Security and Privacy in Vehicular Ad-Hoc Networks: Survey and the Road Ahead

M.A. Razzaque, Ahmad Salehi S., and Seyed M. Cheraghi

Faculty of Computer Science & Information Systems,
University of Technology,
Malaysia
marazzaque@utm.my,
ahmad.salehi.sh@gmail.com,
smcheraghi@yahoo.com

Abstract. Vehicular Ad-hoc Networks (VANETs) can make roads safer, cleaner, and smarter. It can offer a wide range of services, which can be safety and non-safety related. Many safety-related VANETs applications are real-time and mission critical, which would require strict guarantee of security and reliability. Even non-safety related multimedia applications, which will play an important role in the future, will require security support. Lack of such security and privacy in VANETs is one of the key hindrances to the wide spread implementations of it. An insecure and unreliable VANET can be more dangerous than the system without VANET support. So it is essential to make sure that "life-critical safety" information is secure enough to rely on. Securing the VANETs along with appropriate protection of the privacy drivers or vehicle owners is a very challenging task. In this work we summarize the attacks, corresponding security requirements and challenges in VANETs. We also present the most popular generic security policies which are based on prevention as well detection methods. Many VANETs applications require system-wide security support rather than individual layer from the VANETs' protocol stack. In this work we will review the existing works in the perspective of holistic approach of security. Finally, we will provide some possible future directions to achieve system-wide security as well as privacy-friendly security in VANETs.

Keywords: Security, Privacy, VANETs, Roadside Units, Key Management.

1 Introduction

It is now widely accepted by academician and industry that VANETs can significantly improve traffic safety, road efficiency and reduce environmental impact [1]. Studies [2] show that about 60% roadway collisions could be avoided if the driver of the vehicle was provided warning at least one-half second prior to a collision.

S. Khan and A.-S.K. Pathan (Eds.): *Wireless Networks and Security*, SCT, pp. 107–132.
DOI: 10.1007/978-3-642-36169-2_4

VANETs allow vehicles to communicate with each other (V2V) and/or with roadside infrastructure (V2R). Based on these communications VANETs can offer a wide range of services. In a report [3], US Dept. of Transport has already listed more than75 different application scenarios where it can be useful. These can be broadly categorized in two: safety and non-safety related services/applications. Many safety-related ITS applications are real-time and mission critical, which would require strict guarantee of quality of service (QoS), in terms of latency, error rate, and security. For instance, a safety message to prevent a probable accident has to reach concerned vehicles within a fraction of a second (e.g. 100ms [3]) so that the vehicles and their drivers can take necessary actions to prevent the accident. Security is key concern for future VANETs implementations. In VANET a road user will relay on it and does action accordingly whereas on typical systems user takes actions by his/her observation and knowledge. An insecure and unreliable VANET can be more dangerous than the system without it. So, secure VANETs system is more than necessary. Potential security measures could include a method of assuring that the packet/data was generated by a trusted source (neighbor vehicle, sensors, etc.), as well as a method of assuring that the packet/data was not tampered with or altered after it was generated. Any application that involves a financial transaction (such as tolling) requires the capability to perform a secure transaction.

Securing the VANETs along with appropriate protection of the privacy drivers or vehicle owners is a very challenging task. As the applications of VANETs are diverse, their communications and/or system-level security requirements could be diverse too. There are some very good works on VANETs' security and privacy [4-9], which review security related issues attacks, requirements, challenges, and security solutions. But none of these comprehensively covers all of these issues related VANETs' security and privacy except [9]. In [9] security and privacy implementation related issues are missing, precisely communication perspective. In this work we summarize the attacks, corresponding security requirements and challenges in VANETs. We also present the most popular generic security policies which are based on prevention as well detective methods. Many VANETs applications require system-wide security support rather than individual layer from the VANETs' protocol stack. In this work we will review the existing works in the perspective of holistic approach of security. Finally, we will provide some possible future directions to achieve system-wide security as well as privacy-friendly security in VANETs.

The rest of this book chapter is organized as follows. We first present a brief overview of VANETs in section 2. In section 3 we provide an elaboration of the possible adversaries and their possible attacks in VANETs. The security, privacy requirements and major challenging issues faced by VANETs to satisfy the security requirements are described in section 4. This section clearly shows how security and privacy my conflict in VANETs. Section 5 summarizes the generic security mechanisms including some specific attacks based works. We analyze the existing works and provide some future directions in section 6, before we conclude in section 7.

2 Overview of VANET

2.1 What Is VANET?

A modern vehicle can be considered as a network of sensors/actuators on wheels. VANET is a special kind of Mobile Ad-hoc Network (MANET) where vehicles equipped with the technologies are the key constituents. Generally, a VANET differs from MANET in the following aspects:

- Large scale – potentially billion
- Fleeting contact with other vehicles
- Nodes not as constrained in terms of energy, storage and computation.
- Higher mobility
- Privacy requirements

The single most important objective of a VANET is to provide communications between different vehicles on the roads and roads' environments (e.g. roads' condition, weather, traffic, etc.), to improve the driving experience and make driving safer. In doing so, in VANET each vehicle needs to have an OBU (On-Board Units)– communication devices mounted on vehicles and also a WSNs supported roadside unit (RSU) as shown in figure 1. By using OBUs, vehicles can communicate with each other as well as with RSUs. A VANET is a self-organized network that enables communications between vehicles and RSUs, and the RSUs can be connected to a backbone network, so that many other network applications and services, including Internet access, can be provided to the vehicles. So in VANET communications can be Vehicle to Vehicle (V2V)/inter vehicle and/or with roadside infrastructure (V2R) [10]. Figure 1 presents an example VANET, which shows possible communications within a VANET.

To make VANETs intelligent, it integrates multiple ad-hoc networking technologies such as WiFi IEEE 802.11p, WAVE IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA, ZigBee for easy, accurate, effective and simple communication between vehicles on dynamic mobility. One of the IEEE1609 (P1609.2) explicitly defines security, secure message formatting, processing, and message exchange. Use of these technologies in VANETs helps in defining safety measures in vehicles, streaming communication between vehicles, infotainment and telematics. VANETs are expected to implement a variety of wireless technologies such as Dedicated Short Range Communications (DSRC), are one or two way short- to medium-range wireless communication channels explicitly designed for automotive use and a corresponding set of protocols and standards. Other candidate wireless technologies are Cellular, Satellite, and WiMAX. VANETs can be envisioned as the most important entity of the Intelligent Transportation Systems (ITS) [1, 3, 10].

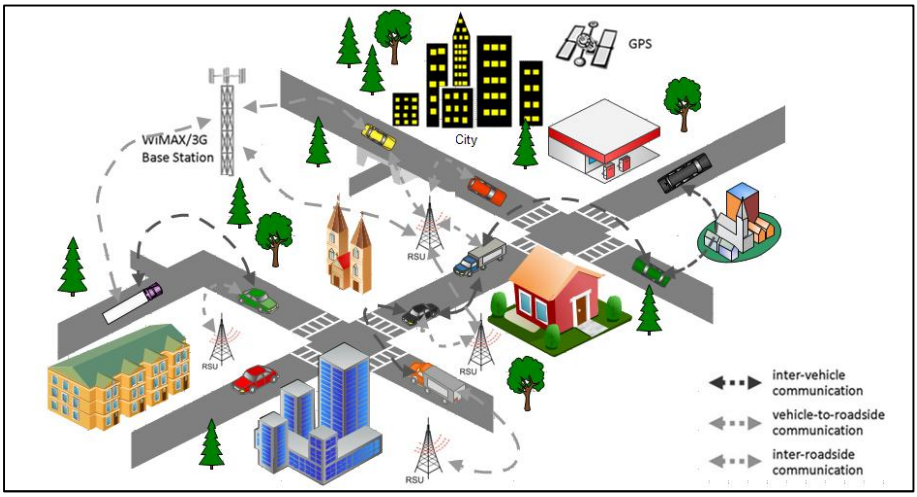


Fig. 1. An example of VANET

2.2 Applications of VANETs

VANETs can offer a wide range of services or applications. In a report [3], US Dept. of Transport has already listed more than75 different application scenarios where VANETs can be useful. These applications can be broadly categorized in two: safety and non-safety related services/applications. Congestion control is one of the non-safety related applications. As shown in Table 1, a little reduction in congestion can contribute very significantly. A snapshot of key applications of VANETs is presented in figure 2.

