

# Smart Car Privacy: Survey of Attacks and Privacy Issues

Akshay Madhav Deshmukh  
 Department of Informatik  
 Technische Universität Darmstadt  
 64289, Darmstadt  
 Email: madhavdeshmukh.akshay@stud.tu-darmstadt.de

**Abstract**—Automobiles are becoming increasingly important in our day to day life. Modern automobiles are highly computerized and hence potentially vulnerable to attack. Providing many wireless connectivity for vehicles enables a bridge between vehicles and their external environments. Such a connected vehicle solution is expected to be the next frontier for automotive revolution and the key to the evolution to next generation intelligent transportation systems. Vehicular Ad hoc Networks (VANETs) are emerging mobile ad hoc network technologies incorporating mobile routing protocols for inter-vehicle data communications to support intelligent transportation systems. Thus security and privacy are the major concerns in VANETs due to the mobility of the vehicles. Thus designing security mechanisms to remove adversaries from the network remarkably important in VANETs.

This paper provides an overview of various vehicular network architectures. The evolution of security in modern vehicles. Various security and privacy attacks in VANETs with their defending mechanisms with examples and classify these mechanisms. It also provides an overview of various privacy implication that a vehicular network possess.

**Index Terms**—Vehicular Ad hoc Networks (VANET), Road Side Unit, On-board Unit, Black Hole Attack, Masquerade, Sybil Attack, Wormhole Attack, Illusion Attack, Intelligent Transportation System (ITS), V2X Architecture.

## I. INTRODUCTION

Vehicles have advanced into complex systems incorporating many different Electronic Control Units (ECUs) which are interconnected based on the required functionality of different tasks. ECUs and a set of sensors are used to gather information about the vehicle's behaviour and environment, and to control the functionalities of the vehicle. These ECUs are associated by exchanging messages resulting in an in-vehicle network also known as on-board network. Thus, internal network infrastructure in vehicles has advanced in providing different use cases for different properties through a common bus system.

Vehicles in motion communicate with their neighbouring vehicles (closer vicinity vehicles) and with Road Side Units (RSUs) either directly or indirectly - through intermediate nodes. Each vehicle updates its neighbouring RSUs with its own information (speed, location etc.) and traffic updates on a regular bases. These RSUs and vehicles constitute Vehicular Ad-hoc Networks (VANets) also known as inter-vehicle Network to have the shared knowledge of the on going traffic updates[2]

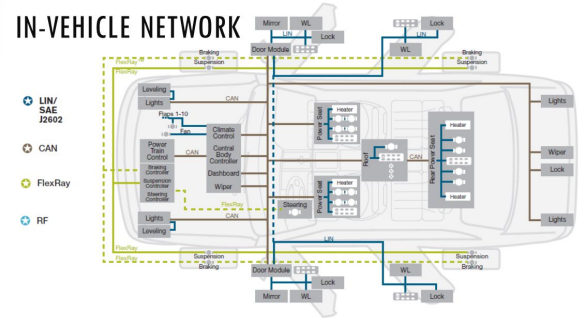


Fig. 1: In-Vehicle Network [1]

Furthermore, today's vehicles provide connectivity bridge to the outside world through wired and wireless interfaces. A Wireless Personal Area Network (WPAN) devices that comprise of wireless technologies which communicate through short range (upto 100m) such as Bluetooth, USB, Near Field Communication (NFC), Cellular networking, onboard diagnostic ports (ODBs) and many more. WPAN gateway provides a medium for communication between personal devices and in-vehicle ECUs. For example the driver can control the lights, windshield wipers, air flow, heat control, automatic ignition of the engine, automatic door lock systems and various other features through a bluetooth connected PDAs[3].

Vehicles that are connected to mobile devices can communicate with Service Centers (SCs) through mobile network (cellular network). Service Centers exchange information with RSUs by providing the required information about their location, behaviour and environment to the vehicle owners. The cellular network provides communications to the devices that have wireless communication capabilities with mobile and landlines[4].

These technologies have their own advantages in providing useful services and functionalities, but the main concern seems to be the degree of vulnerability that a system involves. It provides the room for intruders to carry out a potential attack on the system. In particular, with wireless interfaces to the outside world open up possibilities for remote attacks.

Considering the new attack surfaces, it is very important to reconcile that security mechanisms are a vital aspect to add to the on-Board (in-vehicle networks) infrastructure. There are many state of art research proposals on reinforcing the automotive security based on cryptographic mechanisms that provide manipulation and authentication to solve bus security issues[5] and establishing an authentic confidential communication between the components of the vehicle and authentic controllers (authentic certified users)[6]. Nevertheless, the biggest challenge of automotive security is its long life cycle of vehicles and by their safety requirements which mandates a traditional approach to make changes in the deployed vehicles. Thus, every changes introduced in the safety-critical system should be regression free and flawless.

#### A. Security in modern vehicles

Security in modern vehicles can be classified into on-Board (in-vehicle) security and V2X (Vehicle-to-Everything) communication security. V2X security infrastructure in turn are classified into Vehicle-to-vehicle communication security and Vehicle-to-infrastructure security.

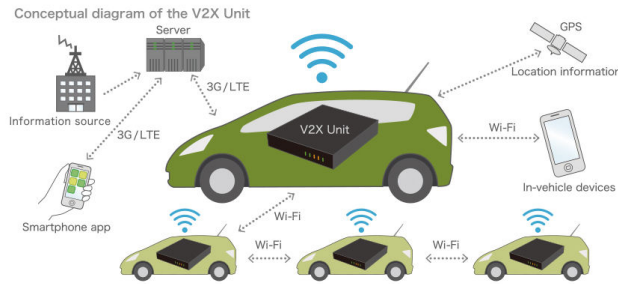


Fig. 2: V2X Architecture - Conceptual Level  
source: <http://world.honda.com/safety/hearts/2016/14/>

All the modern vehicles are embedded with ECUs which are categorised based on their functionalities-Powertrain Control Module (PCM), Transmission Control Module (TCM), Brake Control Module (BCM), Central Control Module (CCM), Central Timing Module (CTM), General Electronic Module (GEM), Body Control Module (BCM), Suspension Control Module (SCM). With respect to the comfort of the owner, a vehicle can comprise of a system for infotainment (e.g. radio and navigation system) and telematics units through a cellular network. Further, V2X capabilities can be broadly enhanced with vehicular adhoc networks (VANETs)[7].

Conversely, the on-board system acts as the attack surface for controlling the core aspects of the vehicle which involves safety-critical functionalities such as brake system and throttle (fueling system) by withdrawing arbitrary data by reading their memory from ECUs and feeding ECUs with malicious code that creates a havoc[8].

As VANETs are young, and still under test beds, there are no real attacks documented as such. The IEEE standard specifies to embed vehicles with certificates with signature messages (Public Key Infrastructure) among the communicating partners to guarantee integrity within the system[9].

On-board vehicular systems should be provided with integrity, authentication, authorization, and availability in order to safeguard against malicious attacks on ECU software and unauthorized spoofing of messages. Thus, research has initiated to secure the Controller Area Network (CAN) itself and provide a secure on-board system architecture[10],[11].

In V2I scenarios, when the vehicle wants to get the access to services like internet service or information about the nearest restaurant which are inturn provided by the RSU's, they send requests to the nearest RSU. The figure 3 provides a flowchart which presents the process of vehicles requiring services from the nearest RSU[12].

