CHALMERS

Vehicular Networks – Security, Vulnerabilities and Countermeasures

Master of Science Thesis in the program Networks and Distributed Systems

KASRA AMIRTAHMASEBI
SEYED REZA JALALINIA

Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
Göteborg, Sweden, June 2010

Vehicular Networks Vulnerabilities and Countermeasures

KASRA AMIRTAHMASEBI,
SEYED REZA JALALINIA

Examiner: TOMAS OLOVSSON

Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
SE-412 96 Göteborg
Sweden
Telephone + 46 (0)31-772 1000

Department of Computer Science and Engineering
Göteborg, Sweden June 2010

Abstract

Vehicular networks are becoming more popular every day. There are several applications of vehicular networks which are discussed by manufacturers and also academics which will be both time and money saving. Due to the growing interest in distribution of traffic and road information among drivers and connecting vehicles to other networks such as the Internet, vehicular ad hoc networks (VANET) are the topic of interest among many manufacturers and academics. There have been numerous solutions and methods in order to improve the efficiency, privacy and security of such networks. On the other hand, in-vehicle networks are formed recently to add more functionality and options to vehicles. Furthermore, subjects such as remote firmware updates of in-vehicle networks have drawn a lot of attention as well. Security, however, has always been an issue in vehicular networks which must be seriously considered and a security infrastructure has to be designed and implemented in such networks.

In this work, we have done a survey of existing approaches to solve the problems associated with vehicular networks. We discuss security vulnerabilities in vehicular networks and their countermeasures, both in inter-vehicle (VANET) and in-vehicle networks, in order to secure the vehicular networks. In our work, we found that vehicular networks in general have several vulnerabilities and are exposed to different cyber attacks. There are a number of suggested countermeasures which will provide short-term security for vehicular networks. Cyber attacks in in-vehicle networks can be a threat to the vehicle and its passengers; therefore, security issues must be carefully addressed in in-vehicle networks. We believe that there will be a need for a new infrastructure to deal with current vulnerabilities in in-vehicle networks. By doing so, current and future advancements in vehicular networks can be applied with less security issues and risks which will culminate in secure and reliable vehicular networks.

Table of Contents

Table of Figures

1 Introduction

There have been numerous solutions and methods in order to improve the efficiency of vehicular networks. Vehicular networks are mainly divided into two main categories which must be studied and analyzed separately:

- Inter-vehicle networks which are called VANETs and are mainly for distribution of traffic and road conditions among vehicles in range. There are also additional Road-Side Units (RSU) which vehicles can get information from.
- In-vehicle networks which are a combination of Electronic Control Units (ECU), sensors and actuators. These networks are mainly used for communicating sensor information and ECU messages along the whole vehicle. Depending on functionality and speed, different communication buses are used for transferring ECU messages.

Security, however, has always been an issue in vehicular networks which must be seriously considered and a security infrastructure has to be designed and implemented in such networks. From inter-vehicle point of view, an attacker can inject false and invalid traffic messages into the network to distract drivers from choosing a specific route, or can use the network to determine a driver's location or identity. On the other hand, by gaining unauthorized access to in-vehicle network, an attacker can gain the control of critical components of a vehicle and cause irreparable damage to the vehicle or its passengers. In this thesis work, we have analyzed the security vulnerabilities in vehicular networks, both in inter-vehicle and in-vehicle networks and present a number of known and practical countermeasures with regard to real-time constraints.

1.1 Scope

The scope of this thesis work is to study vehicular network security issues and their countermeasures. Therefore, both VANET and in-vehicle network security vulnerabilities and countermeasures are presented. The purpose of this thesis work is to find a study these vulnerabilities thoroughly and to present a solution to securing vehicular networks from unauthorized and malicious access.

1.2 Method

The thesis work is divided into two main parts. In the first part, VANETs are discussed and analyzed while in-vehicle network security is studied in the second part. The work continues with the study of characteristics of VANETs. Afterwards, common attacks in the Vehicular Ad hoc Networks (VANETs) and also VANET's security requirements are studied followed by ways of securing VANETs against cyber attacks. Later on, common and known attacks in the in-vehicle networks are presented and discussed. These attacks include attacks on CAN and FlexRay buses as well as ECU behavior upon receiving malicious or malformed packets. A discussion is followed by summarizing the whole report and our proposed solution to overcome security vulnerabilities of vehicular networks is presented. Finally we have ended the thesis work by concluding our work and the list of references and appendices are presented at the end.

1.3 Acknowledgements

This thesis work was initiated by the Sigyn II project initiated by Volvo Cars AB, a project at Volvo where the robustness of in-vehicle networks with respect to safety and security malfunctions is assessed. We would like to thank our supervisor Tomas Olovsson for introducing us to this new and trendy topic and also Pierre Kleberger for his guidance and insights.

2 Vehicular Ad Hoc Networks (VANET)

Vehicular Ad hoc Networks (VANETs) are a subcategory of mobile ad hoc networks which are recently being discussed in great extent. The main idea behind VANET is providing communication among vehicles and also among vehicles and a number of fixed equipment located on the road. Several research projects have focused on this interesting and useful area in order to implement it in the best possible way.

The main intention with VANET's is to enhance vehicles' passengers' safety and comfort by distributing traffic, road and weather conditions among nearby vehicles. Among its applications collision warnings, road sign alarms and automatic toll/parking payment can be mentioned.

VANETs consist of a number of On-Board Units (OBU) which are located inside the vehicles and a number of Road-Side Units (RSU) which form the infrastructure of the network. OBU is a wireless gateway which can be connected to other OBUs and RSUs. Each vehicle equipped with the OBU can become a part of the network and will be able to send, relay and receive messages throughout the network. Due to its ad hoc nature, there won't be any centralized servers and vehicles are in charge of network management themselves. Communication in VANET is divided into two different categories:

- Vehicle-to-Vehicle (V2V) Communication, were the nearby vehicles will communicate traffic and road conditions to one another
- Vehicle-to-Infrastructure (V2I) Communication, were vehicles communicate their gathered information to the nearest RSU in order to distribute the information faster and more effectively.

Figure 1 below presents a conceptual model for Vehicular Ad hoc Networks (VANETs).

2.1 VANET Characteristics

Since VANETs are ad hoc networks, they have the characteristics of typical Mobile Ad hoc Networks with a few exceptions like the order of movement in VANETs, which is more organized compared to MANETs. Additionally, there are other positive properties of VANETs according to [1]. VANETs do not have energy constraints since they are connected to the vehicle's electrical system. This will reduce a number of known attacks on mobile ad hoc networks which target low energy sources of network nodes. Also, time and position in VANETs are known and are used for traffic messages and also security. Physical access to the network is limited to the driver and the authorized service center which will make unauthorized and malicious access harder. Also, due to vehicle's periodic maintenance, regular checks on the network can be done.

There are also a number of negative properties of VANETs compared to MANETs. Nodes in vehicular networks have more mobility. Since the average speed is usually more in VANETs, changes in the network topology will be more common and therefore, some characteristics or features may not work properly in VANETs. Also, as the interest in vehicular networks increase, larger networks will be created which require sufficient performance. Privacy is the main

drawback of vehicular networks. There needs to be a planned privacy plan for vehicular networks since a vehicle's life cycle is fairly long and there may be multiple owners of a single vehicle during its life cycle. Also, due to the ad hoc nature of vehicular networks, there will be no centralized infrastructure in order to manage security and privacy issues. Therefore, some IT-based security and privacy countermeasures, such as key management, may not work properly in vehicular networks. Finally, since VANET users are mainly the drivers of the vehicle, they should not be constantly disturbed with network messages and required actions. Therefore, user interaction will be an issue in vehicular networks.

