Security of Vehicular Networks: A Comparative Study

Md Mahbubul Haque, Jelena Mišić, Vojislav B. Mišić, Subir Biswas, and Saeed Rashwand

University of Manitoba, Winnipeg, Manitoba, Canada

April 17, 2009

Abstract

The main goal of wireless vehicular networks is to ensure safe driving environment, but they also offer a wide variety of services and applications, most of which are safety related. Integration of effective security techniques in vehicular networks is a difficult task due to the many constraints imposed by those networks. In this Chapter, we give an overview of communication and security architectures for wireless vehicular networks, discuss some common threats and ways in which they can be alleviated, and point to the areas of possible improvement.

1 Introduction

With rapid advancement of wireless networks, wireless vehicular networks are getting closer to reality. It is envisaged that in near future all vehicles on the road will be able to communicate with each other to ensure a safe driving environment. By providing early traffic congestion reports and accident location information along the road, a vehicular network will also save the driving time. Finally, vehicular networks will offer new commercial possibilities which were hitherto impossible to achieve with existing technology.

Since vehicular networking is an emerging area, unified terminology has not yet been generally adopted. A vehicular network is also called a vehicular ad hoc network (VANET). Blum and Eskandarian referred to a vehicular network as an intelligent transportation system [8]. Recently, Zhang et al. [40] investigated the convergence of vehicular networks and vehicular sensor networks. Despite the proliferation of names, the purpose and principles of a vehicular network remains the same.

There have been many research contributions in the areas of routing, medium access control (MAC), and physical layer protocols of vehicular networks. A standard for dedicated short range communication (DSRC) has been developed [1]. Currently, the IEEE 802.11 standards committee is working towards the final version of the IEEE 802.11p standard [20]. As the 802.11p standard is based on 802.11, it specifies the standard for physical and MAC layers only. For upper layers, another standard known as IEEE 1609 has been developed. The IEEE 1609.2 specifies the security standard for vehicular communications, which is based on public key cryptography with the support of elliptic curve cryptography [22]. Moreover, in the United States, the FCC has allocated bandwidth for vehicle-to-vehicle communications [2].

Main components of a VANET are on-board units (OBU) and road-side units (RSU). For inter-vehicle communication, each vehicle will be equipped with OBU through which it will communicate with other vehicles as well as with suitably located base stations or RSUs. The base stations of cellular networks can play the role of RSUs in vehicular networks, which may significantly reduce the cost of VANET deployment. We cover the details of communication architecture in section 3.

The security attributes of a VANET differs from other wireless networks due to high mobility and drivers' privacy requirements. We identify the most important security requirements of VANETs and look at the currently proposed various security architectures. After analyzing several security architectures for VANETs, we also focus on the future directions of security research in VANETs.

The Chapter is organized as follows. We begin in section 2 by evaluating the application categories of VANET. In section 3, we describe communication architecture of vehicular networks. We move ahead to explain attacks in section 4 and identify the security requirements in section 5. Then we categorize and clarify the security architecture of VANETs in section 6, which describes how the security architecture conforms to communication architecture. Some comments regarding secure batch processing of messages is given in section 7, while several revocation schemes in section 8. Security architecture for value added services is explained in section 9. The Chapter concludes with a brief overview of issues which are still open at the time of this writing.

2 Applications

Vehicular networks have the great potential to improve driving safety and serve as the platform for development of many infotainment applications. In safety-based application, a vehicular network can generate traffic reports and suggest detours in case of congestion, which could help many drivers. Automatic toll collection in highway, electronic parking payment, critical point of interest warning (e.g. school), automated lane change warning and Internet service are other examples of vehicular network applications.

Raya and Hubaux [30] categorized the applications into following two categories:

1. Safety-related applications include traffic information for congestion and collision avoidance, and liability related application in the case of an accident. There are three technical possibilities for such applications [37][30]:
   (a) Passive: Vehicles will send periodic safety messages to other vehicles and RSUs. Mostly this type of message will contain the current status. For example, a vehicle will keep sending its current speed and lane number to make other vehicles aware of the environment.
   (b) Active: In case of an emergency situation, a vehicle needs to broadcast safety message with high priority. For example, if a vehicle loses control suddenly, the information should be forwarded to other close vehicles as soon as possible to avoid collision. An active message should always get the highest bandwidth.
   (c) Liability related safety applications: In case of any dispute, for example an accident, the legal

authority needs to obtain the identity of the vehicle. In this case, messages containing liability information needs to be forwarded to the proper authority.

2. Value added service: Internet access is the most common value added service. Electronic parking payment, automated toll collection also fall into this category. Moreover, a vehicular network can also help provide emergency roadside assistance service quickly and protect against the theft of a vehicle [11]. Legal authority will be able to track down a vehicle with the help of OBU to RSU communication. However, in case of tampering of an OBU, authority can gather data from nearby vehicle information (e.g., camera images).

3 Communication architecture

We can categorize the communication architecture of vehicular communication into two broad parts: intra- and inter-vehicle communication.

3.1 Intra-vehicle communication

Nowadays all vehicles are equipped with sophisticated electronic devices, and their number is increasing. It is estimated that luxury vehicles cost 23% extra because of electronic devices they contain [25]. All electronic devices within a vehicle – media (audio and video) player, GPS, cellular phone, camera, to name just a few – are capable of communicating with each other through a controller area network (CAN). A CAN for a vehicle can be wireless with limited communication range. However, the wireless area of a CAN can be extended (alternatively, a multi-hop strategy can be used) if the vehicle dimensions are large (e.g., train). A master electronic device can manage the communication between all other devices [25].