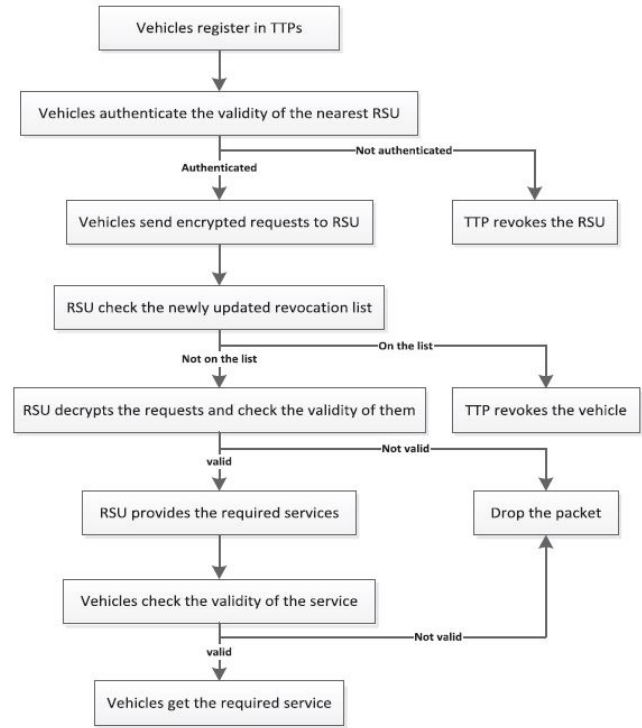


Fig. 3: The process of vehicles requiring services from the nearest RSU[11].

In most cases, in order to broadcast messages, the vehicles should first get authenticated with RSU and seek the permission[13]. When the vehicles passes the RSU which is in its nearest vicinity, it should also authenticate the validity of the RSU in case it is a fake RSU. As soon as the RSU authentication is completed, the vehicle sends the encrypted request messages and its certificate to the RSU. The RSU decrypts the request and then looks up the newly updated revocation list retrieved from TTP to check whether the vehicle is entitled to obtain the service. If the certificate is on the revocation list, the RSU rejects the request, otherwise the vehicle is authenticated. If the vehicle is authenticated, the RSU sends the response back to the vehicle and provide the service request.

## B. Evolution of Security

The evolution of security can be well understood by accessing and classifying the security mechanisms of in-vehicles and V2X systems. The classification is based on risk analysis of security technologies used in vehicles at different layers - software, hardware, cryptography, architecture, network technologies, and protocols. Based on the above mentioned layers, we categorize the security mechanisms into:

1) *Software implementations*: ECUs software implementation may consist of design flaws or bugs through which an intruder can easily evade a security mechanism. For example, classical buffer overflow were used in Heartbleed attack (a security bug) on openSSL, A FREAK (man-in-the-middle) attack in openSSL that allowed to use weak easily crackable RSA keys .

2) *Configuration*: According to OWASP Top 10 list[14], the fifth place being the “Security Misconfiguration” is the most critical web application security flaw. Usually security mechanism are very difficult to configure due to its high complexity. There are high chances of committing mistakes, for example firewall configuration, intrusion detection rules, or access control lists. Some of the common misconfigurations are displaying error handling messages, directory listing in web servers, misconfiguration of firewall rules, or using default passwords.

3) *Protocols*: Secured communication protocols are known as security protocols. They encapsulate the communication between the two agents. Insecure communication protocols are usually vulnerable and are often exposed to various attacks, such as replay, man-in-the-middle attack, and impersonation. In order to overcome these attacks, defining a security protocol has always been a big challenge, which leads to false assumptions resulting in a potential attack. For example, Wired Equivalent Privacy (WEP) protocol, used to protect from eavesdropping and other attacks securing the link-layer communication, has several security flaws in the protocol, deriving from mis-application of cryptographic primitives[15].

4) *System Security*: In ECUs, the system security mechanism deployed is inadequate. If more complicated attacks become available, Address Space Layout Randomization may fail.

5) *Symmetric cryptography*: Attacks against cryptographic ciphers and hash functions may become more powerful or robust, but as far as the security is concerned it might not be as secure as it was couple of years ago. Furthermore, even if the algorithm may be very secure but the cryptographic key length may be the loophole for vulnerability in the coming years[16]. For example, in construction of a quantum computers, most of the implementations use keys of 128-bit, as per the Grover’s algorithm[17] it is required to change the key length to 256-bits which in turn reduces the bits in half.

6) *Asymmetric cryptography*: The main difference between symmetric and Asymmetric cryptography is the mech-

anism and the key lengths (longer). For example, Many servers used a single 512-bit group for Diffie-Hellman key exchange . But later it was improvised by using 2048-bit or longer primes to avoid Logjam Attack on TLS[18].

7) *Hardware security modules*: In most of the above mentioned mechanism replacing a hardware is not easy due to their hardware being immutable and performance and various cost reasons. Even if hardwares with higher flexibility like FPGAs are used there will be a huge difference in their performance of powerful mechanisms.

## II. BACKGROUND

For most of us, we think the beginning of smart cars as a very new concept in the world of automobile. A humble beginning of smart car started in early 1990’s when the Swiss watch company Swatch, the founder Nicolas Hayek came up with the idea of Smart cars and then ended up partnering with Mercedes Benz and the concept of smart car was born. The name “smart” comes from the partnership between Swatch and Mercedes (S & M) and the fact that they wanted to design an “artistic” little car. In 1994, Mercedes-Benz engineers started with a full development concept car and the smart fortwo vehicle was launched in the year 1997 at Frankfurt Motor Show.

### A. Definitions of smart cars

Though there are many different definitions of smart cars available in the literature, yet there is no officially all-accepted definition present till date. As per SAE International Standard J3016[19], which provides the taxonomy and definitions for automated driving in order to facilitate collaboration among technical and policy domains. Figure 4 depicts the levels of automation defined by SAE J3016.

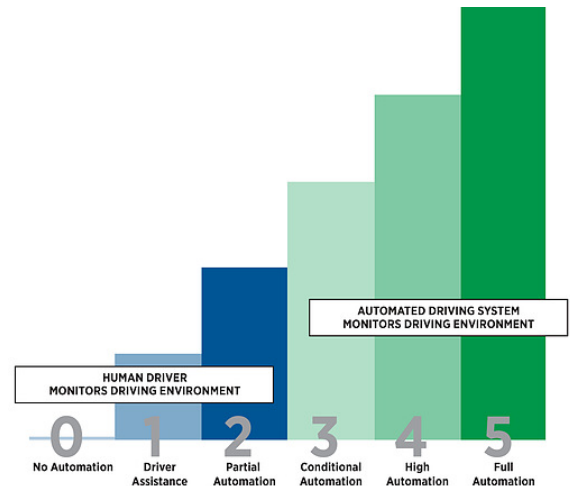


Fig. 4: Automation Levels of Vehicle

source: [www.sae.org/autodrive](http://www.sae.org/autodrive)

Another definition comes from the Declaration of Amsterdam under Cooperation in the field of connected and automated driving[20] which lists out major distinction between connected cars involving communication between

vehicles and also with the infrastructure (CITS) and automated driving involving use of on-board sensor, cameras, navigation system and various associated softwares.

### B. Architecture of a smart car

Defining a generalized architecture for smart cars is not possible. It varies from vehicle to vehicle. The architecture of subnetworks and protocols differ from vehicle to vehicle. Hence figure 5 depicts an abstract high-level architecture of a smart car system[21].

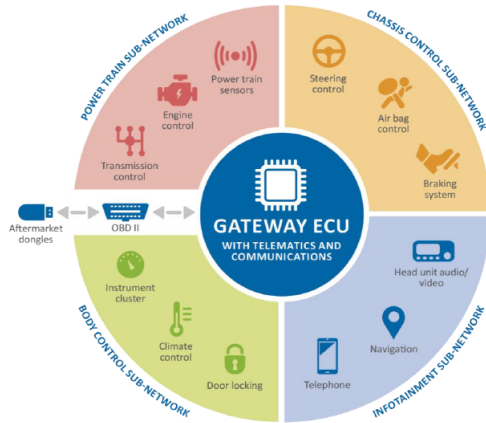


Fig. 5: High-Level architecture of a smart car [19]

Majority of the car architectures contains a central gateway Electronic Control Unit (ECU) which are interconnected with different domains. These domains are distinct independent features of the car. These entities are prone to potential risks considering the amount of diverse domains they are interconnected to. The influence of these risks may differ between safety, security or privacy concerns.