Table 1. Cost of Congestion in few developed Countries [1]

Country	Congestion Cost (billion$)
USA	200 (890 within 20yrs)
Japan	109
Australia	12.5
UK	35

3 Adversaries and Attacks

Knowing the type and the resources of the adversary can greatly help in determining the scope of the defenses required to secure a VANET. It is really hard to make a precise list of all the possible adversaries in any security system. A realistic analysis

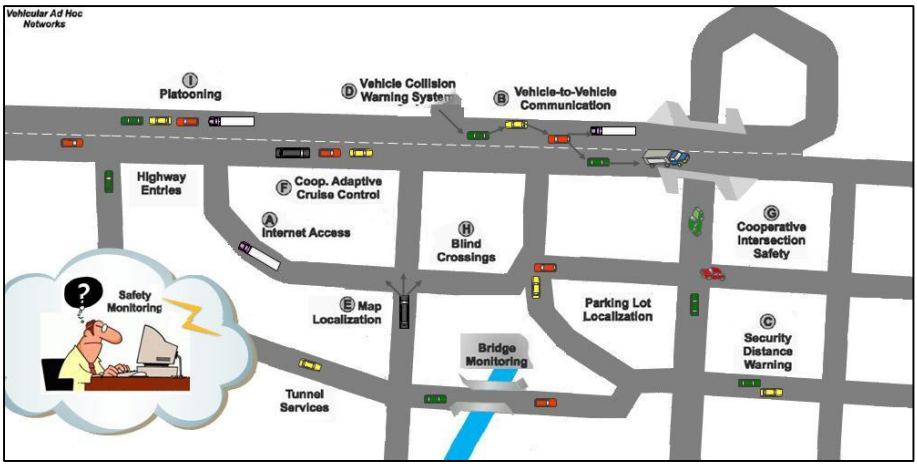


Fig. 2. Possible Applications of VANETs [11]

of the application environment can help in finding the type of typical adversaries. Thus VANETs environment recommends the following categories of adversaries [12, 13]:

Greedy Drivers: It is highly unexpected that all drivers in the system will be trusted to follow the protocols specified by the application. Always there will be some drivers who will attempt to maximize their gains, regardless of the cost to the system. For example, in a congestion control system, a greedy driver might attempt to convince the nearby vehicles that there is considerable congestion ahead, so that they will move to alternate routes and allow the greedy driver a clear path to his/her destination.

Eavesdroppers (Snoops): This type of adversary can includes everyone from a nosy next-door neighbor to a government agency trying to profile drivers. For example, companies may want to track consumers' purchasing habits and use correlated data to alter prices and discounts. Data mining to find pattern over aggregated data may be acceptable, but it can easily conflict with users' privacy concerns if one can extract identifying information about a person.

Pranksters: Like computer and network security, pranksters could be a serious adversary in VANETs. It includes jaded teenagers searching for vulnerabilities and hackers looking for fame via their exploits. For example, a prankster siting by the road can easily create "intelligent collision" by convincing one vehicle to slow down while persuading the vehicle behind it to speed up. The hard real-time response requirement in VANETs potentially leaves it vulnerable to DoS attacks. A prankster could exploit this vulnerability to disable applications or prevent critical information from reaching targeted vehicle.

Industrial Insiders: Inside attackers are very deceptive, and hard defend them. The extent to which VANETs are vulnerable to these depends on other security design decisions. For instance, any mechanic who can update the software on a vehicle can also has the chance to load malicious software. If vehicle makers are in charge of key distribution, then a single rogue employee at one maker could create keys that would be accepted by all other vehicles.

Malicious Attackers: This category of adversary deliberately attempt to cause harm via the applications available on the VANETs. Usually, these attackers have specific targets, and they have access to more resources than the aforementioned attackers. For instance, terrorists might manipulate the warning system to create jam before detonating a bomb. On the other hand criminals might spoof the congestion control application to facilitate getaways. In general, while this class of attackers rarer than those outlined above; their combination of resources and directed malice makes them a serious concern for any security system.

3.1 Attacks

Like other networks attacks in VANETs can be classified into the following categories [12, 13]:

- *Outsider vs. insider attacks:* Outside attacks are defined as attacks from nodes which do not belong to a VANETs; insider attacks occur when legitimate vehicle or node of a VANETs behave in unintended or unauthorized ways.
- *Passive vs. active attacks:* Passive attacks include eavesdropping on or monitoring packets exchanged within a VANET; active attacks involve some modifications of the data steam or the creation of a false stream.
- *Malicious vs. rational:* Usually, a malicious attacker looks for no personal benefits from the attacks, just aims to harm the users or network. Hence, attacker may employ any means disregarding corresponding costs and consequences. On the other hand, a rational attacker looks for personal benefit and hence is more predictable compared to a malicious attacker.
- *Local vs. extended*: An attacker can be limited in scope, even if he controls several entities (vehicles or base stations), which makes him local. An extended attacker controls several entities that are scattered across the network, thus extending his scope. This distinction is especially important in privacy-violating and wormhole attacks that we will describe shortly.

It is also possible to categorize attacks in according to the security requirements in VANETs as:

- *Attacks on secrecy and authentication:* Standard cryptographic techniques can protect the secrecy and authenticity of communication channels from outsider attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets.

- *Attacks on network availability:* Attacks on availability are often referred to as denial-of-service (DoS) attacks. DoS attacks may target any layer of a sensor network.
- *Stealthy attacks against service integrity:* In a stealthy attack, the goal of the attacker is to make the network accept a false data value.

Being a special implementation of MANETs supported by WSNs (RSUs), a VANET inherits all the known and unknown security weaknesses associated with MANETs and WSNs, and could be subject to many security and privacy threats. In this context we obviously cannot anticipate every possible attack on VANETs; we can enumerate some of the more likely scenarios and ensure that applications are robust against this known set of potential attacks. These attacks can be concerned with the physical security of VANET and messages communicated within it. Here we consider only the attacks against messages rather than vehicles, as the physical security of vehicle electronics is out of the scope of this work. Message related attacks in VANETs can be summarized [13] as below:

Denial of Service (DoS): Like any other networks, it is a very common attack where the attacker can overpower a vehicle's resources or jam the communication channel used by the VANET to bring down the VANET or even cause an accident. This attack is active and malicious in nature. For instance, if a malicious adversary wants to create a massive pileup on the highway, he could provoke an accident and then use a DoS attack to prevent the dissemination of warnings message to other drivers. As shown in figure 3 (iii) jamming can easily cause DoS in VANETs.

Fabrication Attacks: An attacker can initiate a fabrication attack by broadcasting false or bogus information into the network. For example, a greedy driver might behave as an emergency vehicle to speed up his/her own journey. An attacker may also fabricate his/her own information related to his/ her identity, location, or other application-specific parameters. Finding an appropriate defense mechanism against fabrication attacks in VANETs is particularly challenging, as the customary remedy of using strong identities along with cryptographic authentication may conflict with the privacy requirements of drivers or vehicle owners. This generic attack has some variants (may not be mutually exclusive) which are important for VANETs as below [9, 12, 13]:

i. **Bogus Information:** Attackers of this attack are generally insider, rational and active as shown in figure 3(i). They diffuse wrong information in the network to affect the behavior of other drivers (e.g., to divert traffic from a given road and thus free it for themselves).
ii. **Cheating with Sensed Information:** Attackers of this category are insider, rational, active and local who exploit this attack to alter their perceived position, speed, direction, etc. in order to escape liability, notably in the case of an accident.
iii. **Hidden Vehicle:** Here fabrication happens on positioning information. It follows the basic safety messaging protocol described [12], a vehicle broadcasting

warnings will listen for feedback from its neighbors and stop its broadcasts if it realizes that at least one of these neighbors is better positioned for warning other vehicles. As shown in figure 3 (vi), the hidden vehicle attack consists in deceiving vehicle A into believing that the attacker B is better placed for forwarding the warning message, thus leading to silencing A and making it hidden to other vehicles. This ultimately stops the dissemination of the warning message, hence causing a DoS.

iv. **Tunnel:** As in GPS signals disappear in tunnels or underground, an attacker can exploit this temporary loss of positioning information to inject false data once the vehicle leaves the tunnel and before it receives an authentic position update as shown in figure 3 (iv). An area jammed by the attacker may cause the same effects.

v. **Masquerading:** The attacker of this kind actively pretends to be another vehicle by using false identities and can be driven by malicious or rational objectives. Intelligent collision (figure 3 (ii)) is an example of this attack.