3.2 Inter-vehicle communication

The main communication components in a inter-vehicle communication are on-board units (OBU) and roadside units (RSU). The vehicles will be equipped with OBUs while RSUs will be placed alongside the roads. OBUs will communicate with each other as well as with RSUs. Based on the type of inter-vehicle communication, we categorize them into three groups.

1. Ad hoc vehicular network: In case of unavailability of RSU on the road, OBUs will have to communicate with each other directly forming an ad hoc network. Figure 1 shows the communication architecture for this sort of communication. The ad hoc vehicular network is limited to very short range of communication. Without the help of an RSU, vehicles will have to adopt to a multi-hop forwarding for a long distance communication.

2. RSU aided vehicular network: In case of RSU aided scenario, OBUs will communicate directly with nearby RSU. Each RSU then forward the message to legal authority if necessary. Figure 2 shows an example of RSU aided vehicular network. If a RSU is located far away from a vehicle then the vehicle will use multihop strategy [38] to forward the message to the destination.

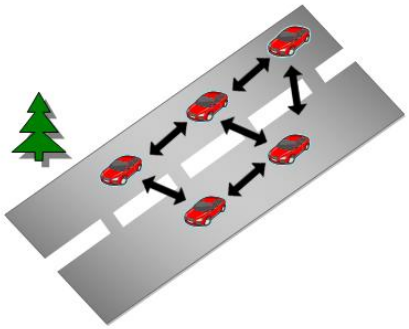

Figure 1: Ad hoc vehicular network.

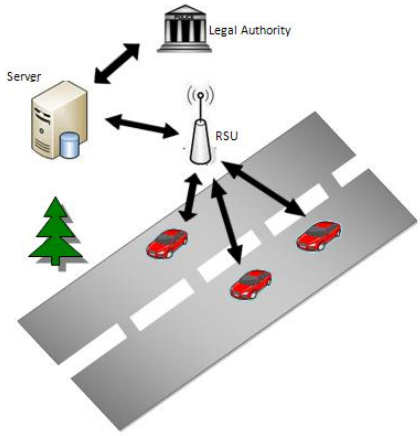

Figure 2: RSU-aided vehicular network.

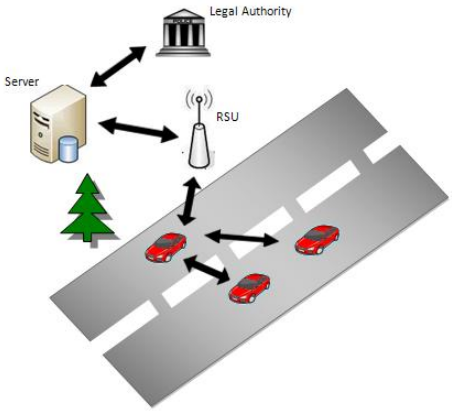

Figure 3: Cluster-based vehicular network.

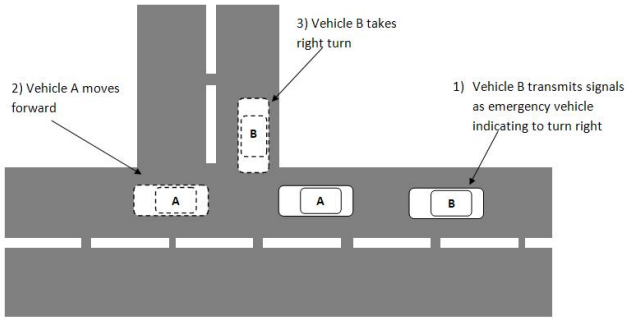

Figure 4: Impersonation attack

3. Cluster based vehicular network: In a cluster based network [8], among several OBUs one group leader will be selected. Any communication between an OBU and RSU will take place through OBU group leader all the time. Figure 3 depicts a cluster based vehicular network.

Reliable and timely inter-vehicle communication aided by intra-vehicle networks can ensure a safe driving environment. In case of an immediate emergency situation (e.g., if a pedestrian comes along the way and vehicles ahead brake rapidly), a CAN can initiate the emergency brake if the driver cannot response quickly.

An OBU in a VANET can work as master controller for intra-vehicle communication. Most importantly the security architecture of a vehicular network must comply with the communication architecture.

4 Security Attacks on Vehicular networks

Like any other wireless network, VANET is also vulnerable to various attacks from adversaries. Some of the attacks in vehicular networks are similar with other wireless networks while some others are specific for VANET. Before making a vehicular network secure, we need to understand the types of possible attacks on VANET.

Parno and Perrig [27] identified some possible attacks on vehicular networks. Later Raya and Hubaux [30] and Raya et al. in [31] elaborated the types of attacks. In the following, we list some of the better known attacks.

- Impersonation attack: A vehicle might impersonate an emergency vehicle, thus making its way free even under high traffic congestion. Figure 4 depicts this type of attack. Likewise, an RSU can be impersonated too. In this case, other vehicles will trust impersonated RSU and divulge confidential information.
- Denial of service(DOS) attack: An adversary may intentionally jam a network or block the communication of a targeted vehicle. As a result, vehicle will not be able to receive any message. For example, in case of sudden break, the information will not reach other nearby vehicles, thus resulting in a collision. It is possible to jam a network signal at physical layer.
- Alteration attack: An attacker could alter the content of a message. Alteration attack will misguide other vehicles with false information. For example, in case of an accident a vehicle can change liability

information which will misguide the legal authority to take inappropriate action.