### C. Assets of a smart car

The car architectures differentiate between various domains (components) which are interconnected with a central gateway (as shown in figure 6). These components may cause risks. This is the reason why components of a smart car are described as assets which needs a stronger protection.

Components of a smart car can be categorized into following:

1) **Powertrain Control:** This domain takes care of the link between the car's energy source to the car until motion.

**ECUs and sensors:** The electronic and the mechanical part (powertrain, brake, airbags etc.) of today's modern cars are controlled by Electronic Control Unit (ECU). Different domains have different ECUs. Automotive devices usually depends on the ARM platform for application processors, some of the less likely used architectures are SH, V850 and TriCore[22]. The automotive-grade processors are more preferred than commercial-grade processors due to the constrained operating environment like temperature, humidity, lifespan in automotive environments.

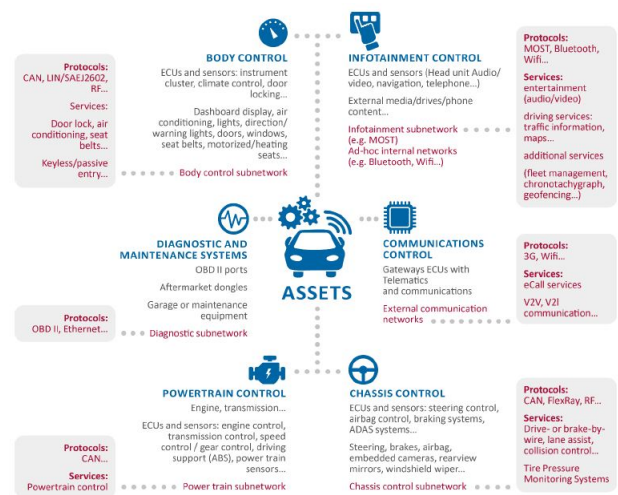


Fig. 6: High-Level architecture of a smart car [19]

In particular for vehicular communications, for increasing the level of security, these system must depend on a Trusted Platform Module (TPM) or Hardware Security Module (HSM). ECU applications may depend on real time operating systems like AUTOSAR, Integrity or VxWorks.

**Subnetwork:** Controller Area Network (CAN) protocol, an ISO standard from 1993 is the widely used and the most popular bus to which most of the ECUs are connected. In a vehicle there may exist many CAN buses to isolate the functions with higher level of criticality like powertrain management from functions with lower level of criticality like multimedia management in a system. The traffic on this bus depends on the solution, at times it can support up to hundreds of messages per second. Hence the CAN bus is the best example and has been analyzed completely by the researchers[23]. The only drawback being some issues with scalability, bandwidth and security.

**Other components:** This domain deals with the body of the car (physical system) such as combustion engine, transmissions, wheels and steering etc.

2) **Chassis Control:** This domain takes care of control frame of the vehicle with respect to its environment.

**ECUs and sensors:** The functionalities of the ECUs are almost the same as that of the powertrain control. They handle the functionalities such as airbag management, steering and brake systems and advanced driver assistance systems.

**Subnetwork:** Subnetwork rely on protocols such as FlexRay or RF usually used for Tire Pressure Monitoring Systems. Also it primarily relies on CAN protocol, but the main drawback is, its on a slower side. Flexray or RF is usually designed for drive-by-wire applications which replaces mechanical functions with softwares.

**Other components:** Other components include embedded cameras, rear view mirrors, windshield wipers and also steering and brake system.

3) **Body Control:** This domain takes care of the body of the vehicle, in the sense it takes care of the passenger's area.



*ECUs and sensors:* The main functionality on ECUs and sensors is the in-car management system like climate control, auto temperature adjustment, door locking system and instrument cluster. They manage all the required comforts of the passenger.

*Subnetwork:* The subnetwork is based on CAN protocol or RF protocols. These RF protocols are used in proprietary protocols like key fobs. They also include other technology like Smart Wave, Bluetooth low energy, Wifi, Zigbee etc.

*Other components:* Other components comprises of dash board display, air conditioning, heating seats, warning lights, seat belts, doors, windows, etc.

4) *Infotainment Control:* This domain takes care of entertainment service installed in the car. This might include navigation system, communication systems (bluetooth telephone access), media system etc.

*ECUs and sensors:* The core functions include the main unit for audio video content, communication systems, entertainment services, internet connectivity, providing information regarding the current traffic and navigation system through maps. They also manage technical services like fleet management, monitoring of speed and distance (tachograph), creating a virtual geographic boundary using geofencing (GPS and RFID).

These additional services makes infotainment ECUs to have a specific architectures. For these systems, even the mobile operating systems can also be used in ECUs (Android, Tizen and WebOS). It is possible to sync the user's smartphone into the vehicle system using QNX. For example, it's used in Apple Carplay and Android Auto technologies which allows the user to view the interface of the phone through the infotainment system installed in the car which in turn helps the user to avoid using his phone while driving. There are many open-source projects that are used to create software solutions for automotive applications. For example, Automotive Grade Linux (AGL) and Linux Genivi.

*Subnetwork:* The subnetwork depends on ad-hoc networks using Wi-fi or Bluetooth and they mostly rely on wireless connectivity provided either by an embedded UICC or by a smartphone connected by USB cable or with Bluetooth. Additionally, camera system can be connected through an Ethernet.

*Other components:* Other components that can be considered as an asset as all the external media devices like drives and phones.

5) *Communications Control:* This domain is a set of communication features offered by a Telematics Control Unit (TCU), which acts a gateway. This domain is completely different of that of the previous ones.

*Gateway ECUs:* Gateway collects the data from many ECUs using the buses available in the vehicle system and provides Internet connectivity remotely by using driver's smartphone or through an embedded GSM. Gateways provides all the security protections like authentication and firewall features required for the communication.

Some of the use cases that use TCU connectivity are as follows:

- Remote engine ignition
- Tracking stolen vehicles
- eCall- Emergency Warnings (compulsory in Europe from 2018)
- Remote transmission of vehicle data
- Smart driving Assistant (e.g.improve driving habits and fuel efficiency)
- Eco-driving

*External communication networks:* Different kinds of services are provided by TCU which typically involves Wifi and 3G connectivity (V2X communication). The figure 7 provides an overview of external interfaces that a car consists of. These interfaces are usually for long range communication, as well as wired or wireless interfaces.

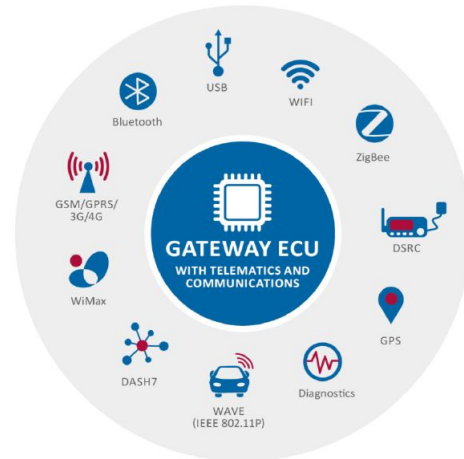


Fig. 7: External interface of a smart car [19]

TCU Provides various wireless protocols in addition to wired protocols such as USB or any diagnostic protocols. Some of the wireless protocols that TCU provides are as follows:

*Long-range wireless protocols:* Telematics depends on wireless connectivity such as 2G, 3G and 4G which are catered by the driver's mobile phone. Some of the mobile protocols such as GSM, GPRS, 3G, 4G, UMTS and LTE are used in different scenarios. GNSS is used as the localization feature in smart cars.