Message Suppression Attacks: It is a delicate attack where the attacker may use one or more vehicles to launch a suppression attack by selectively dropping packets from the network. Some popular attacks of MANETs or WSNs such as selective forwarding, black-hole falls under this generic category. For instance, a prankster might suppress congestion avoidance message before selecting an alternate route, thus trapping subsequent vehicles to wait in traffic.

Alteration Attacks: It is an active and inside attack in VANETs that aims to alter existing data. It includes on purpose delaying the transmission of information, replaying earlier transmissions or altering the individual entries within a transmission. For example, if the traffic congestion application requires a vehicle to collect "votes" from other vehicles at the site of the congestion, then an attacker might collect votes while traveling in normal traffic, but alter the locations and timestamps in the votes to make it appear that all of those vehicles were in the same place at the same time, deceitfully indicating a heavily congested highway. A malicious attacker might alter a message alerting vehicles to an obstacle ahead to convince another vehicle that the way is in fact clear.

Tracking: This attack requires ID disclosure of other vehicles. A central monitoring can be used to monitor trajectories of targeted vehicles and use this data for a range of purposes (e.g., the way some car rental companies track their own cars). For the monitoring, the passive attacker can exploit the roadside infrastructure or the vehicles around its target (e.g., by using a virus that infects neighbors of the target and collects the required data). An example of this sort of attack is shown in figure 3(v), where car A is under tracking attack.

Wormhole: In wireless networking attack, this attack consists in tunneling packets between two remote nodes. Similarly, in VANETs, an attacker that controls at least two entities distant from each other and a high speed communication link between them can tunnel packets broadcasted in one location to another, thus disseminating erroneous (but correctly signed) messages in the destination area.

4 Challenges and Security Requirements in VANETs

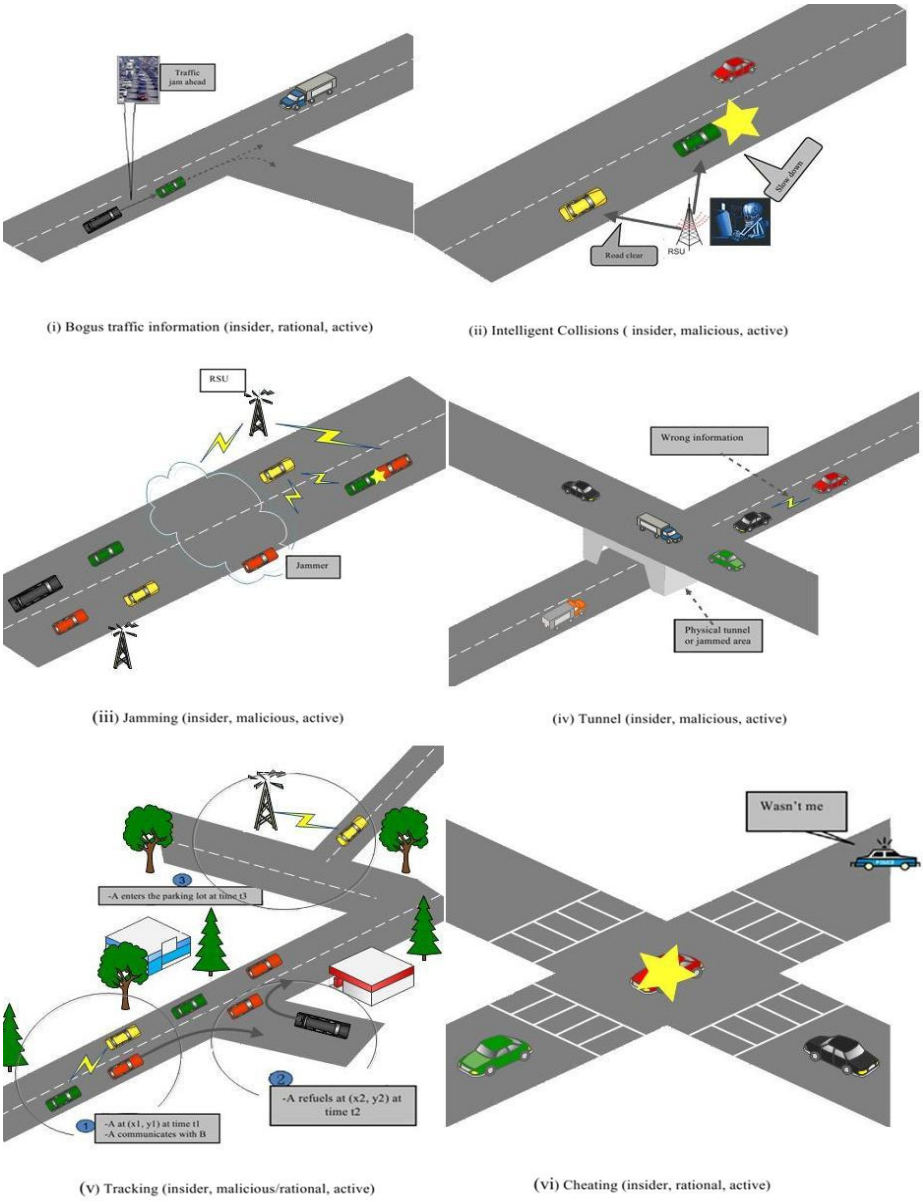
4.1 Security Requirements

As the applications of VANETs are diverse, their communications and/or system-level security requirements could be diverse too. Potential security measures should include a way of assuring that the packet/data was generated by a trusted source, as well as a way of assuring that the packet/data was not tampered with or altered after it was generated.

VANETs pose some of the most challenging problems in MANETs and WSNs research. In addition, the issue of security in VANETs is particularly challenging due to the unique features of the network, such as high-speed mobility of network nodes or vehicles and the extremely large amount of network entities. It is obvious that any malicious user behavior, such as an alteration and replay attack of the disseminated messages, could be disastrous to other users. So in any situation, it is necessary to make sure that "life-critical safety" information cannot be altered by attackers. A security system needs to be capable of establishing the liability of drivers, while preserving their privacy as much as possible. Considering the aforementioned attacks and suggestion made in other works, VANET security should satisfy the following requirements [3, 12, 13]:

i. **Authentication:** This is the most important requirement in preventing most of the aforementioned attacks in VANETs. Vehicle responses to events should be based on legitimate messages (i.e., generated by legitimate users). Therefore we need to authenticate the OBUs, RSUs and senders of these messages.
ii. **Verification of Data Consistency:** The legality of messages also comprises their consistency with similar ones (those generated in close space and time), as the sender can be legal but the message contains false data. This requirement also known as "plausibility".
iii. **Message Integrity:** Message alteration is very common and crucial attacks in VANETs. We need to maintain the integrity of the message to prevent the alteration attacks.
iv. **Availability:** Attacks like (e.g., DoS by jamming) bring the VANETs down even the considered communication channel is robust. So, availability should be provided by some other means.
v. **Non-repudiation:** Drivers causing accidents should be reliably identified to prove his/her liability. Based on this principle, a sender will not be able to refuse the transmission of a message (it may be key for investigation in determining the correct sequence and content of messages exchanged before the accident).
vi. **Privacy:** People are increasingly cautious of being monitored or tracked. Hence, the privacy of drivers or vehicle owners against unauthorized observers should be protected.
vii. **Traceability and Revocation:** Trace and disable abusing OBUs or RSUs by the authority.

viii. **Real-Time Constraints:** At the very high speeds typical in VANETs, strict time constraints should be respected. This ultimately imposes computation and communication wise efficient schemes.



(i) Bogus traffic information (insider, rational, active)

(ii) Intelligent Collisions (insider, malicious, active)

(iii) Jamming (insider, malicious, active)

(iv) Tunnel (insider, malicious, active)

(v) Tracking (insider, malicious/rational, active)

(vi) Cheating (insider, rational, active)

Fig. 3. Few explicit attacks in VANETs [12, 13]

4.2 Challenges

VANETs pose some of the most challenging problems in MANETs and sensor network research. Some of the key challenges [12, 13, etc.] which directly or indirectly related to security of VANETs are summarized below.