- Listening attack: An attacker might observe the communication of nearby vehicles and interpret confidential data. For example, for any value added service if an attacker can read user credentials then later the attacker can access the value added services by using user credentials.
- Replay attack: Replay attack is similar to listening attack with the difference that after recording the message, the attacker will replay the message to RSU to identify himself as the previous originator of the message.
- Physical tampering: A knowledgeable attacker can tamper with the OBU and change some (or even all) vehicle credentials, resulting in auto insurance decrease which in turn is going to make the government lose a lot of money. Physical tampering leads to silent attack as disabling the OBU physically will stop message broadcast. As a result an adversary will be able to escape liability and avoid certificate revocation in many protocols.
- Sybil attack: A vehicle will impersonate itself with multiple entities in the network by using a large number of pseudonyms. A revoked vehicle may launch this attack to gain access to network resources. An adversary will essentially use more resources with the Sybil attack and insert false information [42] into the network. For example, all instances of the same vehicle may report a traffic congestion. Since the RSU or other OBUs see the report coming from multiple vehicles, everyone will trust it.

5 Security requirements in VANET

Before discussing the security techniques, we need to look at the security requirements that would protect a VANET from the attacks. A fully secured scheme for VANET needs to fulfill all the security requirements. We identify the security requirements for VANET and according to the importance of security level we categorize them.

- Integrity and non repudiation: Any message coming from an OBU or RSU should remain unaltered until reaches destination. A secure vehicular network must ensure two types of integrity: data integrity and origin integrity. Data integrity ensures an unchanged message while origin integrity ensures the sender of a message. So, no OBU/RSU can deny the sending of a message. Origin integrity is also known as the non repudiation property of a secure network.
- Confidentiality: Message contents in a vehicular network are not confidential as it contains a vehicle's speed, location and all other safety related information. However, the originator of the message should be confidential since an adversary can track a vehicle if he knows the originator. So, encryption of the originator information is more important than encrypting a message content.
- Authentication: In normal situation, a vehicle should not know the identity of other vehicles. However, a RSU and an OBU must authenticate each other. For example, before accepting a command from an RSU, a OBU has to be sure that the message is really coming from the RSU, not from an adversary.

A trusted third party, for example, certificate authority (CA) can ensure the authenticity between RSU and OBU.

- Privacy and anonymity: Privacy preservation is subject to complex constraints, as it entails both privacy with respect to other OBUs and with respect to authorities. A vehicle should be anonymous to other vehicles and RSUs, however, in case of dispute or accident, legal authority must be able to learn the true identity. Privacy against other OBUs is unconditional and it should be protected by all means. Privacy against authority is hard to achieve since many schemes put the significant amount of trust in authorities and authorities have drivers' credentials. This opens a possibility of privacy violations in rare cases when authority officers are corrupted.
- No single authority should be trusted. Even police officers might abuse their authority using their VANET privileges.
- It is essential to revoke a compromised OBU/RSU from the network immediately.
- Messages in a vehicular network should be prioritized. For example, a message containing accidental information should get highest priority as it conveys an emergency news.
- Each OBU of a vehicle should be tamper proof which will prevent the modification of vehicle information.
- To minimize the cost it is feasible to build an OBU with small storage space. So, the security infrastructure should not overwhelm OBUs with lots of certificates and large revocation list.
- The vehicular network must be robust. In case of denial of service attack [33] or sudden malfunctioned network, it is necessary to ensure the safety of the vehicular network.

6 Security architectures in VANET

To address the security requirements, many schemes have been proposed. Most of the proposals are based on public key infrastructure (PKI). A public key infrastructure ensures a secure communication with the help of private/public key pairs, using RSA cryptography. However, due to the computational overhead associated with PKI, some researchers give preference to symmetric key cryptography. IN this approach, not unlike the well known SSL protocol, a symmetric key is pre-established between two components with the help of public key cryptography. This approach offers significantly reduced computational overhead.

6.1 PKI based architectures

In a PKI based architecture, a common way to achieve integrity is digital signature. With a public/private key pair, a digital signature can ensure the originator of a message. By using a private key an OBU/RSU can sign and send a message. Upon receiving the message, the receiver can apply the sender's known public key to decrypt the data. However, the computation cost for digital signature is high.

To minimize the computation cost hash function with digital signature can be used. As message content is not confidential in VANET, an OBU can make a message digest by using a hash function and encrypt the

digest by private key. After receiving the message, the receiver will generate the message digest and compare with the received digest. If they match then the receiver understand that data is intact and a particular OBU sent the message.

A certificate authority can ensure proper authentication between OBUs and RSUs. During registration, a CA grants certificates to each vehicle. The simplest certificate may contain the following fields.

$$\text{Cert}_A = \{pk, T\}$$

where Cert_A is certificate of an OBU, pk is public key of an OBU and T presents expiry time of the certificate.

As many PKI based architectures have been proposed, we may categorize them as follows.