*Intra-vehicle wireless protocol:* The widely used protocols for intra-vehicular communication are bluetooth and wifi. In recent times there is a transition from the tradition protocols (bluetooth and wifi) to state-of-art protocols such Zigbee, Passive RFID, UWB or 60 GHz mm Wave[24]. For example, DASH7 used for Tire Pressure Monitoring System (TPMS) can be used for communication with sensors from near-range protocols to long-range protocols. For example, Mirrorlink, CarPlay or Automotive Link uses wifi or bluetooth to communicate with smartphones using dedicated protocols. Wearable and smart home devices also gets benefited from these type of interfaces ( Open Connectivity foundation project)[25].

*Vehicle -to-Infrastructure (Inter-Vehicle) wireless protocols:* For ITS communications, Inter-Vehicle communica-

tions uses Dedicated Short Range Communication (DSRC) that has a bandwidth of 5.9 GHz. Such communication uses protocols such as WAVE (Wireless Access in Vehicular Environment) which is a means of operation used in IEEE 802.11. Possible alternatives that the state-of-art research provides are DSA[24], WiMAX for V2I communication[26] or CEN-DSRC for Electronic Tolling.

6) *Security, Safety and Privacy concern:* Assets are related to safety in several ways:

- Compromising powertrain or chassis ECUs and networks may obviously cause a vehicle to behave in an unexpected way, for example if an attacker illegitimately compromises ignition, steering, brakes, speed and gear control, or driving support (such as ABS)[27]
- Compromising body ECUs and networks systems that may increase harm to the passengers, should they malfunction:
  - airbag or safety belts,
  - door force-lock used for child protection,
  - the windshield wipers,
  - air conditioning,
  - motorized or heating seats,
  - automatic trunk closing
- Infotainment ECUs and networks may also cause safety issues : incorrect navigation data may lead the car to unsafe areas, and a disturbance of the audio in the entertainment system (such as high volume burst) may distract the driver.

#### D. Overview of Intelligent Transportation System

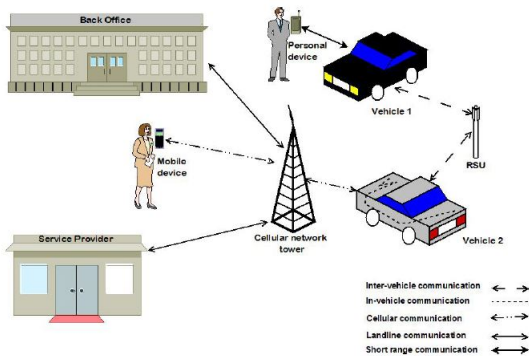


Fig. 8: Example of Intelligent Transportation System [2]

The above mentioned figure comprises of the following entities:

- Connected Cars
- Back office (e.g. Fleet Management System)
- Service Provider (e.g. e-call service)
- Personal Device
- Mobile Device
- Road-Side Units (RSUs)

Each car exchanges the messages in in-vehicle network through ECUs that regulates the functionalities of the vehicle. For example, vehicle dynamics control system (VDCS)

of a vehicle uses the angle of steering wheels and other relevant informations to assist the driver in over-steering, under-steering and roll-over scenarios[28] .

Cars exchange messages between each other through VANets. A standard for inter-vehicle communication-Vehicular Environments (WAVE)[29] uses wireless access to communicate with the nodes of a VANet technology. The exchange of information plays such a vital role in order to avoid collision. With the help of WAVE, vehicles communicate with their neighbouring RSUs in order to provide information about its own activities like current location, speed at which the vehicle is moving and the direction of the vehicle and get the feedback of the ongoing traffic updates based on the location.

Vehicle 1 interacts through WPAN with a personal device and driver can remotely start his vehicle by using his PDA. With the means of cellular network, vehicle 2 interacts with Back Office (Fleet Management System) by sending its data about its location and communicates with Service provider (eCall) in case of some emergency[30].

This paper provides an overview of identifying different types of security and privacy attacks, and classify their defending mechanisms in VANETs. Section III provides an overview of different security attacks in VANETs, their security attributes and types of different malicious vehicles. Further, section IV includes various security attacks and their defensive approaches. Section V provides security implications that a vehicular network possess and Section VI provides a discussion and summerization of the entire paper with respect to security attacks and privacy issues in vehicular network.

### III. SECURITY IN VEHICULAR AD HOC NETWORKS

Vehicular Ad hoc Networks are the latest mobile ad hoc network which consists of mobile routing protocols for communication between vehicle for an intelligent transportation systems. Considering the frequent movements of the vehicle and possessing a hybrid architecture, their security and privacy has been a major concern among researchers. Hence designing a secure platform to authenticate and validate the transmitted messages among the vehicles is very important in VANETs.

In recent times, VANETs has been very popular and widely used in many application in automobile industry such as traffic control and monitoring, toll system, highway internet access, improving safety of the highway system. VANETS are also popularly knows as Wireless Access in Vehicular Environment (WAVE)[31]. WAVE uses Dedicated Short-Range Communication (DSRC) in Intelligent Transportation System (ITS)[32].

The security in VANETs plays a very vital role as it deals with the life critical application and should attain the security requirements such as privacy, Integrity and confidentiality to make the system free from vulnerability and secure against malicious attackers. Security attacks such as Denial of Service (DOS)[33], Wormhole attack[34], Sybil attack[35] and Purposeful attac [36] attacks drivers privacy which leads

to loss of life. The main goal of today's research is to provide a secure communication channel where the identity of the driver is not exposed, if failed, the attacker may consume the data for setting up the attacks with fake identities without even getting caught. But the main challenge of drivers and vehicle is disclosing the identity to RSUs in order to establish the communication. Hence obtaining a secure channel is very important and security and privacy should be handled with at most care.

#### A. Security Attributes

There are many requirements to achieve security in VANETs, which are discussed as follows[37].

1) *Authentication*: It is very important for a vehicle to respond to a message sent an authenticated source. Vehicles should always respond to the messages sent by a genuine member of the network.

2) *Data Verification*: As soon as the authentication is done for the sender vehicle, the receiving vehicle verifies the data to check whether the messages received contains genuine or corrupted data.

3) *Availability*: The performance should not be affected when the network is under an attack. Hence, even if the network is under attack it should be available by using an alternative mechanism.

4) *Data Integrity*: It makes sure that the data is not altered by the attackers. Best example for data integrity is Man in the middle attack, i.e. (In figure 9) If a vehicle B sends a "Road Clear" message to a malicious vehicle C and C changes the message as "Traffic Jam Ahead" and sends the message to vehicle D, thus causing problems to the legitimate vehicle D.

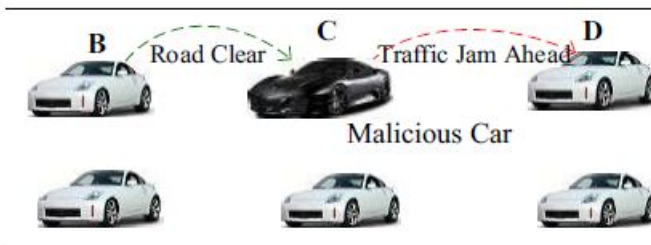


Fig. 9: Data Integrity [39]

5) *Non-repudiation*: Whenever an identity or an investigation of a vehicle is required, sender should not deny the message transmission at any cost.

6) *Privacy*: The driver's personal information should be kept out of reach against unauthorized access.

7) *Real-time constraints*: Should always maintain real-time constraints as vehicles are connected to VANETs for a short duration of time.