Mobility: In general sensor networks often assume a relatively static network, and even MANETs usually assume limited mobility. For vehicular networks, mobility is the norm, and it will be measured in miles, not meters, per hour. This high mobility causes frequent dis-connectivity; hence make the communications highly unreliable which makes security more challenging. The mobility patterns of vehicles on the same road will show strong correlations. Each vehicle will have a frequently shifting set of neighbors, many of whom it has never communicated with before and is unlikely to communicate with again. The short-lived nature of interactions or communications in a VANET will limit the efficacy of reputation-based schemes. For instance, rating other vehicles based on the reliability of their incident reports is unlikely to prove useful; a specific driver is unlikely to receive multiple reports from the same vehicle. Additionally, as two vehicles may only be within communication range for a very short period (e.g. few seconds), we cannot rely on protocols that require significant communication between the sender and receiver.

Privacy vs. Security: Like other IP-based networks (e.g. Internet, MANETs, etc.), it highly desirable to bind each driver or vehicle to a single identity to prevent Sybil or other spoofing attacks. For instance, in the congestion control scheme, it is necessary to prevent one vehicle from claiming to be hundreds in order to create the illusion of a congested road. Authentication is a key security requirement for VANETs that provides valuable forensic evidence and allows us to use external mechanisms, such as traditional law enforcement, to deter or prevent attacks on VANETs. However, drivers or other vehicle users value their privacy and are unlikely to adopt systems that require them to abandon their anonymity. For instance, if we try to prevent spoofing in a way that reveals each vehicle's permanent identity, then we may violate drivers' or users' privacy requirements. So privacy compliant security policies are needed that will require codifying legal, societal and practical considerations. Most countries have widely divergent laws concerning their citizens' right to privacy. As most vehicle makers operate in multinational markets, they will need security solutions that satisfy the most stringent privacy laws, or that can be customized to meet their legal obligations in each market. Authentication schemes must also consider societal expectations of privacy against practical considerations. Vehicles today are not fully anonymous as each vehicle has a publicly displayed license plate that uniquely identifies it and identifies the owner of the car, given access to the appropriate records. Hence, drivers have already sacrificed a portion of their privacy while driving. So, security policies in VANETs should build on these existing compromises instead of encroaching any further upon a driver's right to privacy.

Availability: Number of VANETs applications especially safety-related require real-time, or near real-time, responses and hard real- time guarantees. Other applications

may tolerate some margin in their response times; still this requirement is faster than those expected in traditional WSNs or MANETs. However, attempts to meet real-time demands could make applications vulnerable to Denial of Service (DoS) attacks. For instance, in the deceleration application, a delay of even less than a second can render the message meaningless. The problem is further aggravated by the unreliable communications. The current DSRC standard provides an acceptable latency and high data rate; the reliability is still missing [14]. Since vehicles moving in opposite directions will remain within communications range for only a few seconds, opportunities to retry a broadcast will be limited.

Low Tolerance for Errors: Many applications can afford security protocols that rely on probabilistic schemes. However, in VANETs' safety (mission-critical) related applications, even a small probability of error will be unacceptable. Number of vehicles in the world is in billions, even if an application that functions correctly 99.99999999% of the time, the application is still more likely to fail on at least one vehicle than function correctly on all vehicles. So margin of error of any security protocol in VANETs based on deterministic or probabilistic scheme is infinitesimally small. Additionally, for many applications, security must focus on prevention of attacks, rather than detection and recovery. In MANETs it may suffice to detect an attack and alert the user, leaving recovery and clean-up to the humans. However, in many safety-related VANETs applications, detection will be inadequate, as by the time the driver can react, the warning may be too late. So security must focus on preventing attacks in the first place, which requires extensive foresight into the types of attacks likely to occur.

Key Distribution: Key distribution is often a fundamental building block for security protocols. In VANETs, key distribution faces several significant challenges. First, vehicles are manufactured by many different companies, so installing keys at the factory would require coordination and interoperability between manufacturers. If manufacturers are unable or unwilling to agree on standards for key distribution, then we could turn to government-based distribution. Within a country it can hierarchically go to states and then districts that make the coordination complicating. The government can impose standards, but doing so would require significant changes to the current infrastructure for vehicle registration, and thus is unlikely to occur in the near future. However, without a system for key distribution, applications like traffic congestion detection may be vulnerable to spoofing, sybil attacks. A potential approach for secure key distribution would be to empower the Motor Vehicles licensing authority to take the role of a Certificate Authority (CA) and to certify each vehicle's public key. Unfortunately, this approach has number of weaknesses. Moreover, certificate-based key establishment has the danger of violating driver privacy, as the vehicle's identity is revealed during each key establishment. So finding a realistic and privacy friendly key distribution technique is a challenging issue in VANETs.

Cooperation: Successful deployment of VANETs will require cooperation amongst vehicle manufacturers, consumers, and the government, and reconciling their frequently conflicting interests will be challenging. For instance, law-enforcement agencies might quickly adopt a system in which speed-limit signs broadcast the mandated speed and vehicles automatically reported any violations. Understandably, consumers might reject such invasive monitoring, giving vehicle manufacturers little incentive to include such a feature. Equally, consumers might appreciate an application that provides an early warning of a police speed trap. Manufacturers might be keen to meet this demand, but law-enforcement is unlikely to do so.

5 Securing VANETs

Securing VANETs is a very challenging due to the unique features of networks, such as the high-speed mobility of the nodes and the extremely high node density. Moreover, conditional[1] privacy preservation of drivers or vehicle owner crucial information (including the driver's name, license plate, speed, position, and traveling routes along with their relationships) makes it even harder. Thus, it is critical to develop a group of elaborate and carefully designed security mechanisms for achieving security and conditional privacy preservation in a VANET. Up to recently, however, security and privacy issues of VANETs have been given little attention. Lack of such security and privacy concerns have formed the major barrier, preventing many drivers from employing state-of-the-art smart automobile technologies.

In this section we review the existing VANETs security mechanisms. In earlier part of this section we will discuss the generic VANETs security mechanisms and in later part we will discuss on specific mechanism or solutions.

5.1 Generic Security Mechanisms

Like any other networks (e.g. MANETs, WSNs, etc.) security mechanisms in VANETs can be based on prevention (proactive) and detection (reactive) techniques. Considering the criticality nature of VANETs application, preventive security mechanisms are important than the reactive ones. Hence, most of the existing security mechanisms [10, 11, 13, etc.] in VANETs aim to prevent security attacks rather than detect. Even though works on detection techniques in VANETs are very limited, the usefulness of these can be significant in number of situations. For instance, in case of any fabrication attack if prevention mechanism fails, reliable and efficient detection of the fabrication can help drivers in taking the correct action in that situation. Most of the existing security mechanisms directly or indirectly employ cryptography. So, in the first part of this section we briefly introduce the possible key management approaches and keys [12] in VANETs and then we present the three

[1] Conditional means: the authorities should be able to reveal the identities of message senders in case of dispute such as a crime/car accident scene investigation, which can be used in seeking witnesses.

prevention security mechanisms, which are considered to be the most promising candidates to increase security in VANETs. Later part of this section we briefly present reactive based detection techniques.

5.1.1 Key Management

For the cryptographic approaches we need *unique information* about the vehicles which can be an electronic identity called an Electronic License Plate (ELP) [16] issued by a government, or an Electronic Chassis Number (ECN) issued by the vehicle manufacturer. These unique IDs are needed to identify vehicles to the police in case this is required (usually, identities are hidden from the police). Like license plates, the ELP should be changed (i.e., reloaded in the vehicle) when the owner changes or moves, e.g., to a different region or country. But these unique IDs may disclose privacy of the drivers, so anonymous key pairs that can be used to preserve privacy. An anonymous key pair is a public/private key pair that is authenticated by the CA but contains neither information about nor public relationship with the actual ID of the vehicle such as ELP. For the liability purposes this anonymity is conditional. Usually a vehicle will own a set of anonymous keys to prevent tracking. In the following we briefly present the main activities necessary for key management in VANETs.