6.1.1 Group Signature and Identity based cryptography

The group signature scheme provides anonymity as an adversary will only be able to track a group, not a particular vehicle. Zhang et al. [41] proposed to use the short group signature in vehicular networks. In this approach, a vehicle belongs to a group. Each vehicle will have its unique group private key, while the whole group has single public key. A vehicle will sign a message by using its group private key and the receiver can verify the signature of the message by using group public key. Therefore, an adversary can track only the group, but not a particular vehicle. In case of dispute legal authorities will be able to unveil liability related information.

One of the first proposals for a PKI based architecture is DAHNI [39]. The authors proposed the use of digital signatures along with identity based cryptography that will eradicate the use of public key certificates. The authors also proposed a visual interface called VIVA which provides a better awareness of nearby vehicles.

By observing distinct benefits of two cryptographic techniques, Sun et al. [33] proposed to integrate group signature and identity based signature for VANET. They used group signature scheme for OBU to OBU communication and identity-based cryptography for OBU to RSU communication because of their different security requirements. Identity-based cryptography will eliminate the use of public key infrastructure as identity will be used as public key. For OBU to OBU communications, group signature will ensure anonymity as the verifier will only be able to identify the group to which the signer belongs.

However, all group signature schemes described above are based on centralized key management where keys are preloaded into the vehicles offline [18]. A centralized group signature may well be inefficient due to high system maintenance overhead. Hao et al. [18] proposed a distributed key management scheme for group signature based vehicular networks. All vehicles in this scheme update their group key pairs dynamically which is broadcasted by RSU.

Wasef et al. [35] proposed a different approach. They proposed a hierarchical architecture where they used ID-based cryptography among different certificate authorities and certificate-based authentication(RSA) for authentication between RSUs and OBUs.

6.1.2 Cross certification

In a VANET, every region will have its own certificate authority. For example, each state/province within a country could have a different CA working under different transportation authorities. A vehicle registered under one authority should be able to roam in different regions. To achieve this, each CA needs to cross certify each other. So, a vehicle will be able to form a certificate chain and acquire the public key of another CA. For example, if CA_1 is the certificate issuer of OBU_1 and CA_2 is the certificate issuer of OBU_2 then OBU_1 can verify OBU_2 in the following way.

1. CA_1 certifies OBU_1 and CA_2 certifies OBU_2 ($CA_1 << OBU_1 >>$ and $CA_2 << OBU_2 >>$).
2. CA_1 and CA_2 will cross certify each other. So, $CA_1 << CA_2 >>$ and $CA_2 << CA_1 >>$.
3. OBU_1 will form a certificate chain. $CA_1 << CA_2 >> CA_2 << OBU_2 >>$. OBU_1 can apply the public key of CA_1 on $CA_1 << CA_2 >>$ to retrieve the public key of CA_2. Then the public key of CA_2 will give OBU_1 the public key of OBU_2.

Papadimitratos et al. [26] proposed a hierarchical model for certificate authorities. All the CAs of different countries will cross certify each other in their model. To eliminate the use of cross certification, Wasef et al. [35] proposed another hierarchical model for VANET. In this approach, all CAs work at the same level under one master authority. The master authority generates two types of key for each CA. The first key is a public/private key pair which a CA can use to sign each RSU in its coverage area. Then the master authority generates the second key as partial signing key. Each CA can use this key to generate private key that each RSU can use to sign keys for OBUs. However, if there is only one master authority then the question of single authority comes again.

6.1.3 Pseudonym based approach

If a vehicle has only one certificate then by tracking the certificate an adversary can identify a vehicle. So, a vehicle should have multiple certificates which should be changed frequently. Each of these short term certificates is called pseudonym. However, an authority needs to bind the short term identities with long term identity to track a vehicle for legal action if necessary.

Raya and Hubaux developed a model [30] that uses an electronic identity called Electronic License Plate (ELP) which is the long term identity of a vehicle. The authors proposed to update a vehicle certificate periodically with anonymous certificates. However, vehicles need to store a large number of anonymous certificates. Moreover, the link between old and new pseudonyms still can be traced by observing the spatial and temporal relationship of old and new locations [19]. To address this problem, Sampigethaya et al. proposed the CARAVAN [32] approach which is based on cluster based network. CARAVAN uses silent periods [19] where a vehicle goes into silent state after a predefined interval. All other vehicles update their pseudonym during this silent period. Therefore, a vehicle which listens to other OBU communications within silent period will not be able to track pseudonym change of other vehicles, thus decreasing the linkability between old and new pseudonyms. However, CARAVAN does not provide better performance where vehicles have to send frequent safety messages.

6.1.4 Escrowing

If there is only one certificate authority, abuse of power might occur. Escrowing is a better method to prevent this insider attack. In this method, a CA will blindly sign all the certificates belonging to one vehicle. Later, authority will be able to trace a vehicle by escrowing the links between certificates [3, 22]. The advantage of escrowing is that no single authority will be able to trace a vehicle. To trace a vehicle all the keys from different escrow agencies needs to be combined.

6.1.5 Prevention of Sybil and DOS attacks

Many of the pseudonym based approaches [30, 31, 26] are vulnerable to Sybil attack. To mitigate the problem, an RSU can use a directional antenna [15] or a bi-directional antenna [17] for locating adversary. The motivation behind identifying the location is that if multiple messages of different pseudonyms come from the same location then the vehicle is a Sybil attacker. However, due to the localization error in a dense network the approach might fail to detect true attacker. To improve this scenario, Zhou et al. [42] proposed P^2DAP which is based on hash function. At the beginning, Ministry of transportation will generate the common hash values for different pseudonyms. RSU can check the hash values from pseudonyms and will report to the authority if all pseudonyms belong to the same pool.