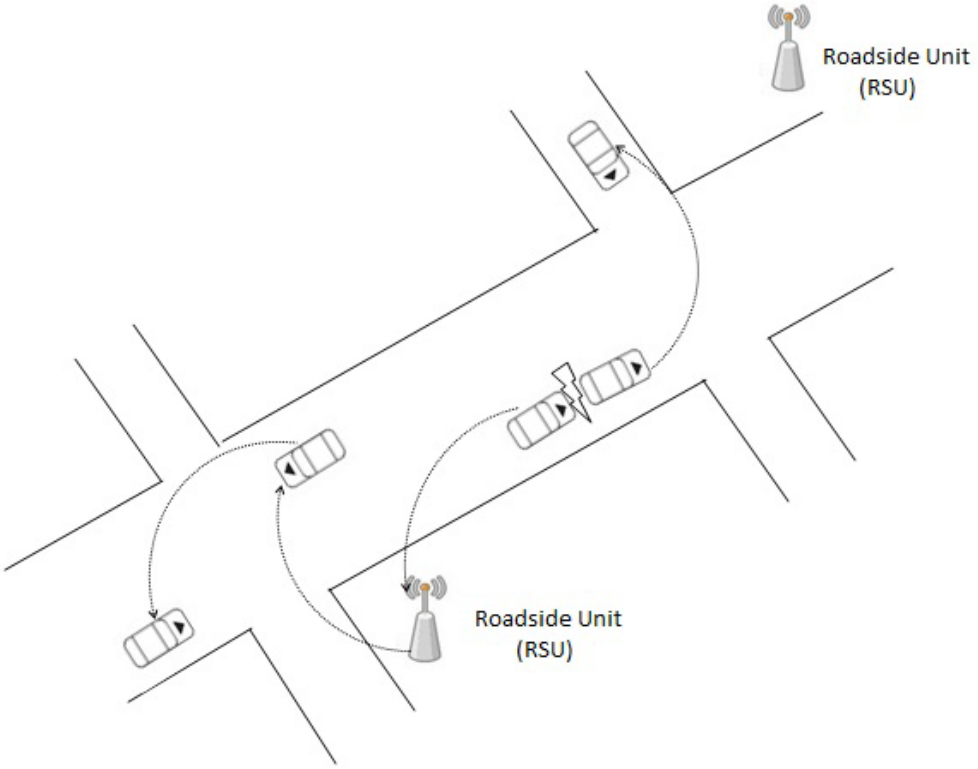

Figure 1. Conceptual VANET Infrastructure

Apart from the mentioned characteristics and drawbacks, security as well as privacy issues will be the main concern in vehicular networks which must be fully considered in order to have an efficient and useful network. By injecting false and invalid information, a malicious user can divert traffic from a specific road and take an advantage. On the other hand, drivers' identity must always be considered and should never be revealed to any other user through the network. Therefore, VANETs must be designed with respect to privacy of drivers' identities and on the other hand, information must be validated on the network in order to be useful.

2.2 Attacks on VANET

Due to the inherent wireless characteristic, VANETs are open networks and can be easily accessed by attackers. Due to the introduction and implementation of new technologies, attackers will be strongly motivated to exploit the vulnerabilities of VANETs. In the following paragraphs, we introduce the most important attack scenarios in the VANET domain.

2.2.1 Sybil Attack

The Sybil attack is a known attack in networking which is forging identities and masquerading as multiple users in P2P networks. It is most common in environments where there are no digital signatures or Certificate Authorities (CA) to verify the identity of users. It is also worth mentioning that the Sybil attack is also possible to be lunched in networks where a node can have multiple digital signatures or can get multiple certificates from a single CA. Since vehicular networks were originally created without the presence of digital signatures or CAs, attackers can easily launch a Sybil attack in order to inject false messages into the vehicular network.

There are a number of methods suggested for preventing Sybil attacks but some of them such as “radio resource testing” are not applicable in VANETs since they mainly require radio channels or resources which can be easily Obtained and used by the attackers in vehicles. The most common countermeasure is to use digital signatures and certificate authorities in which each network device must be allowed only one signature and certificate. It must also be mentioned that digital signatures and CAs must be implemented with minimum overhead on the network nodes and bandwidth otherwise they will be of no use in vehicular networks. Node registration is another method which can be used to identify unique users. Vehicle identities are assigned by a central and trusted authority and license plate numbers are an example of this method [2]. But in this case, serious privacy issues will be raised since vehicle location and driver information must be transparent and should not be revealed. Finally, position verification is introduced in [2] where the network verifies the position of each node. In this method, identities that come from the same location are assumed to belong to the same participant [2].

2.2.2 Bogus Information

This attack particularly targets messages transmitted between vehicles. An attacker can affect other drivers’ behavior by spreading wrong information in the network. For instance a driver can simulate a heavy traffic and thus preventing other drivers to choose the road he is driving on. This attack can be launched by both legitimate network nodes as well as outsiders. One proposed solution to mitigate this attack is to verify the received data in correlation with the data received from other sources. The important issue in this context is the correctness of the received data rather than its source [3].

2.2.3 Denial of Service (DoS)

Vehicular networks working on a wireless medium are specifically vulnerable to denial of service attacks. By jamming a vehicular network channel or flooding a vehicle's resources by injecting dummy messages, an attacker will be able to prevent messages from traveling through

the network. Therefore critical applications which require real-time messaging will not operate properly putting the driver's life to danger. One proposed solution in [3] is to switch between different channels or even between communication protocols when one is down as a result of a denial of service attack.

2.2.4 Impersonation (Masquerade)

By using a fake identity an attacker can pretend to be another vehicle. In case of using digital signatures, masquerading attacks will no longer be possible since nodes have anonymous public keys which act as unforgeable Electronic License Plates that are unique and verifiable [3].

2.2.5 Alteration Attack

This attack can be launched by modifying, corrupting and/or reusing the existing data such as delaying message transmission, replaying previous transmitted messages or altering some specific fields in a message. Therefore vehicular applications need authentication of both the source and the data [4].

2.2.6 Replay Attack

As the name suggests, this attack is basically using previously generated frames in new connections. A malicious user can capture a generated frame and use it in other parts of the network. Replay attack is usually used by malicious or unauthorized users to impersonate a legitimate user/RSU.

In order to prevent replay attacks in vehicular networks, [5] suggests two options. The first option is using a globally synchronized time for all nodes which will require a lot of official and organizational work and the other suggested option is using nonces. With a few considerations, this solution sounds more reasonable. Appending geo-synchronized timestamps obtained from GPS is another method [6]. This approach is easier to implement since GPS is becoming more common among drivers and more vehicles become equipped with GPS each day.

2.2.7 Illusion Attack

Typical attacks in vehicular networks are, as described earlier, attempts to try to mislead other vehicles by injecting false or unauthorized messages and frames into the network. But with the illusion attack, the attacker will intentionally try to deceive the sensors on his vehicle to produce wrong sensor readings [13]. By doing so, the messages will be originated from authentic and registered nodes and therefore other users will be more likely to believe the contents. In addition, falsely produced sensor messages will be distributed in the network which may lead to wrong decisions by the drivers.

In order to protect against such attacks, typical signature verification or node registration techniques won’t work since the false information originates from an authorized user. Therefore, [13] suggests using a new protection mechanism called Plausibility Validation Network (PVN). It is basically a database with a number of predefined rules and a plausibility network (PN) which is used for verification purposes [13]. Received messages will be checked in the

plausibility network with their respective rules retrieved from the database. If a match between the received message and a database rule was found, the message will be accepted, otherwise it will be dropped.