- *Key bootstrapping and rekeying:* It is an important activity in key management. Like the physical license plate, it should be "installed" in the vehicle using a similar procedure, which means that the governmental transportation authority will preload the ELP at the time of vehicle registration (in the case of the ECN, the manufacturer is responsible for its installation at production time). Anonymous keys are preloaded by the transportation authority or the manufacturer (briefly mentioned in earlier section). As ELPs are unique and fixed, should attach to the vehicle for a long duration, but anonymous key sets have to be periodically renewed after all the keys have been used or their lifetimes have expired.
- *Key certification:* As briefly mentioned in earlier section, governmental transportation authorities or vehicle manufacturer can act as a CA in VANETs but this is not at all an easy process.
- *Key revocation:* Key revocation is necessary to punish the wrong doers in VANETs. One way to do this is to revocate the certificate related to the wrong doer. For instance, the certificates of a detected attacker or malfunctioning device have to be revoked, i.e., it should not be able to use its keys or if it still does, vehicles verifying them should be made aware of their invalidity. The simplest we can do so by distributing CRLs (Certificate Revocation Lists) that contains the most recently revoked certificates; CRLs are provided when infrastructure is available. There are number of ways we can do the revocation. Such as short-lived certificates method proposed in IEEEP1609.2/D2 draft standard [17] automatically revokes keys. It has number of shortcomings which are aimed to solve in RTPD (Revocation Protocol of the Tamper-Proof Device), RCCRL (Revocation protocol using Compressed Certificate Revocation Lists), and DRP (Distributed Revocation Protocol) [18].

- *Anonymous public keys:* There are several types of privacy. As safety messages will not contain any secret data about their senders, vehicle owners will be only concerned about identity and location privacy. Even though anonymous keys do not contain any publicly known relationship to the true identity of the key holders, privacy can still be hijacked by logging the messages containing a given key and thus tracking the sender until discovering his identity (e.g., by associating him with his place of living). Therefore, anonymous keys should be changed in such a way that a pervasive observer cannot track the owner of the keys. But it will require a vehicle to store a large key and certificate set (depending on the key changing frequency). So generation of efficient and reliable anonymous public keys is an open issue.

5.1.2 Prevention Techniques

- **Digital Signature-Based Techniques:** Digital signature is the building block of these security mechanisms, which primarily aim at providing message authenticity. Along with the digital signature, these techniques can exploit cryptography with certification or without certificate [15].
- *Without Certificate:* In this approach cryptographic digital signatures are apply to messages or hashes over messages. Digital message signatures are usually formed by asymmetric cryptography, i.e. by using public-private key cryptography. Messages (or hashes over the respective messages) are signed with the message originators' private keys. This approach can provide three security improvements to communication, namely message authenticity, message integrity protection and non-repudiation. The key advantage of this approach is that that it is simple to realize with small requirements. Mechanisms [shen] based on this approach are widely deployed and well known. However attacks like message forging, DoS, sybil are still possible. Moreover, the approach does not prevent attackers to create fake warning messages.
- *With Certificates:* In order to enhance the above approach, the signatures can be combined with digital certificates provided by a trusted Certificate Authority (CA). The basic notion with certificates is that nodes, which include certificates in their messages, are trusted by other nodes that are able to verify the certificates. The signed messages include a certificate which is cryptographically linked to the public key that belongs to the private key the message issuer uses to sign messages. The advantage of the certificate concept lies in the possibility to exclude external attackers from the system, as well as in the ability to remove malicious or defective nodes. With the support of suitable mechanisms it can also prevent sybil attacks.

  This is the most widely discussed and popular security mechanism in VANETs. Numerous studies and standards exploit certificate-based cryptosystem to support security for VANETs [7, 19-26, 39, etc.]. For instance, authors in [25] propose a vehicular PKI, based on a certificate-based PKC (digital signature) scheme to support security services for message exchange in the VANETs environment. A security architecture based on certificate-based PKC mechanism

for VANETs discussed in [20]. However, secure messaging based on digital sign with certificate scheme has a number of limitations, including complexity in certificate verification and management, scalability, performance in a large-scale environment, and timely access to certificate revocation information. Some of the works already acknowledged the shortcomings of using digital sign with certificate–based scheme in VANETs [22]. There has been, however, hardly any discussion on how to improve the scalability of employing certificate-based PKC (digital signature) for VANETs.

- **Proprietary System Design:** This category of security mechanisms aim to exploit non-public (proprietary) protocols or hardware to control the unauthorized access to the networks. In case the protocols or hardware remain undisclosed (or highly expensive), like the certificate approach, this concept prevents non-authorized nodes from participating in the network. Ultimate objective of this concept is to increase the required effort an attacker has to put in order to enter into the system. This scheme does not prevent him from doing so, nor do they prevent any attack from an insider. For example, an attacker is still able to distribute fake warning messages using a vehicle's safety communication system. This approach seems not that promising, as vehicle manufacturers are aiming at the development of a common and open standard for the communication system.

- **Temper Proof Hardware:** In order to complement the aforementioned mechanisms, Tamper Resistant Device (TRD) or Tamper-Proof Device (TPD) hardware is meant to provide secure input to the communication system, by securing the in-vehicle communication system and protecting it from manipulation. Along with the storing secret information, this device will be also responsible for signing outgoing messages. To protect itself of being compromised by attackers, the device should have its own battery, which can be recharged from the vehicle, and clock, which can be securely resynchronized, when passing by a trusted roadside base station. The access to this device should be limited to authorized people. For instance, cryptographic keys can be renewed at the periodic technical checkup of the vehicle. Usually, the TPD contains a set of sensors that can detect hardware tampering and erase (self-destructive) all the stored keys to prevent them from being compromised. This sophisticated feature makes the TPD too sensitive for VANET conditions (e.g. the device can be subject to light shocks because of road imperfections, etc.) as well as too expensive for non-business consumers. A TPM (Trusted Platform Module [27]) that can resist to software attacks but not to sophisticated hardware tampering can be an alternative option to a TPD. These are popular in notebooks and cost only a few tens of dollars. The ultimate notion on of the security hardware will depend mainly on economic and technical factors. A tradeoff between TPD and TPM can be good guide to define it.

5.1.3 Detection Techniques

It is very unlikely that a proactive security measure will be always successful in preventing it concerned attacks. If it fails, then it may lead to a disastrous situation as

VANETs is dealing with life-critical applications. In this situation, detection techniques can help us in avoiding disastrous happenings. For instance, as shown in figure 3(ii) if prevention method fails to detect the possible collision than collision between the cars are must. If we can employ a reliable and efficient detection method which can identify in real-time that the attacker has sent bogus message, then it is possible avoid the collision.

These reactive measures are similar to the intrusion detection of other networks. Both the techniques correlate information which is either already available from normal system operation, or which is introduced additionally. Intrusion detection systems or similar systems for VANETs are still hardly explored (initial publications are [28] and [29]). These systems comprise what is also referred to as plausibility checks, information verification, use of side-channel information or context verification. In VANETs, or more precisely for safety systems in VANETs, reactive security mechanisms have to aim at detecting bogus or fabricated information in warning messages and inconsistencies in the inter-vehicle communication system. To do so, upon the reception of warning messages, nodes assess the validity of the warnings and then process the messages accordingly. If the message content is found to be invalid or bogus, the nodes ignore the message (some systems even try to correct the invalid data) and take action accordingly. Moreover, they may communicate their trusted neighbors to share the experiences.

In detecting security threats in VANETs, along with the common signature based and anomaly based detections we can exploit the contexts of a VANET and its application to detect attacks on it.

- **Signature-Based Detection:** In signature-based detection attacks can be detected by comparing network traffic to known signatures of attacks. As soon as an attack is detected appropriate countermeasures can be initiated. The primary concern of this approach is to realize a mechanism that is capable to detect known attacks on a communication system. The advantages of this detection technique are that it is simple and usually provides reliable detection of known attacks. The frequent updates of the attack signature database, the slow reaction on new attacks and of course the difficulty to define attack signatures are the shortcomings of this detection technique.
- **Anomaly Detection:** This approach is based on a statistical approach that defines normal communication system behavior. Any deviation from that behavior is statistically analyzed and as soon as they reach a defined level, the security system concludes that there is an attack ongoing. The advantage of this detection technique is that it enables the detection of previously unknown attacks without requiring an attack database to be updated. But, there are also some disadvantages. The definition of normal system behavior is pretty complex and anomaly detection is known to produce many false positives.
- **Context Verification:** Context verification is an approach that specifically considers the properties of VANETs and applications in VANETs. The notion is to collect as much information from any information source (e.g. the warning system, data from telemetric monitoring, etc.) available by each vehicle and create an independent view of its current status, its current surrounding (physical)

environment and current or previous neighboring vehicles. In order to do the evaluation of the situation this approach will require to define of rule-sets that determine what is to be expected with which probability in which situation. Situation evaluation mechanisms can be either application independent or application dependent. In application independent case, it can exploit position as well as time related information. On the other hand application context dependent evaluation exploits parameters specific to a certain application.