Blum and Eskandarian developed the SecCar protocol [8] which is based on cluster-based VANET. To prevent the DOS attack the authors integrated time-division multiplexing and frequency-hopping spread-spectrum. A known hopping sequence between sender and receiver ensures anti-jamming capabilities.

6.2 Symmetric and Hybrid approach

Since symmetric cryptography allows for faster computation, many researchers proposed security models for VANET based on symmetric key cryptography. However, to exchange the shared key between two entities, asymmetric (public/private key) cryptography can be used.

Oguma et al. [25] describes a remote attestation-based security architecture for intra vehicle communication. The authors proposed to use a symmetric key between each pair of controllers, which will be preloaded into the vehicle during manufacture. Using a tamper proof chip for each controller could be expensive. So, a rich processing power controller embedded with a tamper proof chip can take the role of master controller and take part in remote attestation procedure. Once the vehicle starts, the master controller collects hash values from each of the controllers. Along with the hash values, master controller also receives a challenge from remote verification server. The master controller then sends a response value which will be checked by the remote verification server. Remote attestation scheme provides flexibility in various aspects; for example, the remote server can detect any malfunction or security breach in any controllers and flash the software. Moreover, only one controller needs to communicate with the remote server. However, in this scheme [25], the number of controllers is fixed and no controller can be extended after manufacturing the vehicle.

The work of Youl et al. [11] is based on symmetric key cryptography. In the key registration phase, an ombudsman will use a vehicle's real identity to generate and store long lived pseudonyms in an OBU. Then

the long lived pseudonyms will be used to generate short-lived pseudonyms along with the session key and duration of each short-lived pseudonyms. Short-lived pseudonyms and corresponding session keys will be updated periodically.

Freudiger et al. [14] proposed location privacy based on a hybrid approach. In the beginning, an OBU will receive a symmetric key from RSU through key exchange of asymmetric cryptography. Then all vehicles within a mix-zone (e.g. intersection) will be able to update pseudonyms through the symmetric shared key. The motivation behind using a mix zone and symmetric cryptography is that, since pseudonym change is performed by symmetric cryptography, an adversary will not be able to keep track of two successive pseudonyms.

Moustafa et al. [24] proposed an authentication, authorization and accounting model (AAA) where they used the Kerberos protocol. An OBU request for a ticket (TGT request) to nearby RSU. Each RSU represents AP service manager or Kerberos proxy which forwards the TGT request to key distribution center (KDC). A KDC will issue a TGT to the vehicle. By obtaining a TGT ticket, an OBU gets authenticated. Later, an OBU can use the TGT to request a specific service (TGS) in the same procedure. After obtaining a TGS, an OBU can use it to request various types of services. For example, an OBU can send TGS request to DHCP server for an IP address or to a certificate authority for a certificate.

Motivated by the TESLA approach [28] authentication model, Lin et al. [23] proposed TSVC (TESLA based secure vehicular communication protocol) model for secure vehicular communication. As in TESLA, the foundation of TSVC model is one way hash chain. All the chain elements are considered as secret keys to compute message authentication code (MAC). For each packet a hash value from hash chain is used as secret key. The secret key will be released after a short delay once the receiver receives a data packet. Upon receiving the packet the receiver can verify MAC for each packet. However, due to the time-synchronization and delayed verification problem [11], TSVC model is not suitable for vehicular network. During high traffic load when lots of OBU will compete to get the service from a RSU, the resulting delay for authenticating a message may well not be acceptable.

Wolf et al. [36] used a combination of symmetric and asymmetric cryptography for intra-vehicle communication. Controllers will communicate with each other using symmetric keys. Asymmetric key will be used for periodically updating the symmetric key as well as for the registration of a new controller. Since controllers will frequently exchange messages, symmetric key will provide faster computation speed.

7 Batch Verification

Certificate management is a big issue in vehicular network due to rigorous requirement of message processing time. According to the DSRC protocol a vehicle needs to send safety messages to RSU every 100 to 300 ms. Surrounded by a lot of vehicles in rush hour, a RSU might have to verify a few hundred messages each second [40], thus creating a bottleneck for RSU. To solve this problem, Zhang et al. [40] proposed a batch verification scheme which verifies multiple messages simultaneously. The authors integrated identity-based cryptography and batch processing to maximize the efficiency. However, the authors investigated the approach only for OBU to RSU communication only. Sometimes, in the absence of a RSU, vehicles have to

communicate with each other directly. As a result, vehicles should be able to perform batch processing too. Moreover, in this batch processing all the messages are assumed to be authentic. If an adversary sends false message it is going to disable batch verification.

Wasef et al. [35] proposed a similar type of model based on bilinear pairing. They improved the model of Zhang et al. by using a hierarchical model. All the CAs will communicate in the same layer. As a result vehicles registered under one CA will be able to receive a new certificate in another region under new CA. However, the approach still failed to issue the identification of bogus messages in batch verification.