#### B. Types of Attacker's Vehicle

In VANETs, malicious vehicles attacks legitimate vehicles in different ways. Capacities on an attacker can be classified as below:

1) *Insiders Vs Outsiders*: Member nodes who communicate with each other inside the network are called as Insider. Insider is an authenticated member of the network, always possess a certified public key and can have different varieties of attacks. Outsiders are the external entity who cannot communicate directly with the members of a network i.e. they are considered as an intruder by the members of the network and have less variety of attacks.

2) *Malicious Vs Rational*: A malicious attackers are less predictive and attacks a network without any personal benefit. In the process it damages various member nodes and the network. On the other hand, rational attackers are highly predictive and always follow a pattern. They always perform attacks for some personal benefits.

3) *Active Vs Passive*: An active attacker can generate new packets to damage the network where as a passive attacker can only listen to the wireless channel but cannot generate the packets. Passive attackers are relatively less harmful than the active attacker.

### IV. SECURITY ATTACKS AND DEFENSIVE MECHANISM

This section provides an overview of various security attacks that takes place on Vehicular Ad hoc Networks (VANETs) and proposes the defensive mechanism to overcome these attacks[38][35][39] [40][41][42]

#### A. Bogus Information

An attacker can inject wrong (bogus) information into the network of their choose. These attacks are generally related to authentication security requirement. For example, an attacker can feed wrong information about the traffic conditions in the network in order to make its movement fast and easier on the road.

A message authentication scheme called as Elliptic Curve Digital Signature Algorithm (ECDSA)[36] keeps the message secure and provides a strong authentication for the destination vehicles by a technique called hashing. This message authentication scheme works by generating public and private keys from the source vehicle. Public key is available in all the vehicles present in the network. With the help of hash algorithm and private key, the source vehicles hashes the message and send the encrypted message to the destination vehicle. The destination vehicle then decrypts the message using the public key. Changes made in messages will also change in the hash messages making this scheme a unique one. Hashing being a strong technique makes this scheme more secure on message authentication.

#### B. Denial of Service (DoS)

Efficiency and performance of a network can deteriorate when the attackers transmit dummy messages to jam the channel. Figure 10 illustrates the operation on DoS where a malicious black car creates a dummy message "Lane close Ahead" to RSU and another vehicle behind it to create a jam in the network. Figure 11 demonstrates a Distributed DoS where the attack takes in a distributed manner. Many malicious cars attacks the legitimate cars in the network. V1

is attacked by many malicious cars from different locations at different time. Hence V1 cannot establish a communication to other vehicles in the network.

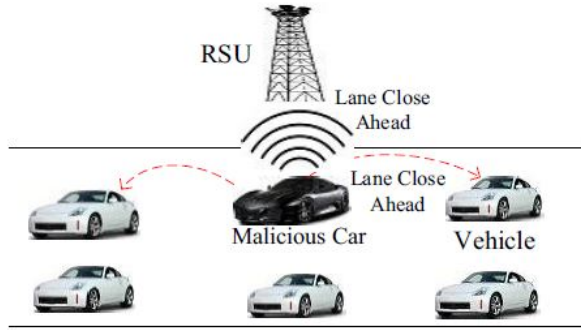


Fig. 10: Denial of Service (Dos) Attack [39]

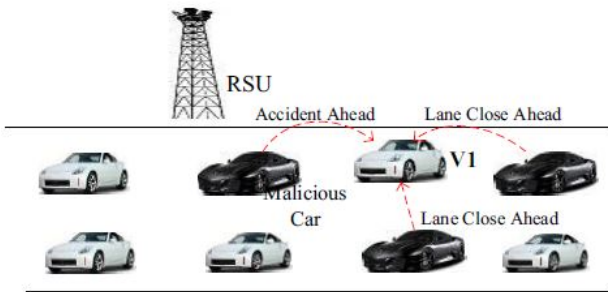


Fig. 11: Distributed Denial of Service (Dos) Attack [39]

### C. Masquerade

With the help of message fabrication, alteration and replay a vehicle fakes its identity to be another vehicle for its personal advantage. For example, a malicious vehicle can fake around as an ambulance vehicle to defraud other vehicle to slow down the ongoing traffic.

### D. Black Hole Attack

Black hole attack is an attack where many malicious cars acts as a barrier between the other (legitimate) cars by changing the path of the messages in a network. A black hole is a part of network where the network traffic is redirected. The black hole area usually does not consist of any nodes, even if it exists they are less likely to be participated in the network resulting in the loss of data packets.

### E. Malware and Spam

Viruses and spams can cause a huge negative impact on a VANETs operations. These attacks are usually initiated by insiders rather than outsiders whenever there is an update performed by on board units (OBU) and road side units (RSUs). These attacks causes an increase in the latency of a transmission which can be made less severe by using a centralized administration.

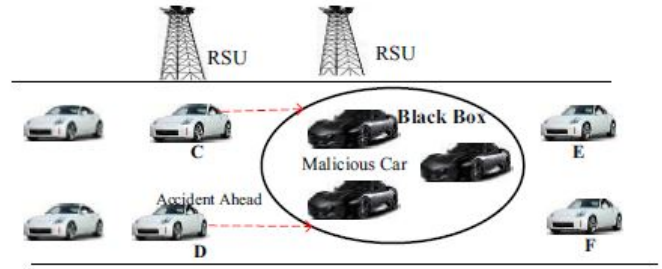


Fig. 12: Black hole Attack [39]

### F. Timing Attack

Data Integrity and security is achieved by transmitting the data from one vehicle to the other at the right time. In this attack when a malicious car receives any emergency message they do not forward it to the neighbouring vehicle at the right time, instead they add some timeslots to the message to create some delay in transmitting it. Hence neighbouring vehicles receive message when it's too late to act upon that emergency situations.

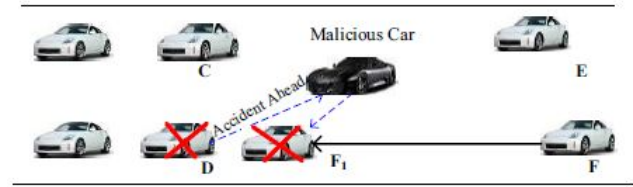


Fig. 13: Timing Attack [39]

The above figure depicts that when the car D sends "Accident Ahead" message to the malicious black car, it does not forward the message to its neighbouring vehicle at the right position F but transmits by adding some timeslots so that when the vehicle receives its message its position would be at F1 where the emergency situation has already taken place.

### G. Global Positioning System (GPS) Spoofing

A location table that contains a log of geographic locations and vehicles identity in the network is maintained by a GPS satellite. An intruder can inject false reading in GPS positioning system to mislead vehicles to think that they are in a different location. These attackers uses GPS satellite simulators as a medium to produce stronger signals than those of the actual ones.

### H. Man in the Middle Attack (MiMA)

A malicious vehicle listens to the other communication in the network and inject false information between the vehicles. Figure 14 illustrates MiMA attack where the malicious black car interferes in between B and D and also, sends the false information to the car E, (original message) that was received from the car A.



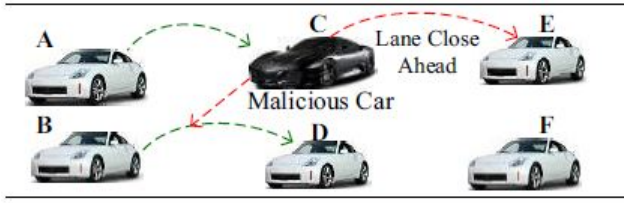


Fig. 14: Man-in-the-Middle Attack [39]

### I. Sybil Attack

In this attack each node send messages with several identities. The attacker creates several identities to simulate several nodes. Hence other vehicles in the network assumes that there are several vehicles in the network at the same time [43][44]. This problems leads to a catastrophe where a vehicle can claim to be at many positions at the same time creating a huge security risk in the network.