5.1.4 Standards

In the following we briefly review the IEEE 1609.2 and the Vehicle Safety Communications (VSC) project, which specify methods of securing Wireless Access in Vehicular Environments (WAVE) messages against numerous attacks, such as eavesdropping, alteration, source spoofing, message modification, and replays [30, 31]. This standard is still under revisions.

IEEE 1609.2 and the VSC Project: The IEEE 1609 WAVE communication standards, also known as DSRC protocols, have formed recently to enhance 802.11 to support wireless V2V and V2R communications in VANETs [31]. The IEEE 1609.2 standard addresses the issues of securing WAVE messages against eavesdropping, spoofing, and other attacks. As shown in figure 4, the components of the IEEE 1609.2 security infrastructure are based on industry standards for public key cryptography. It also includes support for elliptic curve cryptography (ECC), WAVE certificate formats, and hybrid encryption methods, in order to provide secure services for WAVE communications. The security infrastructure is also in charge of the administrative functions necessary to support core security functions such as certificate revocation (ongoing work). IEEE 1609.2 yet to define driver identification and privacy protection, and has left a lot of issues open. On the other hand, the VSC project also evaluates the feasibility of supporting vehicle safety related applications through the DSRC standard. It proposes to maintain a list of short-lived anonymous certificates for the purpose of keeping the privacy of drivers. Once the certificates are used, they are discarded. The scheme can provide higher security assurance as the certificates are blindly signed by the certificate authority (CA) in order to deal with any possible insider attack. The CA can abuse its authority and mishandles driver information. A linkage marker is devised for the escrow authorities to associate each blindly signed anonymous certificate with a single vehicle. All compromised and expired vehicles will be revoked by putting certificates belonging to those vehicles into the certificate revocation list (CRL). The main drawback of this scheme is that the CRL may grow quickly and make the real-time validation of certificates impossible. Another shortcoming depends on the fact that for tracing purpose, a unique electronic identity is assigned to each vehicle by which the identity of the vehicle owner can be inspected by the police and authorities in any dispute. Even though this scheme can effectively fulfill the conditional anonymity requirement, it is far from efficient, and suffers in scalability and reliability as the ID management authority has to keep all the anonymous certificates for the vehicles in the administrative region. Once a malicious message is discovered, the authority has to

exhaustively search a huge database to find the identity related to the compromised anonymous certificate. To solve these issues, in [6] authors have presented an effective and efficient solution for achieving certificate revocation and conditional privacy preservation.

SeVeCom Project [32]: The SeVeCom project defines a baseline security architecture for VANETs systems. The baseline architecture contains different modules, which addresses different aspects, such as secure communication protocols, privacy protection, and in-vehicle security. The baseline specification provides one instantiation of the baseline architecture, building on well- established mechanisms and cryptographic primitives, thus being easy to implement and to deploy in upcoming VANETs. As shown in figure 5, the security manager is the central part of the SeVeCom system architecture. It instantiates and configures the components of all other security modules and establishes the connection to the cryptographic support module. To deal with different situations, the security manager maintains different policy sets, which can adaptively enable or disable some of the components or adjust their configuration. Even though this architecture is not yet accepted as standard, still it can be exploited as a good guideline for the implementation of security and privacy in VANETs.

5.2 Specific Security Solutions for VANETs

Majority of the existing works address the generic security policies rather than their implementation. Works on the implementation of overall security policies are very limited. Most of the existing works target to detect or prevent very specific attacks, such as sybil [33], DoS [34], etc. Moreover to achieve the full guarantee of security of message intensive VANETs applications, along with the message security in communion security is also necessary. To have a complete secure communication in VANETs, it is necessary have the support from all the layers of communication protocol stack (e.g. TCP/IP) rather than individual layer. Most of the existing research works (e.g. [35, 36, 37, 38, etc.]) on VANETs' security implementation focus on specific layer issues (e.g. routing, link, etc) rather than stack-wide. Moreover, these layer specific works are dominated by secure routing, few on secure MAC for VANETs. In the following we first briefly present few works which addresses some specific attacks and then present secure routing and secure MAC in VANETs respectively.

5.2.1 Specific Attack-Based Solutions

Privacy-Preserving Detection of Abuses of Pseudonyms (P2DAP) [33] explicitly targets sybil attacks in VANETs. It presents a lightweight and scalable protocol to detect Sybil attacks. In this protocol, a malicious user pretending to be multiple (other) vehicles can be detected in a distributed manner through passive overhearing by RSUs. In this scheme, detection of Sybil attacks does not require any vehicle in the network to disclose its identity; hence privacy is preserved at all times. It can detect

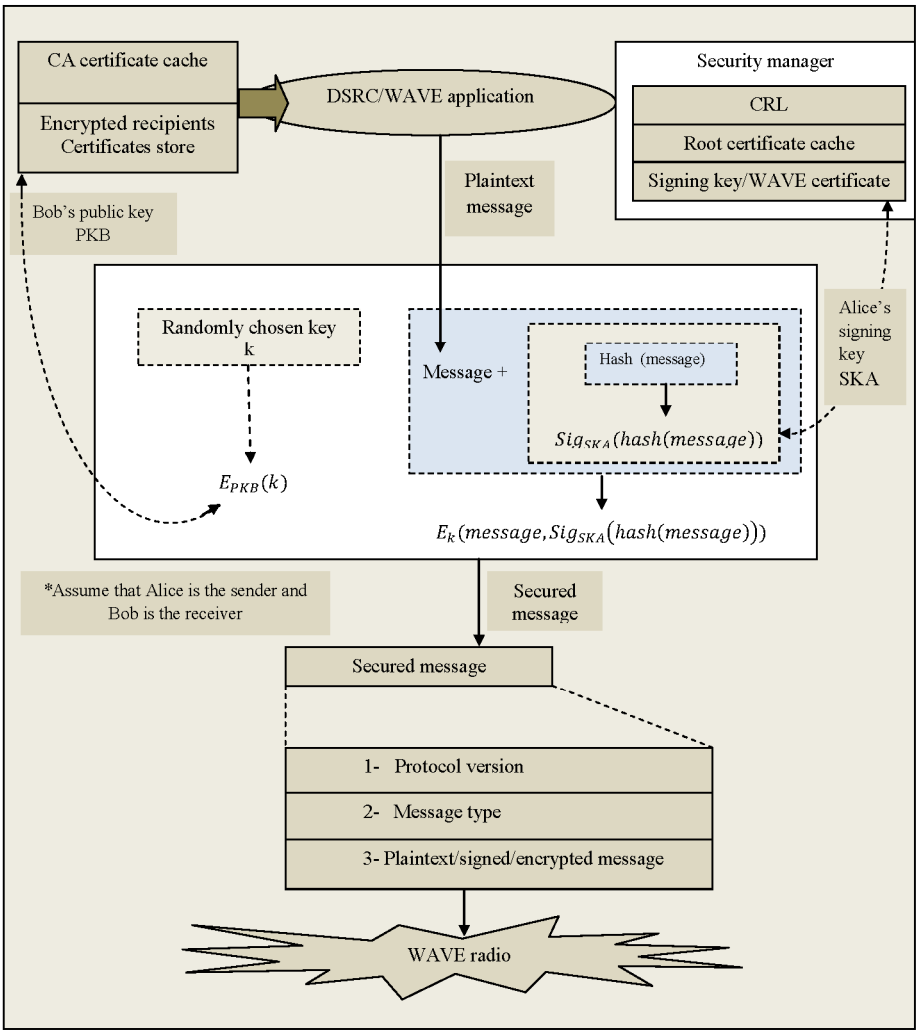


Fig. 4. The IEEE Std 1609.2 security services framework [7]

sybil attacks at low overhead and delay, while preserving privacy of vehicles but it may fail in colluding attacks. Authors in [34] present DoS and Distributed DoS and their severity level in VANET environment. They also introduce a model to secure VANETs from the DoS and DDoS. The solutions are able sorted out DoS but fail to protect privacy, prevent sybil attack, even information cheating.