To improve the scenario, Jiang et al. [21] proposed a tree-based signature scheme called binary authentication tree (BAT) which can detect the bogus messages from received messages. BAT ensures a faster batch processing with bilinear pairing. The authors used a different set - FS, to store all the bogus messages. To verify the authenticity of all messages Jiang et al. used a recursive approach. If the root of the tree is authenticated then the whole tree is authenticated, however, if the root is not authenticated then the algorithm recursively calls child nodes until it finds the bogus message. In this way, FS will store all the bogus messages.

8 Revocation

With the revocation of certificate, a vehicle will lose its right to use the vehicular network. Certificate revocation of a vehicle is necessary since the identified attacker or malfunctioning vehicle needs to be eliminated from the network [31]. For a pseudonym-based approach [26] setting a expiry time for each pseudonym is one way to revoke certificates. So, after a certain time when old certificate expires, an adversary will not be able to get a new certificate. However, this approach creates a vulnerability window as the attacker will still be able to communicate for a certain period of time. To improve the scenario, the frequency of changing pseudonyms should be increased, however, this will increase network load. Papadimitratos et al. [26] proposed to choose a tradeoff of pseudonym refill depending on the security level a network seeks.

Before granting a certificate, a RSU needs to check the certificate revocation list (CRL) which will store all the certificates of revoked nodes. However, over the time the list might get pretty large. Raya et al. [31] developed a revocation scheme that uses compressed certificate revocation lists (CRLs). The revocation scheme uses a Bloom filter [7], thus reducing the size of the CRL. A tamper proof device installed in vehicle will store and check the CRL to verify the certificate of other vehicles. However, relying on a vehicle to store and check the CRL is infeasible, as the vehicle might generate silent attack which will avoid certificate revocation.

Motivated by the tampering problem Lin et al. [22] proposed RSU-aided certificate revocation. Once CA decides to revoke a vehicle's certificate, it will broadcast the message to all the RSUs. By predicting the movement of the revoking vehicle, RSU will send a warning message to update CRLs of nearby vehicles. In this way, all other vehicles will avoid communication with the revoked vehicle. To prevent the silent attack, Lin et al. also proposed to use automatic periodic revocation of each certificate. So, after a certain time when old certificate expires, revoked vehicle will not be able to get a new certificate. Still, this approach creates a vulnerability window as the adversary is not removed instantly.

Sun et al. [34] developed revocation method for group signature scheme. In this approach, the unrevoked

nodes will update their private key and group public key whereas adversary will not be able to update keys. The authors also investigated the CRL-based approach but did not recommend due to the problems mentioned earlier.

For a distributed group signature scheme, only the RSU will store a certificate revocation list [18]. In case of revocation, RSU will check the CRL and broadcast new group private key/public key. Except the adversary, all other vehicles will be able to update key pairs. The advantage in this approach is that a RSU does not need to send CRL to all OBUs, thus reducing network load whereas in a centralized approach a RSU needs to send new CRL to each vehicle every time it is updated.

Recently, Wasef et al. [35] modeled a revocation protocol by using two CRLs, CRL_{OBU} and CRL_{RSU}.

CRL_{OBU}: It is the list of all revoked vehicles. All RSUs will store a copy of CRL_{OBU}. Before granting a new certificate to an OBU, each RSU will check the list.

CRL_{RSU}: It is the list of all revoked and inoperative RSUs. Each OBU will have a copy of CRL_{RSU}. An OBU will check the list before accepting a new certificate from a RSU. The list helps a OBU against impersonation attacks.

Since RSUs are much smaller in numbers than OBUs, CRL_{RSU} will be small. However, the size of CRL_{OBU} still might get large quickly.

9 Security architecture for value added services

Besides a secured safety applications of VANET, it is essential to ensure a secure architecture for value added services too. Sun et al. [33] designed a three layer architecture for wide deployment of Internet access and other applications through IEEE 802.16e mesh network. The authors proposed to install mesh routers alongside the road, which will be connected with backbone Internet through a wired or wireless network. The routers will be capable of supporting both IEEE 802.16 and 802.11p network. Therefore, the mesh routers can receive the broadcasted safety messages from vehicle as well as providing Internet services.

Papadimitratos et al. [26] identified that for a download session, a vehicle IP address must not change throughout the whole session and this situation creates a problem for pseudonym-based approach. As the pseudonym should change frequently depending on the security level, all other credentials (e.g. IP address) should also change. However, for a long download session if the IP address does not change the attacker will be able to track a vehicle easily. To solve this problem Papadimitratos et al. proposed tunneling of old IP packet datagram into new IP packet. Although the vehicle will get a new IP address for a new pseudonym, the old IP address will be used to continue the service.

The work of Coronado and Cherkaoui [12] evaluates a service architecture for on demand value added services. The authors proposed a secured service architecture for on demand services. A district domain contains the security module that provides security for different types of services. Governmental authority (GA) and private trusted authorities (PA) are two major security modules of the district domain architecture. GA will be responsible for preloading key certificates into the vehicle during registration while PA will provide

temporary key certificates for each type of services. The authors also included banking module for secure transaction.

10 Open issues

Vehicular networks are a rapidly emerging area, and many among the issues regarding security are still wide open for development.

One problem which is frequently overlooked is the choice of security procedures for handover from one RSU to another RSU. Similar to the cellular network, a vehicular network needs a secured handover process when a vehicle changes region. Choi et al. [11] mentioned one secure handover procedure where each RSU will transfer handle (long lived pseudonyms) to another RSU. Upon receiving the handle, the RSU will generate short lived pseudonyms once again. The vehicle will be unaware of the situation. Sun et al. [33] also mentioned handover, however, they did not provide any secure procedure to support it.