PVN has a number of drawbacks. Since new rules must be added to the PVN database frequently, and the addition should be done by the manufacturer, vehicles must be called in for service more often which can be unpleasant for owners and costly for manufacturers. On the other hand, some transmitted messages require real-time processing and sudden reaction which might not be fulfilled if PVN has a number of messages waiting to be validated.

2.3 VANET Security Requirements

In order to have a secure and dependable vehicular network, a number of security requirements must be considered. Some of these security requirements are the same for all networks but some are valid and specific to vehicular networks only.

With respect to the mentioned attacks and vulnerabilities in the previous section, securing vehicular communications in all aspects is a must. Here we provide a list of some general security requirements that must be taken into consideration in order to mitigate vulnerabilities and attacks against VANETs.

2.3.1 Authentication

As mentioned earlier, despite the lack of need for confidentiality, network nodes must be authenticated in order to be able to send messages through the network. Before reacting to messages and events a vehicle must verify the legitimacy of the message and its sender, therefore there is a need for authentication. Without authentication, illegitimate and malicious users can inject false messages into the network and confuse other vehicles by distributing false information. With authentication, vehicles can simply drop messages from unauthenticated users.

2.3.2 Authorization

Authorization is on a higher level implemented by access control which itself is defined by network policies. Authorization defines the role of a node in the network which includes the types of messages a node can read or write on the network, actions it is allowed to take and generally the protocols that it can execute [1].

2.3.3 Data Consistency

In addition to authenticating the sender, the consistency of messages with similar ones regarding time and location must also be considered, because false messages from legitimate senders are not impossible [3]. It is extremely important for warning messages to meet the time and location constraints. A warning message must be shown to the driver before it is too late to react and also before passing the corresponding geographic location of the warning [7].

2.3.4 Confidentiality

Since security in vehicular networks is related to safety, all network users should normally have full access to network data, i.e. traffic information, road conditions, etc. in order to make informed decisions. Since messages in VANETs don't contain any sensitive information and are not confidential, there is no need for encryption and confidentiality is not an important issue. Therefore, vehicular networks do not have to be protected against eavesdropping [8]. However, network data should be sent from authenticated sources and this can be done by source authentication.

2.3.5 Integrity

All messages which are sent and received on the network should be protected against alteration attacks. A secure vehicular network should provide protection against message alteration. A message can be altered in several ways during its transit from source to destinations and all possible attacks must be considered.

When it comes to integrity there are three main threats directly related to message contents. System threats regarding integrity include (1) wrong or forged messages, (2) messages which are modified during transmission and (3) replayed messages.

2.3.6 Availability

Since vehicular networks require real-time responses, they are vulnerable to denial of service (DoS) attacks [4]. In order to remain operational, protocols and services must be resilient against denial of service attacks. The communication channel must be available at all times, it must also be reliable otherwise attackers can launch Denial of Service attacks. Such attacks can disrupt the entire network which will lead to failure in delivering network messages to other vehicles in range. Therefore they must be securely designed and be fault-tolerant in order to work under faulty conditions [1].

There are a couple of security measures such as channel monitoring which is a means to increase channel availability. Besides, new technologies are always under development which will try to increase availability in communication channels.

Although availability can never be completely guaranteed, yet there are still a couple of security measures such as channel monitoring which is a means to increase channel availability. Besides, channel switching and using different communication technologies in case of jamming attacks can be helpful [14].

2.3.7 Non Repudiation

When a node sends out a message, it shouldn’t be able to later deny sending that message. In case of accidents or investigations, problem-causing drivers should be reliably identified, to correctly address the sequence and contents of exchanged messages. This can be done by signing outgoing messages with an anonymous key exclusively related to the sender and also a time-

stamp associated to the message preventing the user to claim that a particular message has been replayed [3].

In case of using digital signatures, each message is signed with its private but anonymous key. Therefore the vehicle owner cannot claim that he hasn't sent the message [3].

2.3.8 Privacy

Driver privacy is an important issue in vehicular communications. Drivers don't want their personal and private information to be accessible by others. Since the vehicle information such as location, speed, time and other car data are transmitted via wireless communication, there should not be possible to infer the driver's identity from this information. Among this information, driver's location and tracing vehicle movements are more sensitive and must be taken into consideration carefully [7].

Regarding this issue we come to another requirement called "anonymity" which is discussed below.

2.3.9 Anonymity

Anonymity defines the requirement that network nodes must not be able to infer if a node performed or will perform some specific action in future. In order to prevent such inferences, there must be an equal probability of doing a specific action by all nodes, or have strong probabilistic anonymity, with the probabilities being equal for all nodes [9]. By not requiring a vehicle to authenticate with its exact identity to other vehicles to which it sends information, an anonymization service can also help to mitigate the compromise between authentication and privacy [4].

2.3.10 Real-time Constraints

In order to have vehicular networks secured, specific measures and techniques have been suggested. Although these techniques seem applicable and useful, there is one important issue that must be taken into account, real-time constraints. Out-dated messages, e.g. out-dated traffic or road/weather conditions, are of no use in vehicular networks and must be eliminated in order to let the newly generated messages get to their destinations on time. On the other hand, solutions such as digital signatures and certificates must be designed specifically for vehicular networks in order to fulfill real-time constraints of such networks.

2.4 Securing VANETs

There are currently a number of known techniques and methods in order to prevent the attacks mentioned in the previous sections. In this section, we present three possible methods which can reduce attacks against VANETs to a great extent.

2.4.1 Digital Signatures and Certificates

Since exchanged messages in VANETs (e.g. traffic information) do not contain any sensitive information, there is no need for confidentiality. Therefore message passing in VANETs requires

only authentication but not encryption and therefore digital signatures seem the best suitable solution.

Symmetric and asymmetric authentication techniques are the two main approaches in implementing digital signatures. Comparing symmetric and asymmetric authentication techniques, symmetric mechanisms don't require handshake for establishing a shared key, hence they have less overhead per message than asymmetric techniques and are more efficient.

Due to the large number of network members and occasional connections to authentication servers, the most appropriate solution for implementing authentication would be a Public Key Infrastructure [3].

2.4.1.1 Digital Signatures without Certificates

The concept of digitally signing messages is usually done by implementing a public-private key infrastructure using asymmetric cryptography. The sender of a particular message signs the message using its private key. Upon receiving, the other party (receiver) decrypts the message using sender's public key. Using this procedure the ***integrity*** and ***authenticity*** of the corresponding message will be verifiable by the receiver.

In addition to message authentication and integrity protection, digital signatures also provide non-repudiation protection. Therefore, impersonation attacks will no longer be possible to launch [7].

Simplicity, small system requirements and little overhead are the advantages of this concept. System nodes merely need to have the capability of sending, receiving and storing cryptographic keys in addition to having the processing capacity of encryption-decryption of messages.

However, digitally signing messages will not protect the system against message forging, denial of service and sybil attacks [7].

2.4.1.2 Digital Signatures with Certificates

Using certificates provided by a trusted certificate authority provides a system in which only messages form trusted nodes that have a valid certificate are accepted. Therefore, in such a system, the certificate authority will be able to trace back all the signed messages to their real sender's identity based on the link between issued certificate and the key used to encrypt the message.

A public key infrastructure is necessary to implement the concept of certificates issued by an authority. Before sending a message, the sender signs the message with its private key and provides the receiver with its CA's certificate. Before signing the message there is a time stamp concatenated with the message to guarantee message freshness.

Upon receiving, the receiver will decrypt the message (verify the sender's signature) using its certified public key. Sender's public key is verified by the receiver with respect to its certificate [14].