Misusing VANETs could cause destructive consequences. Authors [38] proposed DRTA (Dynamic Revocation using Threshold Authentication) to punish misbehaving users. This can be employed in both V2V and V2R for anonymous communications.

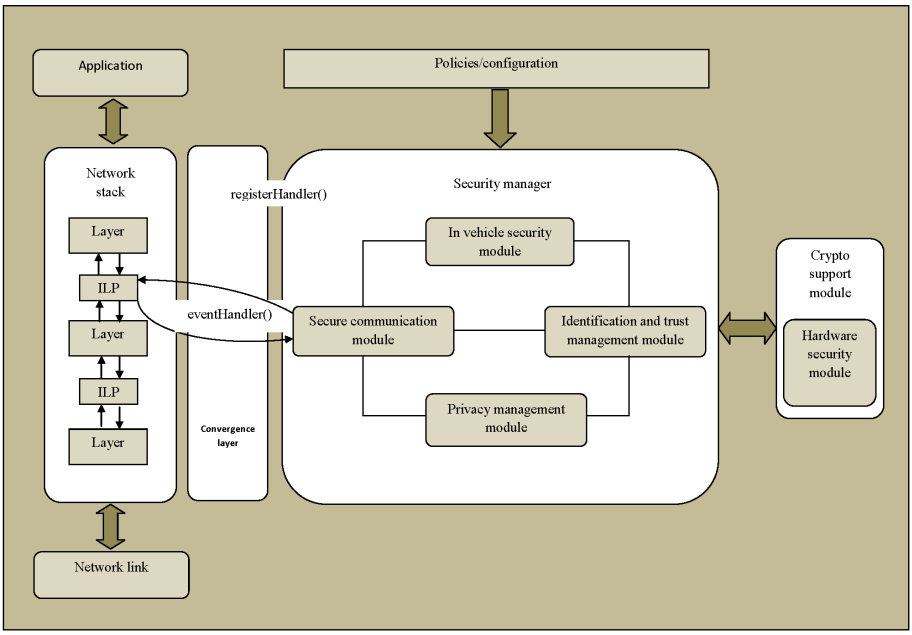


Fig. 5. Baseline architecture: deployment view [8, 32]

It is based on some threshold authentication technique that dynamically revokes a user's credential, while providing the flexibility of whether to reveal the user's identity and tolerating unintentional misbehavior such as hardware malfunctioning. DRTA outperforms its counterparts such as RTPD [12]. Work in [41] proposes protocols, as components of a framework, for the identification and local containment of misbehaving or faulty nodes, and then for their eviction from the system. Results show that the distributed approach to contain nodes and contribute to their eviction is efficiently feasible and achieves a sufficient level of robustness.

5.2.2 Secure Routing

Secure routing is the most important requirement for any secure communication. In VANETs routing can be based on ID of the vehicle or geography of the vehicle. ID methods are for sending data to an individual node, whereas geography methods are for sending data to a group of nodes. ID based routing protocols (e.g. Secure Routing Protocol (SRP) [43], Secure Beaconing [40], etc.) tend to sacrifice privacy frequently but geographic location or position based routing protocols (e.g. PRISM [35], Position-Based Routing [36], etc.) may not. Most secure routing algorithms build on top of insecure routing protocols as no routing protocol was originally built with security in mind.

Table 2, summarizes the secure routing protocols in VANETs. It is clear from the table that most of the secure routing protocols are not privacy compliant. Moreover, privacy compliant secure routing protocols such as PRISM is not secure from sybil attacks.

Table 2. Summary of the secure routing protocols in VANETs

Protocol	Key features	Advantages	Disadvantages
AOD-SEC[42]	-based on ID and a centralized PKI	-based on simple AODV - no impersonation attacks	-based on insecure routing protocol -privacy not protected
SRP[43]	-extension to existing ID-based reactive protocols (AODV, DSR) -assumes secure link between two nodes already exists	-deals with non-colluding malicious nodes. -prevents IP spoofing, ensures privacy.	–route cache poisoning renders efficient algorithms less efficient/ effective. –colluding malicious nodes can "alter" topology
Secure-Beaconing [40]	-ID based, believes most communications are direct. -not all beacons need to be encrypted –tries to strike balance between security and efficiency -omitting Certificates and Certificate Verifications	–saves bandwidth –better data throughput	-no privacy whatsoever. -some messages might be lost. -critical situations mean an exponential load on network
PRISM [35]	-uses AODV to establish path -destination is an area, not a node -uses group signatures on both side -once link is established, create one-time-use secret key between parties -hit and miss approach	-preserves privacy. -avoids creation of pseudonyms(expensive)	-deals with rogue/bad nodes reactively (TTP) -difficult to ensure that DST-AREA value has not been tampered with -sybil attacks are easy
Position-Based Routing [36]	- location table with ID and positions of nodes - location is plausible - end-to-end & hop-by-hop encryption	-two levels of encryption -broadcasts deter wormhole attacks	-caching of location and certificates is a great loss of privacy

5.2.3 Secure MAC

Like secure routing secure MAC protocol is necessary for VANETs. Unfortunately works in this area is very limited [37]. It is important design efficient medium access control (MAC) protocols so that safety related and other application messages can be timely and reliably disseminated through VANETs. In this work authors propose a secure MAC protocol for VANETs, with different message priorities for different types of applications to access DSRC channels. Results show that the proposed MAC protocol can provide secure communications while guarantee the reliability and latency requirements of safety related DSRC applications for VANETs.

6 Analysis of the Existing Mechanisms and Future Directions

It is clear from the discussion of section 4 that, security and privacy may conflict in number of VANET applications. While people or drivers of the vehicles are considering that privacy is their right, on the contrary to have security in certain situations we need to break their privacy. So, a trade-off between privacy and security may be necessary. Moreover, in secure communications precisely in routing it is really hard to find an efficient protocol that can response in real-time as well as maintain the privacy of the drives is very challenging and yet to solve. So scope of further study in this area is highly visible.

Most of the existing security and privacy related works mainly address policies not their implementations. But to make the VANET reality in near future we need to work more on implementation based security solutions which are cost effective and fast responsive. Moreover, certificate-based schemes are still suffering, especially in fixing CAs, real-time certificate verification, certificate revocation, etc. These issues also require further attention from the research community as well Govt. and vehicle manufacturers.

Reactive approach based attack detection techniques has great potential. But these are rarely considered by the VANETs researches. Further research could bring out the potential of these techniques.

For the implementation of comprehensive security and privacy policy, may require the support of all the layers in the protocol stack rather than from single layer support. This protocol stack-wide holistic implementation of security and privacy is missing in the existing works. Further study in this area is a must need. In number of applications, VANETs (e.g. Traffic Signals Violation Warning, Pre-crash Sensing, etc. [3]) exploit V2V and V2R communications. For these application security policy and solution has to take care of both communications which are different in nature. It means any security policy which suits V2V communication might not suit in V2R communication. For example, when a vehicle passes by a RSU; it retrieves fresh environmental data collected by the roadside sensors. After processing, it may interpret the data as a dangerous situation and trigger a safety warning message. In this case if WSNs in RSUs and vehicular communications maintain timeliness (a real-time response requirement for security in VANETs, mentioned section 4) individually (e.g. RSU provides data within 100ms and Vehicle triggers warning within another

100ms, total delay 200ms which is double than the maximum tolerance [3]) than the warning message can be useless and make the situation dangerous. So a combined effort of vehicles and RSUs is needed in guaranteeing overall system-wide security. However, to our best knowledge, there is no published work on the holistic view of security in VANETs. So, further works in this area is an immediate necessity.

Security and efficiency may conflict, especially in WSNs and hard-real time requirements based applications. Even security and QoS in RSUs precisely in WSNs may conflict. So these conflicting issues are needed to be resolved in future.

7 Conclusion

Applications of Vehicular Ad-hoc Networks (VANETs) are very promising and diverse. Majority of the safety-related VANETs applications are real-time and mission critical, which requires strict guarantee of security and reliability. Lack of such security and privacy in VANETs is one of the key difficulties to the wide spread implementations of it. Securing the VANETs along with appropriate protection of the privacy of drivers or vehicle owners is a very challenging task as they conflict with each other in umber of situations. Considering this, in this work we have summarized the attacks, corresponding security requirements and challenges in VANETs. Some of the challenges are not yet tackled at their best level, which require further attention. We have also presented the most popular generic security policies which are based on prevention as well detection methods. Detection-based mechanisms require further attention as they look prospective in VANETs. Many applications in VANETs require stack-wide security support rather than individual layer from the VANETs' protocol stack. In this work we have also discussed the existing works in the perspective of holistic (protocol stack-wide and system-wide) approach of security. These approaches are the concern of our future study.