Protocols for value added services have not been well developed yet. To prevent forgery on value added service, a secured architecture is a must. IPsec protocol can address the security requirement of value added services. The IPsec protocol provides network layer security, which comes in two flavors: authentication header protocol (AH) and encapsulation security payload (ESP) protocol. In ESP, the whole transport layer segment is encrypted, thus providing confidentiality for messages, specially for a credit card transaction. To provide both authentication and confidentiality, combination of AH and ESP protocol is effective.

Another important issue which did not receive sufficient attention is the change of MAC address along with pseudonym. Only [26] mentioned about the importance of changing MAC address. If the IP address changes with pseudonym, MAC address should be changed too. Otherwise, an adversary can easily track a vehicle by tracking it's MAC address.

The development of a full blown simulation environment dedicated to vehicular networks is also a critical issue. Due to the high mobility of the vehicles and complex privacy constraints, existing simulators might not be able to properly simulate a vehicular environment. Straw [10] [4], VANET Mobisim [13], TraNS [29] [6] and SUMO [5] are some examples of VANET simulators. Besides that other efforts are also going on for building a dedicated VANET simulator [16] [9]. However, all of these simulators are still in development phase and many of them do no provide a security platform for VANET.

References

[1] Dedicated short range communications (DSRC). `http://grouper.ieee.org/groups/1616/136_dsrc_advisory.pdf`, Accessed on January 07, 2009.

[2] Federal communications commission. `http://www.fcc.gov/Bureaus/Engineering_Technology/Orders/1999/fcc99305.txt`, Accessed on January 19, 2009.

[3] Vehicle safety communications project. `http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/060419-0843/PDFs/AppendixH.pdf`, Accessed on January 20, 2009.

[4] STRAW - STreet RAndom Waypoint - vehicular mobility model for network simulations. `http://www.aqualab.cs.northwestern.edu/projects/STRAW`, Accessed on March 05, 2009.

[5] SUMO: Simulation of Urban MObility. `http://sumo.sourceforge.net/`, Accessed on March 05, 2009.

[6] TraNS - realistic simulator for VANETs. `http://trans.epfl.ch/`, Accessed on March 05, 2009.

[7] B. H. Bloom. Space/time trade-offs in hash coding with allowable errors. *Communications of the ACM*, 13(7):422–426, 1970.

[8] J. Blum and A. Eskandarian. The threat of intelligent collisions. *IT Professional*, 6(1):24–29, Feb. 2004.

[9] L. Bononi, M. D. Felice, M. Bertini, and E. Croci. Parallel and distributed simulation of wireless vehicular ad hoc networks. In *Proceedings of the 9th ACM International Symposium on Modeling Analysis and Simulation of Wireless and Mobile Systems (MSWiM '06)*, pages 28–35, Terromolinos, Malaga, Spain, Oct. 2006. ACM.

[10] D. R. Choffnes and F. E. Bustamante. An integrated mobility and traffic model for vehicular wireless networks. In *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks (VANET'05)*, pages 69–78, Cologne, Germany, Sept. 2005. ACM.

[11] J. Y. Choi, M. Jakobsson, and S. Wetzel. Balancing auditability and privacy in vehicular networks. In *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks (Q2SWinet '05)*, pages 79–87, Montreal, Quebec, Canada, Oct. 2005. ACM.

[12] E. S. Coronado and S. Cherkaoui. Service discovery and service access in wireless vehicular networks. In *IEEE GLOBECOM Workshops*, pages 1–6, New Orleans, LA, USA, Dec. 2008.

[13] M. Fiore, J. Harri, F. Fethi, and C. Bonnet. Vehicular mobility simulation for VANETs. In *Proceedings of the 40th IEEE Annual Simulation Symposium (ANSS'07)*, Norfolk, USA, Mar. 2007.

[14] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J. Hubaux. Mix-zones for location privacy in vehicular networks. In *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, pages 38–46, Vancouver, British Columbia, Canada, Aug. 2007.

[15] P. Golle, D. Greene, and J. Staddon. Detecting and correcting malicious data in VANETs. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks (VANET '04)*, pages 29–37, Philadelphia, PA, USA, Oct. 2004. ACM.

[16] C. Gorgorin, V. Gradinescu, R. Diaconescu, V. Cristea, and L. Ifode. An integrated vehicular and network simulator for vehicular ad hoc networks. In *Proceedings of the 20th European Simulation and Modeling Conference (ESM)*, pages 142–149, Bonn, Germany, May 2006.

[17] G. Guette and B. Ducourthial. On the sybil attack detection in VANET. In *IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS 2007)*, pages 1–6, Pisa, Italy, Oct. 2007.

[18] Y. Hao, Y. Cheng, and K. Ren. Distributed key management with protection against RSU compromise in group signature based VANETs. In *IEEE Global Telecommunications Conference (IEEE GLOBECOM)*, pages 1–5, New Orleans, LA, USA, Dec. 2008.

[19] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki. Enhancing wireless location privacy using silent period. In *IEEE Wireless Communications and Networking Conference (WCNC)*, volume 2, pages 1187–1192, New Orleans, LA, USA, Mar. 2005.