Associating digital signatures with certificates basically targets excluding external attackers such as a road-side attacker using his laptop computer to launch an attack scenario. Since only valid VANET nodes possess the certificates, other external nodes will not be able to send messages within the corresponding domain. Moreover there exists the possibility to identify and remove the malicious behaving or defective nodes by revoking their certificates [7].

One advantage of using public key infrastructure is the possibility of revoking certificates. By revoking the certificates of an attacker, misbehaving or malfunctioning nodes won't be able to use their keys and thus harm the vehicular network anymore [14].

The basic commonly used mechanism to achieve this concept is implementing CRLs (Certificate Revocation Lists) within the PKI system. CRLs containing the list of revoked certificates or keys are distributed among network nodes by the certificate authority [15].

2.4.2 Tamper Proof Device

One of the most important groups of attackers in the automotive domain are the internal attackers. Having the vehicle at hand, they have unlimited physical access to built-in equipment and can freely test any possible attack scenario. They have unlimited time and don't have to be worried about being tracked or detected.

There are two major primitives that must be addressed in physical security also referred to as ***tamper protection***. The first approach is to protect the internal information such as encryption keys, by preventing any disclosure or modification of the system internal data referred to as ***tamper-resistance*** or providing proper active responses upon detection of such threats and intrusions which is called ***tamper-responsive*** [10].

Tamper-resistant or also referred to as ***tamper-proof*** is a passive hardware security characteristic. This property protects the hardware device against being modified or accessed by unauthorized attackers by providing physical protection measures [11].

On the other hand, a ***tamper-responsive*** device has an active security characteristic, which protects is against tampering or modification attacks based on tamper-detection measures. Upon detection of an attack, a proper response is triggered to mitigate the attack effects [11].

The second approach which is also called ***tamper-evidence*** aims at detecting any potential disclosure or modification of the system internal information. This characteristic does not prevent security breaches, rather provides evidence that there has been an attack attempt. Regarding physical security, tamper-evident is a passive hardware component security

characteristic which determines whether the respective component has been modified or compromised [11].

Tamper Evidence

By using tamper-evident security measures, physical manipulation attacks against cryptographic modules can be detected. For instance a digital tachometer manipulation by a malicious attacker (driver) cannot be prevented but can at least be detected.

Typically, being tamper-evident is achieved through using official security seals, special labels (e.g. holograms and stickers) or different kinds of special packaging (e.g. crazed aluminium, bleeding paint, brittle package) [11]. Any manipulation on a tamper-evident protected device will leave sufficient and notable marks, making the attempt detectable afterwards. Items used for tamper-evident solutions must contain materials with special mechanical and chemical characteristics which are difficult to remove. They must also be sufficiently difficult to fake and must only be commercially available to authorized manufacturers [10].

Regarding this concept there is a need for some kind of a legal control authority, to regularly inspect and check the cryptographic modules for any potential tamper attacks.

Tamper Resistance

The property of being tamper-resistant does not mean that the device can detect tampering clearly, but rather means that it is capable of preventing physical attacks and intrusions or at least make them sufficiently difficult to launch.

According to [11], tamper-resistance is provided through using special packages (e.g. hardened steel, susceptible sealing, epoxy coating), special interlocking (e.g. security screws, welding), small semiconductor mechanisms, shielding mechanisms or logical measures such as bus and memory encryption or obfuscation. Any attack or tamper attempt toward these security measures will remain noticeable remarks which will be a tamper-evidence by itself.

Advanced tamper-resistant mechanisms will also try to mitigate the effect of external probation attempts such as side channel attacks. This can be done by deploying shielding mechanisms or using special materials which protects the device against sensitive electromagnetic frequency leakage.

Another useful solution proposed in [10], is to include a self-test mechanism within the tamper-resistant device. Upon every start-up, the integrity of sensitive internal information along with the validity of hardware resources must be verified. Therefore, any attack or tampering attempt will be detected and thwarted for instance by tamper responsive measures.

Tamper Response

Tampering attempts or intrusion attacks to the cryptographic device can be detected by tamper-detection mechanisms such as intrusion detection systems. There also exist some non-invasive

attacks based on environmental conditions such as temperature and power line attacks [10]. These attacks can be detected by deploying active sensors which constantly supervise the device's operating conditions. In case of such attacks, tamper-responsive security measures will trigger appropriate application and events to protect sensitive internal information.

Depending on the sensitivity of information and running application, tamper-responsive measures will interrupt or completely deactivate the running application and even delete the internal sensitive information [11].

There are two basic requirements assumed for tamper-response systems. First, the protected device must have an independent internal power supply which provides the capability to autonomously detect and react to tamper attacks. In some situations where the main power supply is no longer available, the device must be able to activate its zeroization circuitry independently. Second, internal sensitive information must be stored on RAM memory to make data zeroization (deleting internal secret data) fast [10].

2.4.3 Data Correlation

Data correlation is an effective technique, to discover attacks which are based on sending out false information. Using this technique a vehicle will be able to collect data from multiple different sources. By correlating the received information based on credibility, consistency and relevance, a node can determine whether the received messages are legitimate or not [12]. It is also important to note that, due to the inherent environment dynamism, data correctness is more important than its source legitimacy [3]. Further information about this topic based on data reputation techniques is presented in [2].

2.4.4 IEEE 1609.2 Standard

As a part of IEEE 1609 standard family, the IEEE 1609.2 [16] also referred to as WAVE (Wireless Access in Vehicular Environments) provides communication protocols specifically to be applied in vehicular communications (VANETs). IEEE 1609.2 standard is basically developed to secure vehicular communication messages against threats and attacks such as eavesdropping, masquerading, replay and other attacks. In order to do this, IEEE 1609.2 is based on Public Key Cryptography which also includes support for elliptic curve cryptography (ECC), WAVE certificate formats, and hybrid encryption methods [17]. According to [18], by introducing necessary administrative functions, IEEE 1609.2 will also support core security functions such as revoking a vehicle's certificate.

3 In-vehicle Networks

Modern vehicles do not operate with a number of connected wires and mechanical devices anymore. The number of electrical components and devices in modern vehicles are increasing dramatically which will be to the benefit of drivers, owners and manufacturers in several ways. Since everything will be operated by built-in computer devices, diagnosis of vehicles' problems will take less time since these electrical components can be checked easier by attaching a diagnostics device to the vehicle. Also, a malfunctioning component can alert the driver so that he or she can take appropriate actions. The use of modern technology in vehicles will result in having "smart vehicles" as well. Technologies such as airbags, Anti-lock Braking System (ABS), traction control and electronic differentials which are for the comfort and safety of drivers and passengers are made possible by using electronic components in vehicles.

Modern vehicles consist of Electronic Control Units (ECUs) which are in charge of controlling electronic components in the vehicle. Apart from the hardware, each ECU is controlled by firmware which is in charge of communication and performing specific tasks. ECUs perform different tasks such as engine control, entertainment units, mirror controls, etc. which need different requirements in terms of speed and criticality of message transfer. Since ECUs must communicate their information with each other and also receive data from sensors and controls, a network bus must be designed to transfer the generated information to the proper component. This structure is the basis for the in-vehicle network, which is used extensively in vehicles these days.

3.1 In-vehicle Network Structure

A typical modern car has around 50-70 ECUs onboard. As mentioned above, in order to deliver different messages and information on-time and due to different demands and requirements of ECUs, different network types must be created based on speed and reliability. These networks are connected by gateways in order to be able to communicate with each other as well. Network nodes communicate thorough buses; they put their data on the connected bus and receive data from all other nodes since for most networks there is no destination address in the generated messages in in-vehicle networks. Figure 2 shows a conceptual in-vehicle network infrastructure.

3.1.1 ECU Classification

ECUs can be classified into five different categories based on the criticality of their tasks and the effect of failure on passengers' safety [19].

