hoc Networks (WMAN), Bern, Switzerland (March 2007)
3. Au, M.H., Wu, Q., Susilo, W., Mu, Y.: Compact E-cash from bounded accumulator. In: Abe, M. (ed.) CT-RSA 2007. LNCS, vol. 4377, pp. 178–195. Springer, Heidelberg (2007)
4. Beresford, A., Stajano, F.: Mix Zones: User Privacy in Locationaware Services. In: Proc. of PerSec 2004, pp. 127–131 (March 2004)
5. Blau, J.: Car talk. IEEE Spectrum 45(10), 16 (2008)
6. Boyen, X., Waters, B.: Compact group signatures without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 427–444. Springer, Heidelberg (2006)
7. Calandriello, G., Papadimitratos, P., Lioy, A., Hubaux, J.-P.: Efficient and robust pseudonymous authentication in VANET. In: Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks-VANET 2007, pp. 19–28 (2007)

8. Chaum, D., van Heyst, E.: Group signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (1991)
9. Daza, V., Domingo-Ferrer, J., Sebe, F., Viejo, A.: Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks. IEEE Transactions on Vehicular Technology 58(4), 1876–1886 (2009)
10. Dötzer, F.: Privacy issues in vehicular ad hoc networks. In: Danezis, G., Martin, D. (eds.) PET 2005. LNCS, vol. 3856, pp. 197–209. Springer, Heidelberg (2006)
11. Douceur, J.: The Sybil attack. In: Druschel, P., Kaashoek, M.F., Rowstron, A. (eds.) IPTPS 2002. LNCS, vol. 2429, pp. 251–260. Springer, Heidelberg (2002)
12. Eiland, E., Liebrock, L.: An application of information theory to intrusion detection. In: Proceedings of IWIA 2006 (2006)
13. European Parliament. Legislative resolution on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005)0438 C6-0293/2005 2005/0182(COD)) (2005)
14. Feinstein, L., Schnackenberg, D., Balupari, R., Kindred, D.: Statistical approaches to DDoS attack detection and response. In: Proceedings of the DARPA Information Survivability Conference and Exposition (2003)
15. Fonseca, E., Festag, A., Baldessari, R., Aguiar, R.-L.: Support of anonymity in VANETs - Putting pseudonymity into practice. In: IEEE Wireless Communications and Networking Conference-WCNC 2007 (2007)
16. Gamage, C., Gras, B., Tanenbaum, A.S.: An identity-based ring signature scheme with enhanced privacy. In: Proceedings of the IEEE SecureComm Conference, pp. 1–5 (2006)
17. Golle, P., Greene, D., Staddon, J.: Detecting and correcting malicious data in VANETs. In: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, pp. 29–37 (2004)
18. Groth, J.: Fully anonymous group signatures without random oracles. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 164–180. Springer, Heidelberg (2007)
19. Gruteser, M., Grunwald, D.: Anonymous usage of location-based services through spatial and temporal cloaking. In: Proc. of MobiSys 2003, pp. 31–42 (2003)
20. Guo, J., Baugh, J.P., Wang, S.: A group signature based secure and privacy-preserving vehicular communication framework. In: Mobile Networking for Vehicular Environments, pp. 103–108 (2007)
21. Hubaux, J.-P., Capkun, S., Luo, J.: The security and privacy of smart vehicles. IEEE Security and Privacy Magazine 2(3), 49–55 (2004)
22. IEEE P1609.2 Version 1 - Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages (2006)
23. Jakobsson, M., Wetzel, S.: Efficient attribute authentication with applications to ad hoc networks. In: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks - VANET 2004 (2004)
24. Lee, W., Xiang, D.: Information-theoretic measures for anomaly detection. In: Proceedings of the IEEE Symposium on Security and Privacy (2001)
25. Leinmüller, T., Maihöfer, C., Schoch, E., Kargl, F.: Improved security in geographic ad hoc routing through autonomous position verification. In: Proceedings of the 3rd ACM International Workshop on Vehicular Vehicular Ad Hoc Networks - VANET 2006, pp. 57–66 (2006)

26. Lin, X., Sun, X., Ho, P.-H., Shen, X.: GSIS: A secure and privacy preserving protocol for vehicular communications. IEEE Transactions on Vehicular Technology 56(6), 3442–3456 (2007)
27. Luo, J., Hubaux, J.-P.: A survey of inter-vehicle communication. Technical Report IC/2004/24, EPFL, Lausanne, Switzerland (2004)
28. Nakanishi, T., Fujiwara, T., Watanabe, H.: A linkable group signature and its application to secret voting. Transactions of Information Processing Society of Japan 40(7), 3085–3096 (1999)
29. Ostermaier, B., Dötzer, F., Strassberger, M.: Enhancing the security of local danger warnings in VANETs - A simulative analysis of voting schemes. In: Proceedings of the Second International Conference on Availability, Reliability and Security, pp. 422–431 (2007)
30. Papadimitratos, P., Buttyan, L., Hubaux, J.-P., Kargl, F., Kung, A., Raya, M.: Architecture for secure and private vehicular communications. In: ITST 2007, Sophia Antipolis, France (2007)
31. Parno, B., Perrig, A.: Challenges in securing vehicular networks. In: Proceedings of the ACM Workshop on Hot Topics in Networks (2005)
32. Picconi, F., Ravi, N., Gruteser, M., Iftode, L.: Probabilistic validation of aggregated data in vehicular ad-hoc networks. In: Proceedings of the 3rd International Workshop on Vehicular Ad hoc Networks - VANET 2006, pp. 76–85 (2006)
33. Raya, M., Aziz, A., Hubaux, J.-P.: Efficient secure aggregation in VANETs. In: Proceedings of the 3rd International Workshop on Vehicular Ad hoc Networks - VANET 2006, pp. 67–75 (2006)
34. Raya, M., Hubaux, J.-P.: Securing vehicular ad hoc networks. Journal of Computer Security (special issue on Security of Ad Hoc and Sensor Networks) 15(1), 39–68 (2007)
35. Raya, M., Hubaux, J.-P.: The security of vehicular ad hoc networks. In: 3rd ACM Workshop on Security of Ad hoc and Sensor Networks-SASN 2005, pp. 11–21 (2005)
36. Raya, M., Papadimitratos, P., Aad, I., Jungels, D., Hubaux, J.-P.: Eviction of misbehaving and faulty nodes in vehicular networks. IEEE Journal on Selected Areas in Communications 25(8), 1557–1568 (2007)
37. Raya, M., Papadimitratos, P., Hubaux, J.-P.: Securing vehicular communications. IEEE Wireless Communications Magazine 13(5), 8–15 (2006)
38. Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K., Sezaki, K.: CARAVAN: Providing Location Privacy for VANET. In: Proc. of ESCAR 2005 (November 2005)
39. U.S. Department of Transportation, National Highway Traffic Safety Administration, Vehicle Safety Communications Project, Final Report (April 2006), `http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/060419-0843/PDFTOC.htm`
40. Wu, Q., Domingo-Ferrer, J.: Balanced trustworthiness, safety and privacy in vehicle-to-vehicle Communications, Manuscript (2008)
41. Zarki, M.E., Mehrotra, S., Tsudik, G., Venkatasubramanian, N.: Security issues in a future vehicular network. In: Proceedings of European Wireless 2002 (2002)