In Sybil attacks, to resist these threats many systems uses the concept of redundancy by limiting the physical entities to some resource[38][41]. Sybil attacks can be detected through resource testing. The research contribution done in[38] to test the computational resources of each node is done through computational PUZZLES. But, this approach is not feasible for VANETs[41] because an attacker node can consist of more computational resources compared to an ordinary node. This problem can be avoided by radio resource testing[41].

Another mitigation strategy is using public key cryptography where in each vehicle is authenticated using public keys[45]. Predefined propagation model is another approach used in detecting Sybil attacks in wireless networks[46]. In this model the differences of signal strength between sent and the received signals is matched with the claimed position through Received Signal Strength Indicators (RSSI) approach.

RobSAD is another approach that detects the Sybil attack based on the normal and abnormal motion trajectories of vehicles[47]. This approach detects the attack during the initial deployment phase of VANETs. With the help of RSUs each node can detect attacks on their own. These RSUs can provide vehicles digital signatures with time-stamp regularly on a consistent basis. Each node in the network can keep a log of these digital signatures and compare the differences from their neighbouring nodes signature vectors to detect Sybil nodes. Thus each node can detect attacks own their own by comparing the digital signatures without collaborating with their neighbour nodes resulting in low system requirements and high detection rate.

Another approach is called the Timestamp series approach and its best to use for an initial development stage of VANETs with an RSU infrastructure. Figure 15 demonstrates the working of timestamp series approach. The RSU provides digital certificates to all the vehicles that comes across it and believes that no two vehicles can pass more than one RSUs at a time. Thus, it is easy to detect if a

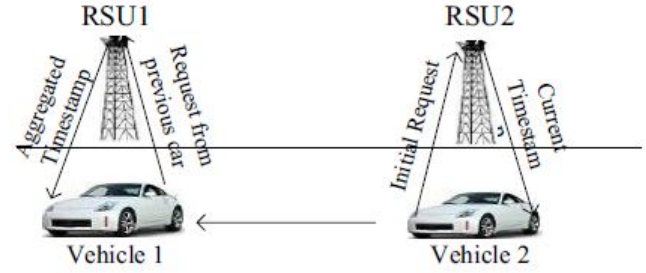


Fig. 15: Timestamp series approach [39]

vehicle receives more than one message with the similar timestamp certificates.

### J. Wormhole Attack

Wormhole is a grievous attack in VANETS and other ad hoc networks. A tunnel is created from two or more malicious nodes that acts as a channel to transmit the data packets from one end of the network to the malicious node at the other end. These data packets are broadcasted to the entire network. These short network connections or the links intimidate the security of transmitting data packets and delete them.

In VANETs and in on-demand routing protocols (such as AODV or DSR), wormhole attack interrupts the multicast and broadcast messages. In AODV protocol the main loop hole for the attack is not using any authentication and protection mechanisms for routing packets. Denial of Service (DoS) attacks are performed by unauthorized access gained by wormholes or malicious node.

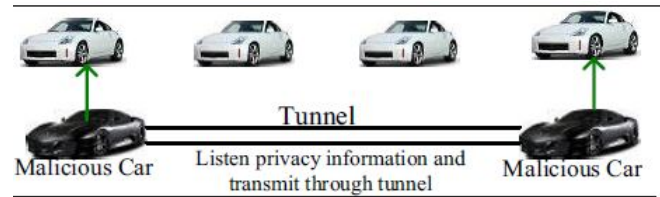


Fig. 16: Wormhole Attack [39]

Figure 16 depicts a wormhole attack where the confidential information is transmitted from one end of the network to the other end by the malicious black car.

The TIK protocol is a packet leases based protocol for detecting and defending against wormhole protocol. Packet lease is an approach to overcome wormhole attacks[48]. All the nodes are synchronized and with clocks in the network and all the nodes are aware of the clock differences between any two nodes.

Asymmetric cryptography is used by TIK protocols to cater immediate authentication of the received packets where it uses  $k$  public keys for  $k$  nodes and hash functions for keeping up-to-date keys data and packets that were received. The difference between the packets travel distance and allowed distance to travel allows to detect the presence of an attacker.

An improvement of packet leases method called HEAP was introduced[34] and it is an efficient approach used to detect the wormhole attacks in AODV routing protocol of VANETs. HEAP provides more security and low overhead. To detect malicious node, HEAP uses geographical lashes rather than local lashes. The main difference in geographical lashes is the limitational of packets travel distance. Hence to overcome this problem, whenever their travel distance is more than the value claimed, the packets are automatically dropped.

#### K. Illusion Attack

As the name suggests an opponent produces an illusion to other vehicles in the neighbour vicinity by broadcasting the traffic warning messages on current road conditions. Illusion Attack is the youngest security threat and not many efficient solutions have been put forward for this attack. Due to the created illusions, the drivers' behaviour is altered and force them to react to those responses. This may lead to traffic jams, car accidents and also decrease the performance of VANETs. Current authentication methods are not effective against Illusion attack because the intruder manipulates the behavior of the sensors to produce false information.

One solution against illusion attack is the Plausibility Validation Network (PVN)[40], which is a new security model for the security of VANETs against illusion attacks. Raw sensors' data are collected by PVN and verifies whether the data collected are plausible or not. Inputs like incoming data from antennas and sensor datas are classified by an input data header. Validity of the input data is monitored by a rule database and data checking module and takes actions if necessary. If the data passes the validity test, the data is assumed to be a clean one, if not it is considered as invalid.

#### L. Intentional Attack

Prevention of Intentional Attack is very difficult as they are authenticated entities that perform peer communications with neighbours. They are trusted entities in the network that communicates with its neighbour in the network.

It is very important to protect against the misbehaviour of intentional attackers or unintentional malfunctioning hardware systems. There are high chances of misbehaving nodes discarding the messages that is received from other nodes, misinterpreting the messages and improper use of bandwidth or injection of bogus messages. A technique is proposed where anonymous communication to protect against misbehavior and promises to keep the privacy of vehicles. This technique is used in vehicle-to-vehicle communication and vehicle-to-infrastructure communication systems[49]. A threshold authentication technique is used to authenticate the misbehaviour of malicious nodes by providing a threshold value. Any authentication above the threshold value guarantees in identification of misbehavior node's details.

#### M. Impersonation Attack

In a network a malicious vehicle delivers the message on behalf of other vehicle to create catastrophe in the network

that leads to traffic jams and accidents. The malicious vehicle after sending the message it gets camouflaged and hides itself from the other vehicles in the network. But, usually in vehicle-to-vehicle communications, one vehicle sends the security message to all the other vehicles that may have an impact on the other vehicles and traffic control system. Hence to reduce the communication overhead, all the messages should be signed and authenticated.

A research contribution has been published in detection of impersonation attack, called as SPECS[50]. It is a scheme used widely in V2V communication systems which provides secure and privacy enhancing communication schemes for VANETs. This scheme is built on the basis of IBV protocol[51] which cannot fulfill privacy requirements due to its suffering from impersonation attack. The security works as follows:

Pseudo-identity and shared secret key  $m_i$  among the vehicles and RSU is used to safeguard the identity of the vehicles. The scheme uses PKI with its real identity RIDi and password PWDi with nearby RSU to authenticate the vehicle. A shared secret key  $m_i$  for vehicle and RSU is generated to authenticate the vehicle. This key is generated by RA. TA forwards  $m_i$  with a hash function and an encrypted block that has  $m_i$  and system secret key,  $s$ . Only the authorized user can decrypt the encrypted block.