- *Powertrain ECUs* are used for controlling critical vehicle components such as engine control (e.g. traction control) and braking system (e.g. electronic brake force distribution). Failure in such ECUs will cause serious risks in vehicle safety and will damage the vehicle; therefore, these ECUs will be classified as safety-critical [20].
- *Vehicle safety ECUs* will provide assistance to the driver in terms of safety and control. Such ECUs use information about road conditions, driving speed, etc. to maximize car safety.

Examples of vehicle safety ECUs are adaptive cruise control, ABS, collision avoidance systems and airbag. This category will also be classified as safety-critical.

- *Comfort ECUs* are of less importance compared to other two categories. These ECUs provide services such as temperature control and parking assistance, therefore, on the condition of failure such ECUs will not put the vehicle in danger.
- *Infotainment* is another category which is a non-safety related category of ECUs [20]. This class of ECUs is in charge of entertainment units such as CD/DVD players, audio streams, navigation systems, etc. which will not affect the safety of the vehicle in case of failure. However, this class requires very fast bus since audio/video information need fast transmission.
- *Telematics* are the final category of ECUs which provide networked software applications to the vehicle [19]**.** This category will also be classified as non-safety related since they won't immediately affect the safety of the vehicle or the driver.

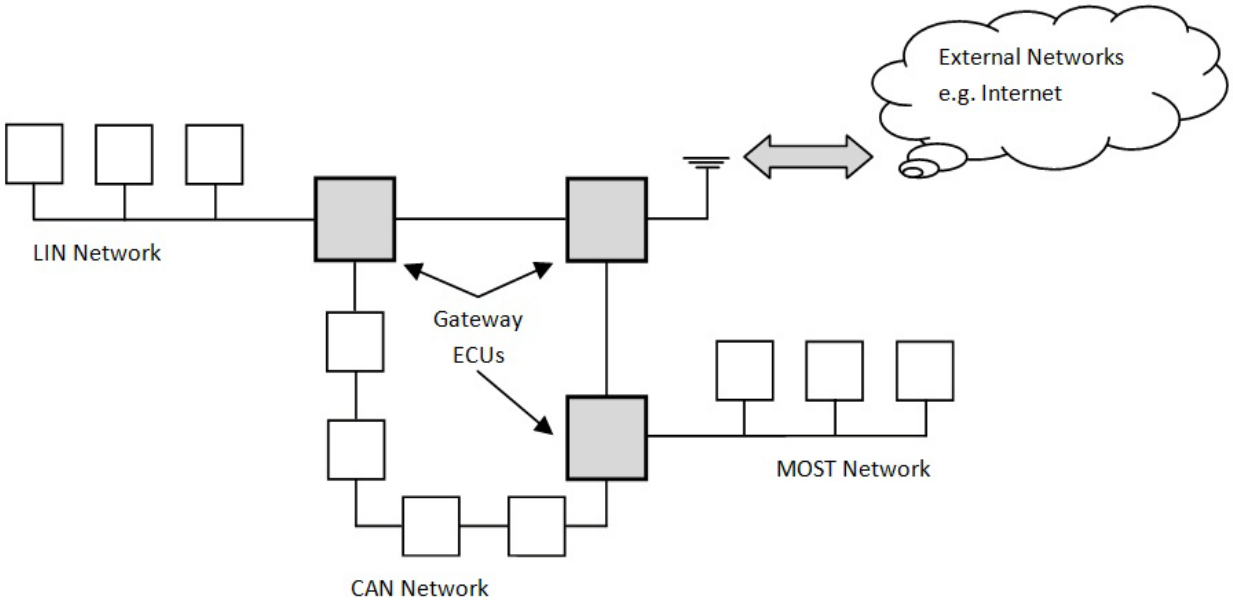

Figure 2. In-vehicle Network Structure

3.1.2 Automotive Bus Systems

Apart from ECU classification, in-vehicle networks require different communication buses with different characteristics as well. These buses are different from one another in terms of architecture, access control, transfer mode, data rate, error protection, etc. Each communication bus is used for a different ECU class to improve the real-time and speed demands of that specific class.

Local Interconnect Network (LIN) is the simplest communication bus with a slow data rate which is used for communication between sensors and actuators. It is used for small autonomous

networks which control basic tasks such as power-windows, automatic door-locking, etc and is ideal for components which do not need priority and also do not communicate critical messages. LIN is single master which will provide collision-free communication among 16 slaves.

Controller Area Network (CAN) is basically used for critical components due to its characteristics. It can have the data rate of up to 1 Megabit per second, is event-triggered and has a multi-master architecture which will lead to a redundant network. Access control is provided through CSMA/CA and protects messages from errors through CRC and parity bits. The mentioned characteristics make CAN an ideal platform for safety-critical ECUs since the network will be redundant and perform error handling. The drawback in CAN is the lack of addressing. CAN messages do not have a receiver's address, therefore, a generated CAN message will be received by all ECUs and each ECU must decide independently whether to drop or read the message.

Media Oriented System Transport (MOST) is the serial high-speed bus used for transmitting audio, video, streams and control data via fiber optic cables [21]. It has a small control channel for transmitting control messages and the data channel can have the data rate of up to 14 megabits per second. The sender and the receiver addresses are specified in the message and access control is provided through Time Division Multiplex (TDM) [21].

FlexRay is the ultimate solution for automotive bus networks and is a replacement for CAN to meet future application demands. It offers high speed and error-tolerant communication which can be used by powertrain ECUs for critical applications. FlexRay is time-triggered which is characterized by a continuous communication of all connected nodes via redundant data buses at predefined intervals [22] and provides access control through Time Division Multiple Access (TDMA). FlexRay introduced a multi-master architecture called Bus Guardian which is used to guarantee the safety and security of the communication channel and protect it against faulty conditions. Table 1 compares the mentioned automotive bus systems.

Bus Type	**LIN**	**CAN**	**FlexRay**	**MOST**
Example of Usage	Door-locking Electric window	Airbag, Engine control, ABS braking, Electronic differential	X-by-Wire systems	Navigation Multimedia applications
Architecture	Single-Master	Multi-Master	Multi-Master	Multi-Master
Access Control	Polling	CSMA/CA CSMA/CR	TDMA FTDMA	TDM CSMA/CA
Data Rate	20 Kbit/sec	1 Mbit/sec	10 Mbit/sec	24 Mbit/sec
Error Protection	Parity Bits Checksum	Parity Bits CRC	Bus Guardian CRC	CRC System Service

Table 1. Automotive Bus Systems

3.1.3 CAN Message Format

CAN is a serial communications protocol and is used by powertrain ECUs to communicate their information and data. In its standard, only the physical and data-link layer protocols are defined which enable the communication between the network nodes [23]. Other layers such as application layer must be designed by manufacturers based on their requirements and standards. CAN uses CSMA/CA which means nodes listen to the communication bus all the time in order to avoid collisions. There are four different message formats in CAN which are data, remote, error and overload. The data frame carries data from a transmitter to the receivers and the remote frame is used for requesting the transmission of the data frame with the same identifier. Error frames are generated when a node detects an error and the overload frame is generated by a node when it detects overload conditions. Data frame structure in CAN is shown in figure 3.

SOF	Identifier	RTR	Control	Data	CRC	ACK	EOF
1 bit	11 bits	1 bit	6 bits	0-8 bytes	16 bits	2 bits	7 bits

Figure 3. CAN Message Format

Data frames in CAN begin with the Start-Of-Frame (SOF) bit and is followed by an identifier field which contains information about the message. RTR indicates whether the frame is a data frame or a remote frame. Control bits contain the length of data field. Data field contains the main information. CRC is used for redundancy checks and ACK is for acknowledgement. Finally EOF indicates the end of frame.