References

[1] Ezell, S.: Explaining International IT Application Leadership: Intelligent Transportation Systems. The Information Technology & Innovation Foundation (January 2010)

[2] David Wang, C., Thompson, J.P.: Apparatus and method for motion detection and tracking of objects in a region for collision avoidance utilizing a real-time adaptive probabilistic neural network, US. Patent No. 5,613,039 (1997)

[3] US Dept. Transportation, "Vehicle Safety Communications Project Task 3 Final Report" (March 2005), http://www.its.dot.gov/research_docs/pdf/59vehicle-safety.pdf

[4] Raya, M., Hubaux, J.-P.: Securing vehicular ad hoc networks. Journal of Computer Security 15(1), 39–68 (2007)

[5] Raya, M., et al.: Securing vehicular communications. IEEE Wireless Communications 13(5), 8–15 (2008)

[6] Papadimitratos, P., et al.: Secure Vehicular Communications: Design and Architecture. IEEE Commun. Mag. (November 2008)

[7] Lin, X., Lu, R., Zhang, C., Zhu, H., Ho, P.H., Shen, X.: Security in vehicular ad hoc networks. IEEE Communications Magazine 46(4), 88–95 (2008)
[8] Kargl, F., et al.: Secure vehicular communication systems: implementation, performance, and research challenges. IEEE Communications Magazine 46(11), 110–118 (2008)
[9] Zeadally, S., Hunt, R., Chen, Y.S., Irwin, A., Hassan, A.: Vehicular ad hoc networks (VANETs): status, results, and challenges. Telecommunication Systems, 1–25 (2010)
[10] Qian, Y., Moayeri, N.: Design of secure and application-oriented VANETs. In: IEEE VTC 2008, pp. 2794–2799 (Spring 2008)
[11] Boukerche, A., Oliveira, H.A.B.F., Nakamura, E.F., Loureiro, A.A.F.: Vehicular ad hoc networks: A new challenge for localization-based systems. Computer Communications 31(12), 2838–2849 (2008)
[12] Raya, M., Hubaux, J.-P.: Securing Vehicular Ad Hoc Networks. J. Computer Security, Special Issue on Secu- rity, Ad Hoc and Sensor Networks 15(1), 39–68 (2007)
[13] Parno, B., Perrig, A.: Challenges in securing vehicular networks. In: Proceedings of the Workshop on Hot Topics in Networks, HotNets-IV (2005)
[14] Yin, J., ElBatt, T., Yeung, G., Ryu, B., Habermas, S., Krishnan, H., Talty, T.: Performance evaluation of safety applications over DSRC vehicular ad hoc networks. In: Proc. of ACM workshop on Vehicular Ad Hoc Networks, VANET (2004)
[15] Leinmuller, T., Schoch, E., Maihofer, C.: Security requirements and solution concepts in vehicular ad hoc networks. In: IEEE 4th Annual Conference on Wireless on Demand Network Systems and Services, pp. 84–91 (2007)
[16] Hubaux, J.-P., Capkun, S., Luo, J.: The security and privacy of smart vehicles. IEEE Security and Privacy Magazine 2(3), 49–55 (2004)
[17] IEEE P1609.2/D2 – Draft Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages (November 2005)
[18] Jungels, D., Raya, M., Aad, I., Hubaux, J.-P.: Certificate revocation in vehicular ad hoc networks. Technical Report LCA-REPORT-2006-006, EPFL (2006)
[19] Kounga, G., et al.: Proving Reliability of Anonymous Information in VANETs. IEEE Transactions on Vehicular Technology 58(6), 2977–2989 (2009)
[20] Papadimitratos, P., et al.: Architecture for secure and private vehicular communications. In: 7th International Conference on ITS Telecommunications, ITST 2007, pp. 1–6 (2007)
[21] Petit, J.: Analysis of ECDSA Authentication Processing in VANETs. In: 2009 3rd International Conference on New Technologies, Mobility and Security (NTMS), pp. 1–5 (2009)
[22] Plößl, K., Federrath, H.: A privacy aware and efficient security infrastructure for vehicular ad hoc networks. Computer Standards & Interfaces 30(6), 390–397 (2008)
[23] Plößl, K., et al.: Towards a security architecture for vehicular ad hoc networks. In: The First International Conference on Availability, Reliability and Security, ARES 2006, pp. 1–8 (2006)
[24] Rao, A., et al.: Secure V2V Communication With Certificate Revocations. In: 2007 Mobile Networking for Vehicular Environments, pp. 127–132 (2007)
[25] Raya, M., Hubaux, J.-P.: The security of vehicular ad hoc networks. In: Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, Alexandria, VA, USA, pp. 11–21. ACM (2005)
[26] Sunnadkal, R., et al.: A Four-Stage Design Approach Towards Securing a Vehicular Ad Hoc Networks Architecture. In: Fifth IEEE International Symposium on Electronic Design, Test and Application, DELTA 2010, pp. 177–182 (2010)
[27] Trusted Platform Module (TPM), https://www.trustedcomputinggroup.org/groups/tpm/

[28] Golle, P., Greene, D., Staddon, J.: Detecting and Correcting Malicious Data in VANETs. In: Proceedings of the First ACM Workshop on Vehicular Ad Hoc Networks (VANET). ACM Press, Philadelphia (2004)
[29] Leinmüller, T., Held, A., Schäfer, G., Wolisz, A.: Intrusion Detection in VANETs. In: Proceedings of 12th IEEE International Conference on Network Protocols (ICNP 2004) Student Poster Session (October 2004)
[30] U.S. Dept. 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
[31] IEEE Std. 1609.2-2006, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages (2006)
[32] SeVeCom, "Secure Vehicular Communications: Security Architecture and Mechanisms for V2V/V2I, Delivarable 2.1" (2007-2008), http://www.sevecom.org
[33] Zhou, T., Choudhury, R.R., Ning, P., Chakrabarty, K.: P2DAP—Sybil Attacks Detection in Vehicular Ad Hoc Networks. IEEE Journal on Selected Areas in Communications 29(3), 582–594 (2011)
[34] Ahmed Soomro, I., Hasbullah, H., Ab Manan, J.-l.: Denial of Service (DOS) Attack and Its Possible Solution in VANET. In: ICCESSE-WASET 2010 Conference, Tokyo, Japan, May 26-28 (2010)
[35] Karim El Defrawy, M., Tsudik, G.: Privacy-Preserving Location-Based On-Demand Routing in MANETs. IEEE Journal on Selected Areas in Communications 29(10) (December 2011)
[36] Harsch, C., Festag, A., Papadimitratos, P.: Secure Position-Based Routing for VANETs. In: IEEE 66th Vehicular Technology Conference (2007)
[37] Qian, Y., Lu, K., Moayeri, N.: A secure VANET MAC protocol for DSRC applications. In: IEEE GLOBECOM, pp. 1–5 (2008)
[38] Sun, J., Fang, Y.: Defense against misbehavior in anonymous vehicular ad hoc networks. Ad Hoc Networks 7(8), 1515–1525 (2009)
[39] Shen, P.-Y., Liu, V., Tang, M., William, C.: An efficient public key management system: an application in vehicular ad hoc networks. In: Pacific Asia Conference on Information Systems (PACIS), AIS Electronic Library (AISeL), Queensland University of Technology, Brisbane, Qld, p. 175 (2011)
[40] Schoch, E., Kargl, F.: On the Efficiency of Secure Beaconing in VANETs. In: WiSec 2010, March 22-24 (2010)
[41] 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) (October 2007)
[42] Eichler, S., Dotzer, F., Schwingenschlogl, C., Caro, F.J.F., Eberspaher, J.: Secure routing in a vehicular ad hoc network. In: IEEE 60th Vehicular Technology Conference, pp. 3339–3343 (2004)
[43] Papadimitratos, P., Haas, Z.: Secure Routing for Mobile Ad Hoc Networks. In: SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, pp. 27–31 (January 2002)