[20] D. Jiang and L. Delgrossi. IEEE 802.11p: Towards an international standard for wireless access in vehicular environments. In *IEEE Vehicular Technology Conference, 2008 (VTC Spring 2008)*, pages 2036–2040, Marina Bay, Singapore, May 2008.

[21] Y. Jiang, M. Shi, X. Shen, and C. Lin. A tree-based signature scheme for VANETs. In *Global Telecommunications Conference (IEEE GLOBECOM 2008)*, pages 1–5, New Orleans, LA, USA, Dec. 2008.

[22] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen. Security in vehicular ad hoc networks. *IEEE Communications Magazine*, 46(4):88–95, Apr. 2008.

[23] X. Lin, X. Sun, X. Wang, C. Zhang, P. H. Ho, and X. Shen. Tsvc: Timed efficient and secure vehicular communications with privacy preserving. *IEEE transactions on Wireless Communications*, 7(12):4987–4998, December 2007.

[24] H. Moustafa, G. Bourdon, and Y. Gourhant. Providing authentication and access control in vehicular network environment. In *International Federation for Information Processing Security and Privacy in Dynamic Environment (IFIP SEC)*, volume 201, pages 62–73, Karlstad, Sweden, May 2006. Springer.

[25] H. Oguma, A. Yoshioka, M. Nishikawa, R. Shigetomi, A. Otsuka, and H. Imai. New attestation based security architecture for in-vehicle communication. In *Global Telecommunications Conference (IEEE GLOBECOM 2008)*, pages 1–6, New Orleans, LA, USA, Dec. 2008.

[26] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya. Architecture for secure and private vehicular communications. In *7th International Conference on Intelligent Transport Systems Telecommunications (ITST'07)*, pages 1–6, Sophia Antipolis, France, June 2007.

[27] B. Parno and A. Perrig. Challenges in securing vehicular networks. In *Workshop on Hot Topics in Networks (HotNets-IV)*, College Park, Maryland, USA, Nov. 2005.

[28] A. Perrig, R. Canetti, J. D. Tygar, and D. Song. The TESLA broadcast authentication protocol. *RSA CryptoBytes*, 5(2):2–13, 2002.

[29] M. Piorkowski, M. Raya, A. L. Lugo, P. Papadimitratos, M. Grossglauser, and J.-P. Hubaux. TraNS: realistic joint traffic and network simulator for VANETs. *ACM SIGMOBILE Mobile Computing and Communications Review*, 12(1):31–33, 2008.

[30] M. Raya and J.-P. Hubaux. The security of vehicular ad hoc networks. In *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN'05)*, pages 11–21, Alexandria, VA, USA, Nov. 2005. ACM.

[31] M. Raya, P. Papadimitratos, and J.-P. Hubaux. Securing vehicular communications. *IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications*, 13(5):8–15, Oct. 2006.

[32] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki. CARAVAN: Providing location privacy for VANET. In *Proceedings of Embedded Security in Cars (ESCAR)*, Cologne, Germany, Nov. 2005.

[33] X. Sun, X. Lin, and P.-H. Ho. Secure vehicular communications based on group signature and ID-based signature scheme. In *IEEE International Conference on Communications (ICC'07)*, pages 1539–1545, Glasgow, Scotland, June 2007.

[34] X. Sun, X. Lin, and P.-H. Ho. Secure vehicular communications based on group signature and ID-based signature scheme. In *IEEE International Conference on Communications (ICC '07)*, pages 1539–1545, June 2007.

[35] A. Wasef, Y. Jiang, and X. Shen. ECMV: Efficient certificate management scheme for vehicular networks. In *IEEE Global Telecommunications Conference (IEEE GLOBECOM 2008)*, pages 1–5, New Orleans, LA, USA, Dec. 2008.

[36] M. Wolf, A. Weimerskirch, and C. Paar. Security in automotive bus systems. In *Workshop on Embedded IT-Security in Cars (escar)*, Bochum, Germany, Nov. 2004.

[37] X. Yang, J. Liu, F. Zhao, and N. H. Vaidya. A vehicle-to-vehicle communication protocol for cooperative collision warning. In *Annual International Conference on Mobile and Ubiquitous Systems*, pages 114–123, Boston, Massachusetts, USA, Aug. 2004. IEEE Computer Society.

[38] Y. Yang, M. Marina, and R. Bagrodia. Evaluation of multihop relaying for robust vehicular internet access. In *Mobile Networking for Vehicular Environments*, pages 19–24, Anchorage, Alaska, USA, May 2007.

[39] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian. Security issues in a future vehicular network. In *European Wireless Conference*, pages 270–274, Florence, Italy, Feb. 2002.

[40] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen. An efficient identity-based batch verification scheme for vehicular sensor networks. In *The 27th Conference on Computer Communications (IEEE INFOCOM 2008)*, pages 246–250, Phoenix, AZ, USA, Apr. 2008.

[41] J. Zhang, L. Ma, W. Su, and Y. Wang. Privacy-preserving authentication based on short group signature in vehicular networks. In *The First International Symposium on Data, Privacy, and E-Commerce*, pages 138–142, Chengdu, China, Nov. 2007.

[42] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty. Privacy-preserving detection of sybil attacks in vehicular ad hoc networks. In *Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking and Servicess (MobiQuitous 2007)*, pages 1–8, Philadelphia, PA, Aug. 2007.