The CAN bus has an arbitration mechanism which in the event of conflicts between two senders, the sender with higher priority in the identifier field will take over the bus and other nodes will be receivers. If two or more senders start transmitting simultaneously, they will start by sending their SOF bit. Afterwards, they will start transmitting their identifier fields. All the senders will transmit their identifiers as long as identifier bits are equal. Once the identifier bits differ, the sender with higher bit value will continue transmitting and others will stop sending their frames and will become receivers.

3.2 Recent Improvements in In-vehicle Networks

ECU firmware must be possible to updat in order to have maximum performance and fix occasional software bugs. Firmware updates must be done by the manufacturer and its authorized service centers which can be costly for the owner and the manufacturer. Recently, the concept of remote software updates has drawn the attention of the car industry. Remote software updates will not require an authorized service center and needs a secure manufacturer's web portal and a secure communication channel instead. Vehicles can connect to the manufacturer's web portal and download the software to their respective ECUs. The concept is called Firmware Updates

Over the Air (FOTA) and is to the benefit of owners and manufacturers in terms of time and money. The procedure works by re-flashing current ECU software and installing new firmware. By having downloaded the new ECU firmware, the ECU will reboot and work with the new firmware [24]. FOTA is beneficial in a number of ways, namely [24] [25]**:**

- Minimizing the need for customers to visit an authorized service center
- Possibility for the manufacturers to update a massive number of vehicles at the same time
- Possibility of faster firmware updates
- Increased quality
- Time saving and less inconvenience

Apart from FOTA, by connecting in-vehicle networks to external networks, vehicles can be diagnosed remotely without being taken to service centers. A car can be checked up over the Internet and can alert the driver about the resulting diagnosis. After check up, appropriate measures can be taken by the driver.

3.3 Security Considerations

Although the mentioned improvements and concepts will be time-saving and value-adding, security considerations must also be taken into account in order to be able to implement such concepts successfully. *Safety* issues have been addressed completely in CAN networks, as they are quite robust against non-malicious node failures. S*ecurity* issues however, are yet still remained unsolved in in-vehicle networks. Therefore, with the growing interest in applying new technologies and embedding new devices into the vehicles, these security issues must be solved.

Since in-vehicle networks were originally designed to work in isolation and didn't need to be connected to external networks, security issues were not addressed completely. By connecting in-vehicle networks to external networks without securing them, attackers and malicious users will be able to access the network and perform unauthorized actions. These actions may cause an ECU to stop functioning and lead to safety critical events such as accidents on the road.

As an example of design flaw in in-vehicle networks, lack of unicast addressing can be mentioned. Once a message is generated and placed on the bus, all the attached nodes will receive the message and will independently decide whether to execute or drop the message. By exploiting this flaw, attackers can inject messages into the bus system and target any desired ECU. There have been a number of examples in the literature about malicious activities such as controlling the electric window, warning lights, airbag control system, etc [26]**.** These attacks are successful due to lack of proper addressing and checking the authenticity of senders. In the next section, we study the threats to in-vehicle networks which must be addressed in order to have a reliable in-vehicle network.

3.4 Threats to CAN Networks

Apart from the mentioned design flaws, there are a number of considerations in terms of confidentiality, integrity, authenticity, availability and non-repudiation in in-vehicle networks. These issues must be carefully considered in order to secure in-vehicle networks.

3.4.1 Confidentiality

CAN bus messages are sent over the common bus. Therefore all ECUs connected to that bus will receive all messages and decide whether to use the message or not based on the type ID of the message. Hence, privacy will be an issue when ECUs want to communicate confidential information. Therefore, an attacker can read all the data sent on the bus and is also able to even send data on the bus from a remote location using the external gateway. In FlexRay, the attacker can learn secret keys, proprietary or private data which are sent on the bus as well [22].

3.4.2 Integrity

CAN uses CRC checksums in order to verify the message's integrity. Since CRC checksums are non-secure, CAN messages are open to alterations. In [27], using cryptographic hash functions are suggested which may seem convincing, but on the other hand, increased processing time, network overheads and delays must also be taken into account.

3.4.3 Authenticity

A major security flaw in the in-vehicle networks is the lack of sender and receiver address in the frame. Using this design flaw, a message can easily be spoofed and sent on the bus for the victim ECU, e.g. an attacker can create and inject diagnostics messages and force ECUs to perform arbitrary actions [22]. ECUs cannot verify the authenticity of a message and will rely on its contents which may result in performing unauthorized and abnormal actions [27].

3.4.4 Availability

Denial-of-Service attacks are hard to be protected against. Since there is no control over a malfunctioning ECU in CAN networks, an attacker can repeatedly spoof error or high-priority messages and send them over the bus. This will culminate in a Denial-of-Service attack on the communication bus and other nodes cannot use the bus to send their messages. According to [27], "FlexRay considers the option of disconnecting malfunctioning devices or branches from the network by node-local or central bus guardians".

3.4.5 Non Repudiation

Since the mentioned features are not fully addressed in CAN networks, it is almost impossible to identify a faulty ECU or a spoofed message after an attack or malicious behavior has occurred.

3.5 Attacks on In-vehicle Networks

As mentioned earlier, the design of in-vehicle networks has mostly focused on providing safety functionality; therefore they lack several security properties such as data confidentiality, data integrity, data availability, data authentication and data freshness. Therefore, security properties are at best slightly addressed in the implemented protocols [28] which will make it more or less trivial for attackers to perform malicious actions.

There are a number of building blocks defined in [28] which can be performed from any ECU within the CAN network. Some of these building blocks are intended for all ECUs, while some of them are merely intended for gateway ECUs. These building blocks are described below [28]

- Read: Since all data are sent over the CAN network in clear text and also data is broadcasted over the network and lacks unicast addressing, an attacker can easily read all the generated and exchanged information on the CAN network. As shown in figure 4:

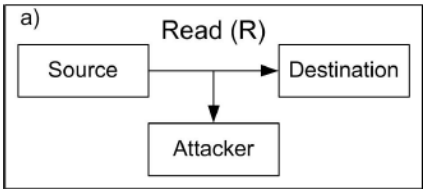

Figure 4. Read Building Block

- Spoof: Due to lack of authentication, the attacker can inject messages targeted to the victim ECU(s) into the network, as shown in figure 5.

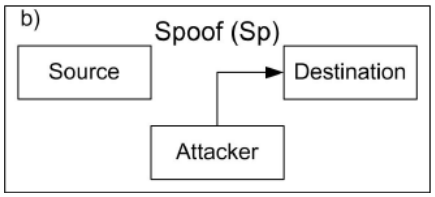

Figure 5. Spoof Building Block

- Drop: In this building block, the attacker will masquerade as the gateway ECU and will simply drop all the messages that pass through the ECU, as shown in figure 6.

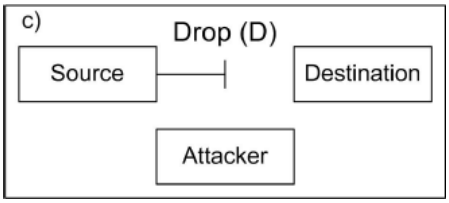

Figure 6. Drop Building Block

- Modify: Similar to drop, in this building block the attacker will masquerade as the gateway ECU, but he/she will change the contents of the incoming ECU messages and send it to other networks. As illustrated in figure 7, modify building block is the combination of read, drop and spoof building blocks [28].