This block is transmitted to the vehicles by RSU. A new shared key is generated whenever a vehicle passes through a new RSU. A shared key and one way hash function with the signing key is used to generate the signature. RSU and TA attackers cannot generate valid signing key to sign the message as  $m_i$  are known only to a vehicle. Using a batch verification process performed by RSU, it is easy to detect the invalid signatures and attackers. The whole batch is dropped in IBV if any invalid signature is identified by using batch verification process. Whereas in SPEC the whole batch is not dropped, instead it uses binary search where in it divides the batch in two halves and checks the invalidity on each half. When an intruder is found, it informs the other vehicles and continues this process until all signatures are validates. RSU sends the message to all the vehicles excluding the hash value which is inturn stored into positive and negative bloom filters. Received message's identity is known by creating the hash value and comparing it with the bloom filters has value. If the hash value of a message is found in positive bloom filters, then the message is considered to be valid. Else, the message is discarded and labeled as invalid message.

#### N. Eavesdropping

This attack happens when an attacker is located in a vehicle, be it stopped or moving, or in a false RSU. The collection of vehicle-specific information from overheard vehicular communications is easy in a wireless network. The attackers obtain the target vehicles' confidential data, including the drivers real identities, their preferences or even their credit card codes, which seriously violates the privacy of the drivers.

### O. Message suspension

This attack happens when adversaries hold onto messages before sending them. An attacker selectively drops packets of messages from the network, which may hold critical information for the intended receiver, and the attacker suppresses these packets and can use them again in the future. One goal of such an attack would be to prevent registration and insurance authorities from learning about collisions involving the attacker's vehicle and/or to avoid delivering collision reports to roadside access points.

TABLE I: Summary of attacks with their types and their security requirements

Name of Attack	Type of Attack	Security Requirement
Bogus Information	Insider	Data Integrity, Authentication
Denial of Service (DoS)	Malicious, insider, network attack	Availability
Masquerading	Active, insider	Authentication
Black hole	Passive, outsider	Availability
Malware	Malicious, insider	Availability
Spamming	Malicious, insider	Availability
Timing attack	Malicious, insider	Data integrity
GPS Spoofing	Outsider	Authentication
Man-in-the-Middle	Insider, monitoring attack	Data Integrity, Confidentiality
Sybil	Insider, network attack	Authentication
Wormhole/Tunneling	Outsider, malicious, monitoring attack	Authentication, Confidentiality
Illusion Attack	Insider, malicious	Authentication
Purposeful attack	Active, insiders, malfunctioning hardware	Authentication
Impersonation	Insider, network attack	Authentication

## V. PRIVACY IMPLICATIONS

In both wired and wireless networks, privacy has always been a key concern, and many researchers have dedicated their work on tackling this problem. Even so, while the level of privacy could be enhanced, the most ideal situation where the users' information could never be traced, may never come to fruition. Given the large scale and frequent usage of the internet and cellular networks, small little flaws in the aspect of privacy seem to be acceptable. Still, privacy is a decisive factor in the public's acceptance of and the commercial deployment of vanets[52]. Leaking drivers' private profiles could lead to serious consequences. For example, location tracking of any vehicle provides access to past and current locations of the vehicle[53]. Once the location history has been accumulated, adversaries could infer the driver's personal interests and daily routine by combining

these data with additional information. The information could then be misused for crimes, such as abductions or automobile thefts.

Security has been one of the most challenging problems in VANETs and should be considered along with privacy. To secure the communication in VANETs, the data must be authenticated. Through authentication, the network can be aware of the precise location of a specific user at a specific time, which ensures that the TTP could intervene in the vehicle when an issue arises. For example, when a vehicle has an accident on the road and leaves the scene, the TTP could reveal the real identity of the vehicle and track it until the police were able to catch up with the responsible vehicle. However, some drivers are not willing to let the TTP have access to their confidential information. Therefore, how to preserve privacy while still enabling authentication has become one of the main challenges of implementing VANET[54].

The automobile has gradually evolved from an analog machine with mechanical components to an electronic system with a growing number of computer-based systems. Within this revolution of "smart car", GPS vehicle navigation has been the main focus and attention. There are efforts underway to use GPS vehicle navigation infrastructure for additional value-added services like mobility pricing of insurance[55], infrastructure-less electronic toll collection, and GPS enabled parking fee collection[56].

These applications would require disclosure of positional data by its users in real time. Systems would process the positional data to charge the motorist for the services rendered. A decrease in the cost of electronic storage means that this captured data intended for a specific purpose, transaction processing, may be retained indefinitely or at least for long periods of time. Since GPS data is information rich, the temptation to use it for secondary purposes may be too great to resist.

While theoretical research has tried to raise awareness about these threats and has proposed algorithms to protect the privacy of individuals[57], limited research has been conducted to assess these threats in a real-life scenario.

## VI. CONCLUSION

This paper provides an overview of various vehicular network architectures. The evolution of security in modern vehicles. Various security and privacy attacks in VANETs with their defending mechanisms with examples and classify these mechanisms. It also provides an overview of various privacy implication that a vehicular network possess. Finally, this paper concludes with discussions and summarization of all the security attacks and the privacy issues that a vehicular network consists.

## REFERENCES

- [1] E. W. O. Staff, "Communications protocols proliferate in the drive toward autonomous vehicles," 2021. Accessed: 2021-08-05.
- [2] R. R. Brooks, S. Sander, J. Deng, and J. Taiber, "Automobile security concerns," *IEEE Vehicular Technology Magazine*, vol. 4, pp. 52–64, June 2009.