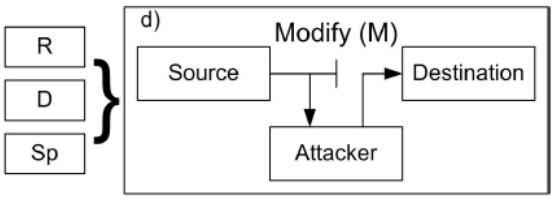

Figure 7. Modify Building Block

- Flood: By replaying messages at a high rate, an attacker can launch a flooding attack and cause the CAN bus to stop functioning due to high amount of generated traffic. This can ultimately result in a Denial-of-Service attack which is a serious vulnerability in in-vehicle networks. A flood building block is shown in figure 8.

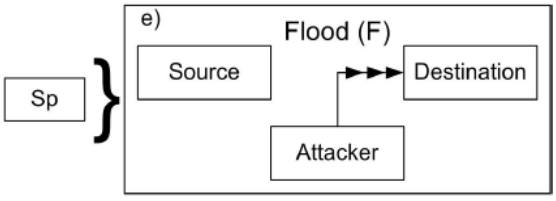

Figure 8. Flood Building Block

- Steal: In this building block, the attacker combines read and drop building blocks as shown in figure 9. Steal building block is a result of exploiting confidentiality and availability vulnerabilities within the network.

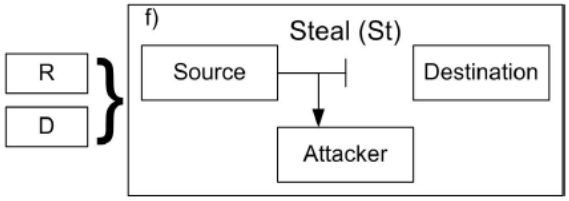

Figure 9. Steal Building Block

- Replay: As the name indicates, replay building block is a combination of reading and spoofing and targets lack of freshness in the in-vehicle network [28]**.** A replay attack is illustrated in figure 10 below.

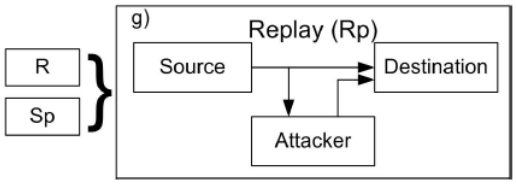

Figure 10. Replay Building Block

3.5.1 Logical Attacks

Logical attacks are basically launched by both internal and external attackers who have access to built-in interfaces as well as external communication. An external attacker, for instance, can exploit the available wireless communication interface used for VANET applications (e.g. C2C cooperative driving system). Likewise, an internal attacker can benefit from available on-board interfaces such as telematics or software update interfaces [11].

Logical attacks are typically launched by sending tricky messages to a device and cause it, for instance, to reveal cryptographic keys or running malicious software. These attacks are mainly based on exploiting design or implementation flaws in software development. Despite applying security mechanisms such as code reviews or sandboxing, there are still some security gaps and critical defects present in developed software, which is caused by the ever increasing software complexity [27].

According to [27], some security gaps regarding design and implementation flaws in software development include: buffer overflows, failure to secure code update processes, using insecure cryptographic algorithms, cryptographic protocol flaws, key management failures, random

number generator defects, using debug (test) functions that bypass security, improper error handling, incorrect algorithm implementations, improper reuse of keys, poor user interfaces, using weak passwords, operator errors, operating system weaknesses, sequence counter overflows, inability to reestablish security after compromises, among many others.

3.5.1.1 Software Attacks

Software attacks are particularly based on software errors and flaws occurring in the design or implementation phase such as: buffer overruns, incorrect input or output data, resource exhaustion, etc. By exploiting these vulnerabilities and weaknesses an attacker can cause unexpected program behavior in order to launch his desired attack scenario.

By injecting malicious code for instance, an attacker can try to exploit the ECU software update functionality. The malicious code will be downloaded to the ECU and will result in sending malformed or invalid frames with wrong intervals on the bus which will confuse other ECUs within the vehicle.

In some cases, an ECU's memory can be accessed without any restrictions by using its regular interface [29]. Also, ECUs can be physically disconnected and analyzed offline by internal attackers (e.g. the driver), in order to develop a proper malicious code in an unlimited period of time.

Today's embedded IT systems in vehicles contain up to 100 megabytes of embedded code [30], and it is extremely difficult and expensive to test and verify such a large amount of code. Therefore, software attacks based on exploiting vulnerabilities and flaws are one of the most important security issues in In-vehicle IT systems [11]

3.5.1.2 Communication Channel Attacks

Since vehicle manufacturers are trying to connect their vehicles to external networks, securing the communication channel between the vehicle and the external network will be an immediate need. From the attackers' point of view, the communication channel seems the best entry point to the whole vehicular network since there is no need for external attackers to gain physical access to the vehicle and they can perform their attacks and damages remotely.

As a primary security threat to vehicular IT applications, communication attacks target almost any communication channel used for data transmission. The external attacker as well as the malicious insider can mount both active and passive attack scenarios on any accessible channel.

Active attacks are based on intercepting, modifying or injecting the transmitted messages on the respective channel. On the other hand, *passive* attacks are generally based on eavesdropping the transmitted information and not actively interfering the communication channel.

Since the dawn of vehicle-to-vehicle and vehicle-to-infrastructure concepts, there have been numerous attacks on the communication channel which proves the importance of securing the

communication channel. Communication attacks range from very simple comfort restrictions to serious dangers for driver, passengers and others on the road [11]. In this section, common communication channel attacks on in-vehicle networks will be discussed.

Eavesdropping (Reading)

This attack which is also called wiretapping attack, records the transmitted information between two nodes without being authorized. The recorded data can be used later to extract sensitive information or mount other attack scenarios by the attacker [11].

Modification Attacks

By interfering with the communication flow, the attacker will modify, suppress or change the transmitted information to achieve his malicious goal, for instance gaining unauthorized access to a particular node [11].

Injection attacks or Insertion/Fabrication Attacks

In this type of attack, the attacker sends false messages into a communication flow, which will look like messages originating from a legitimate source. Hence he will be able to generate and inject new messages or even retransmit previously recorded and modified data (e.g. by eavesdropping) [11].

Replay Attacks

These attacks are based on repeating or delaying a valid data transmission. Therefore, by intercepting or eavesdropping a transmission flow and retransmitting it later, an attacker can bypass an authentication procedure (in which a fixed secret key is used each time) [11].

Impersonation and Masquerading Attacks

In this scenario the attacker tries to hide his identity and pretend to be a legitimate node by applying data modification or injection attacks. Therefore, the attacker will be able to gain higher privileges, abusing other's identities while not being detected [11].

Logical Denial of Service Attack

Logical denial of service attack is a malicious jamming attack which logically prevents or confines the availability of the communication channel. Denial of service attacks generally don’t require bypassing a particular security or cryptographic measure, and are therefore easy to launch. Comparing with physical DoS attacks which will be discussed later, logical DoS attacks don’t deal with physical channel properties, but are rather performed by repeatedly sending faulty messages or excessively running a particular program.

3.5.2 Hardware/Physical Attacks

Physical attacks can be launched by attackers who have access to physical on-board equipment. These attackers can explore the system offline and invent new attacks during a virtually unlimited period of time. Therefore, they will be able to try possible attack scenarios and finally launch a successful one. Once a target vulnerability is detected by the attacker, he can use it for a long period of time. This is due to the long vehicle life cycle and the slow software update rate, which makes the vulnerability available to the attacker even when there is a security solution issued for the case [11].

3.5.2.1 Physical attacks classification

Physical attacks can be classified into passive, active, invasive and non-invasive attacks [11]. During an *active attack*, the target device including its resources and functional operations will be directly manipulated by the attacker to act abnormally, using code injection for instance. However, physical *passive attacks* benefit from using system's information during its normal operation (e.g. by eavesdropping) and do not affect system internal resources.