- [3] S. M. Mahmud and S. Shanker, "In-vehicle secure wireless personal area network (swpan)," *IEEE Transactions on Vehicular Technology*, vol. 55, pp. 1051–1061, May 2006.
- [4] J. Zhang and I. Stojmenovic, "Handbook on security," 2005.
- [5] M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," in *Workshop on Embedded Security in Cars*, 2004.
- [6] A. Groll and C. Ruland, "Secure and authentic communication on existing in-vehicle networks," in *2009 IEEE Intelligent Vehicles Symposium*, pp. 1093–1097, June 2009.
- [7] L. B. Othmane, H. Weffers, M. M. Mohamad, and M. Wolf, "A survey of security and privacy in connected vehicles," in *Wireless Sensor and Mobile Ad-Hoc Networks*, pp. 217–247, Springer, 2015.
- [8] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, 2015.
- [9] "Ieee standard for wireless access in vehicular environments security services for applications and management messages," *IEEE Std 1609.2-2013 (Revision of IEEE Std 1609.2-2006)*, pp. 1–289, April 2013.
- [10] P. Kleberger, N. Nowdehi, and T. Olovsson, "Towards designing secure in-vehicle network architectures using community detection algorithms," in *Vehicular Networking Conference (VNC), 2014 IEEE*, pp. 69–76, IEEE, 2014.
- [11] M. Wolf, A. Weimerskirch, and T. Wollinger, "State of the art: Embedding security in vehicles," *EURASIP Journal on Embedded Systems*, vol. 2007, p. 074706, Jun 2007.
- [12] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.
- [13] D. Huang, S. Misra, M. Verma, and G. Xue, "Pacp: An efficient pseudonymous authentication-based conditional privacy protocol for vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, pp. 736–746, Sept 2011.
- [14] "Owasp top ten project." [https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project#OWASP\\_Top\\_10\\_for\\_2013](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#OWASP_Top_10_for_2013), June 2013. Accessed July 12, 2017.
- [15] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: The insecurity of 802.11," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, MobiCom '01, (New York, NY, USA), pp. 180–189, ACM, 2001.
- [16] M. Stevens, P. Karpman, and T. Peyrin, *Freestart Collision for Full SHA-1*, pp. 459–483. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016.
- [17] L. K. Grover, "A framework for fast quantum mechanical algorithms," in *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC '98, (New York, NY, USA), pp. 53–62, ACM, 1998.
- [18] D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. A. Halderman, N. Heninger, D. Springall, E. Thomé, L. Valenta, B. VanderSloot, E. Wustrow, S. Zanella-Béguelin, and P. Zimmermann, "Imperfect forward secrecy: How diffie-hellman fails in practice," in *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, (New York, NY, USA), pp. 5–17, ACM, 2015.
- [19] O. road Automated Vehicle Standards Committee *et al.*, "Sae j3016: Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems," *SAE International*.
- [20] "Declaration of amsterdam." <https://www.regjeringen.no/contentassets/ba7ab6e2a0e14e39baa77f5b76f59d14/2016-04-08-declaration-of-amsterdam---final1400661.pdf>. Accessed July 12, 2017.
- [21] ENISA, "Cyber security and resilience of smart cars." <https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars>, January 2017. Accessed August 01, 2017.
- [22] C. Hammerschmidt, "Arm architecture leads in the automotive market, semicast finds." <http://www.eenewsautomotive.com/news/arm-architecture-leads-automotive-market-semicast-finds>, 2011. Accessed July 12, 2017.
- [23] C. Miller and C. Valasek, "Adventures in automotive networks and control units," *DEF CON*, vol. 21, pp. 260–264, 2013.
- [24] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," *IEEE Internet of Things Journal*, vol. 1, pp. 289–299, Aug 2014.
- [25] T. Cheng, "Project launched to advance interoperability between automotive and other iot ver-
- ticals." <https://openconnectivity.org/announcements/open-connectivity-foundation-announces-automotive-project>, August 2016. Accessed July 10, 2017.
- [26] I. C. Msadaa, P. Cataldi, and F. Filali, "A comparative study between 802.11p and mobile wimax-based v2i communication networks," in *2010 Fourth International Conference on Next Generation Mobile Applications, Services and Technologies*, pp. 186–191, July 2010.
- [27] "Tesla's autopilot has had its first deadly crash." <https://www.wired.com/2016/06/teslas-autopilot-first-deadly-crash/>. Accessed June 9, 2017.
- [28] R. Alur, K.-E. Arzen, J. Baillicul, and T. Henzinger, *Handbook of networked and embedded control systems*. Springer Science & Business Media, 2007.
- [29] R. A. Uzcategui, A. J. D. Sucre, and G. Acosta-Marum, "Wave: A tutorial," *IEEE Communications Magazine*, vol. 47, pp. 126–133, May 2009.
- [30] "ecall: Time saved = lives saved." <https://ec.europa.eu/digital-single-market/ecall-time-saved-lives-saved>, June 2014. Accessed July 5, 2017.
- [31] D. Jiang and L. Delgrossi, "Ieee 802.11p: Towards an international standard for wireless access in vehicular environments," in *VTC Spring 2008 - IEEE Vehicular Technology Conference*, pp. 2036–2040, May 2008.
- [32] S. Biswas, R. Tatchikou, and F. Dion, "Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety," *IEEE Communications Magazine*, vol. 44, pp. 74–82, Jan 2006.
- [33] X. Liu, Z. Fang, and L. Shi, "Securing vehicular ad hoc networks," in *2007 2nd International Conference on Pervasive Computing and Applications*, pp. 424–429, July 2007.
- [34] S. M. Safi, A. Movaghar, and M. Mohammadzadeh, "A novel approach for avoiding wormhole attacks in vanet," in *2009 Second International Workshop on Computer Science and Engineering*, vol. 2, pp. 160–165, Oct 2009.
- [35] G. Guette and B. Ducourthial, "On the sybil attack detection in vanet," in *2007 IEEE International Conference on Mobile Adhoc and Sensor Systems*, pp. 1–6, Oct 2007.
- [36] S. S. Manvi, M. S. Kakkasageri, and D. G. Adiga, "Message authentication in vehicular ad hoc networks: Ecdsa based approach," in *2009 International Conference on Future Computer and Communication*, pp. 16–20, April 2009.
- [37] 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, (New York, NY, USA), pp. 11–21, ACM, 2005.
- [38] J. R. Douceur, "The sybil attack," in *Revised Papers from the First International Workshop on Peer-to-Peer Systems*, IPTS '01, (London, UK, UK), pp. 251–260, Springer-Verlag, 2002.
- [39] M. Raya and J. Pierre, "Hubaux. the security of vehicular ad hoc networks," in *Proc. SASN*, 2005.
- [40] N. W. Lo and H. C. Tsai, "Illusion attack on vanet applications - a message plausibility problem," in *2007 IEEE Globecom Workshops*, pp. 1–8, Nov 2007.
- [41] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis & defenses," in *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks*, IPSN '04, (New York, NY, USA), pp. 259–268, ACM, 2004.
- [42] I. A. Sumra, I. Ahmad, H. Hasbullah, and J. I. bin Ab Manan, "Behavior of attacker and some new possible attacks in vehicular ad hoc network (vanet)," in *2011 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pp. 1–8, Oct 2011.
- [43] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '01, (London, UK, UK), pp. 213–229, Springer-Verlag, 2001.
- [44] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against sybil attack in vehicular ad hoc network based on roadside unit support," in *MILCOM 2009 - 2009 IEEE Military Communications Conference*, pp. 1–7, Oct 2009.
- [45] M. Raya, P. Papadimitratos, and J. p. Hubaux, "Securing vehicular communications," *IEEE Wireless Communications*, vol. 13, pp. 8–15, October 2006.
- [46] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in vanets," in *Proceedings of the 2006 Workshop on Dependability*



*Issues in Wireless Ad Hoc Networks and Sensor Networks*, DIWANS '06, (New York, NY, USA), pp. 1–8, ACM, 2006.

- [47] C. Chen, X. Wang, W. Han, and B. Zang, “A robust detection of the sybil attack in urban vanets,” in *2009 29th IEEE International Conference on Distributed Computing Systems Workshops*, pp. 270–276, June 2009.
- [48] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Packet leases: a defense against wormhole attacks in wireless networks,” in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 3, pp. 1976–1986, IEEE, 2003.
- [49] J. Sun and Y. Fang, “Defense against misbehavior in anonymous vehicular ad hoc networks,” *Ad Hoc Networks*, vol. 7, no. 8, pp. 1515 – 1525, 2009. Privacy and Security in Wireless Sensor and Ad Hoc Networks.
- [50] T. Chim, S. Yiu, L. C. Hui, and V. O. Li, “Specs: Secure and privacy enhancing communications schemes for vanets,” *Ad Hoc Networks*, vol. 9, no. 2, pp. 189 – 203, 2011. Advances in Ad Hoc Networks (I).
- [51] C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, “An efficient identity-based batch verification scheme for vehicular sensor networks,” in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, April 2008.
- [52] S. Goudarzi, A. H. Abdullah, S. Mandala, S. A. Soleymani, M. A. R. Bae, M. H. Anisi, and M. S. Aliyu, “A systematic review of security in vehicular ad hoc network,” in *Proc. 2nd Symp. WSCN*, pp. 1–10, 2013.
- [53] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, “Amoeba: Robust location privacy scheme for vanet,” *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, 2007.
- [54] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, “Enforcing privacy using symmetric random key-set in vehicular networks,” in *Autonomous Decentralized Systems, 2007. ISADS'07. Eighth International Symposium on*, pp. 344–351, IEEE, 2007.
- [55] E. Nelson, “Norwich union pay as you drive car insurance.” <https://www.aviva.co.uk/media-centre/story/2840/norwich-union-launches-innovative-pay-as-you-drive/>, October 2006. Accessed October 01, 2017.
- [56] B. Grush, “Optimizing gnss-based mobility pricing for road-use, parking, and payd insurance,” *4th European Traffic Congress, (Salzburg, Austria)*, 2005.
- [57] M. Duckham and L. Kulik, *A Formal Model of Obfuscation and Negotiation for Location Privacy*, pp. 152–170. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005.