In a *non-invasive attack*, the outer physical environment and interfaces will be accessed and manipulated by the attacker. In this type of attack, there is no access beyond the cryptographic boundary[1]. On the contrary, in an *invasive attack*, there will be direct access to the components placed behind the so called cryptographic boundary. This attack will cause irreparable damages as a result of physical manipulations to the target device.

Physical invasive and non-invasive attacks versus logical attacks are illustrated in figure 11 below.

[1] The cryptographic boundary is where the security-sensitive devices such as processor, memory and clock generator are enclosed.

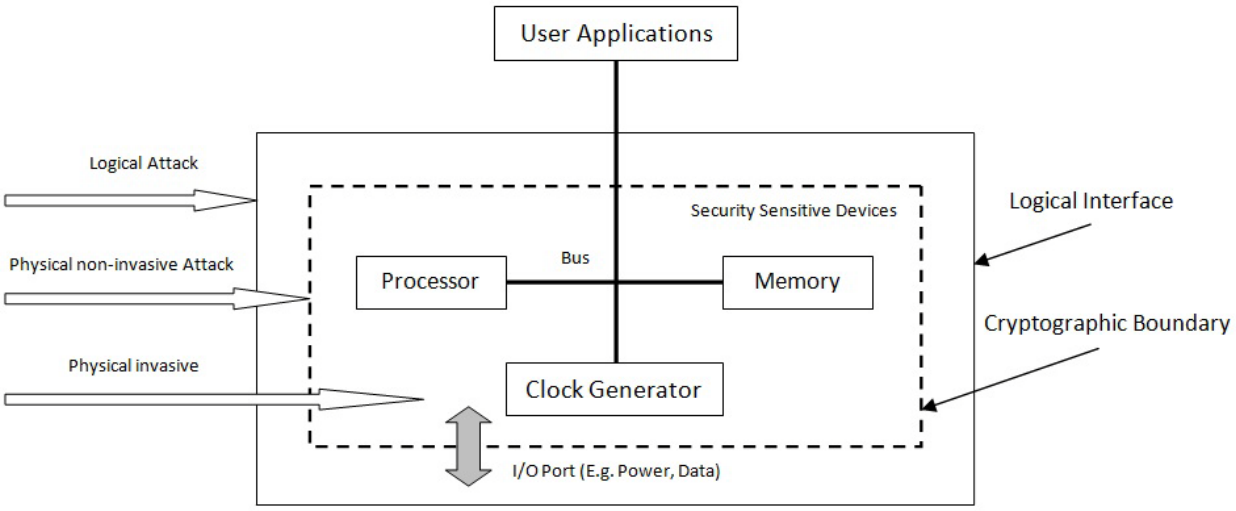

Figure 11. Physical vs. Logical Attacks

3.5.2.2 Physical attacks on in vehicle networks

In this attack type, malicious users or attackers will try to replace or modify critical and important components [30]. For less critical parts, this may not be to the detriment of the vehicle or its passengers, therefore these parts are not usually protected. However, for more critical components such as tachograph, speedometer or the airbag system, some basic protection mechanisms are used [29].

Side-Channel Attack

A side channel attack, also called a monitoring attack, is performed by examining the exposed characteristics of any device (e.g. ECU) or channel (e.g. CAN) available to the attacker such as power consumption, electromagnetic radiation or timing analysis. The attacker will intercept these signals while a cryptographic algorithm is being executed. Later, the secret key used in that specific encryption algorithm can be recovered by applying signal processing techniques and thus violating the security of the device.

A side channel attack is a passive and non-invasive attack and does not cause any damage to the system; therefore it is hardly noticeable which makes it a serious threat to the vehicular IT system [31].

Fault Injection Attack

A fault injection attack, sometimes called an active side channel attack is another type of physical attack. This attack will cause the target device to malfunction by changing its operating environment. In order to do this, the attacker may use different scenarios, for instance overheating the target ECU, overclocking, manipulate power or use high power electromagnetic fields. These abnormal operating environments will cause the target ECU to malfunction.

Therefore it produces faulty outputs which will eventually result in execution disruption and/or information leakage from cryptographic algorithms [31], [11].

Penetration Attacks

Also being referred to as reverse engineering, penetration attacks are based on directly reading the internal memory (e.g. RAM, ROM, Flash ROM) of the target ECU, intercepting the transmitted data or monitor any internal activity. This is done by using complicated microprobing mechanisms or by depacking the target ECU followed by a layout reconstruction [11]. Here, there is no need to go through a complete traditional reverse engineering process, since recovering a single cryptographic key would be enough to perform a successful attack.

This particular attack clearly reveals the importance of using tamper-resistant hardware (which here is the system memory) in In-Vehicle communication systems. Although available, tamper-resistant memory is not widely used in automotive communication systems due to cost or legacy restrictions [31].

Physical Denial of Service Attack

Denial of service attacks belong to the category of active attacks which can be both invasive and non-invasive. According to [11], physical denial of service attacks refer to disruption of physical availability by preventing or considerably delaying access to critical resources, communication or functionality.

Physical denial of service attacks are mostly done by signal jamming, data deletion or communication deactivation. These can be done by launching non-invasive attacks such as noise distribution using strong electromagnetic fields, as well as invasive attacks such as short-circuits, shielding wired communication channels or detaching transmission devices.

Test/Debug functionality

Almost all embedded systems are equipped with some kind of after sales maintenance mechanisms such as test, verification or diagnose functionality, which in most cases are not deactivated or disabled properly [11]. Later, software updates, validity tests, fault detections and many other verifications regarding the embedded hardware and its running software can be done using the aforementioned functionality.

By detecting this mostly undocumented functionality, an attacker can gain access to the system-internal information. Depending on his access level, the attacker will be able to modify internal values and functionality of the respective device to change the device's behavior or launch further attacks [11].

Apart from the mentioned threats and vulnerabilities, a combination of these attacks can also be built and launched against the in-vehicle network in order to form more sophisticated attacks. The concept is called vehicle virus [28] and can be built into a piece of code and be sent to the vehicle's network through a FOTA process. By a combination of the mentioned building blocks,

the virus can become more intelligent and may be able to cause considerable damage to the vehicle's network or extract invaluable information. Therefore, the mentioned security properties must be considered completely in order to prevent such actions to take place.

3.6 In-vehicle Networks Security Solutions

On a fairly high level, the concept of vehicular networks is divided into three main areas:

- Hardware, which are different devices such as ECUs, sensors, actuators, gateways, etc.
- Software which refers to ECU firmware which operates and controls ECU behavior.
- Communication Channel is the basis for different communication types including Vehicle-to-vehicle, vehicle-to-infrastructure and in-vehicle.

In order to have a secure and reliable vehicular network, all the mentioned areas must be carefully planned and designed. Since these networks were originally designed to work in isolation, there are different known threats and attacks against all the above areas which must be considered and fixed. In this section we will discuss different security solutions in the automotive area.

3.6.1 Physical Security

Although it is very difficult to stop highly motivated attackers, there still exist some security measures to at least make physical attacks somewhat harder and more costly to launch. Therefore, relying merely on physical security measures would not be sufficient to completely secure an In-Vehicle network system. Rather it must be assured that a security breach to individual hardware components will not allow the attacker to gain access to the whole In-Vehicle IT system [11].

Physical security countermeasure for in-vehicle networks is based on tampering protection mechanisms and tamper proof devices which has been comprehensively explained in details in section 2.4.2.

3.6.2 Software Security

In order to have ECU software protected, the vehicle must only accept original software and it must only accept software originated from trusted and authorized parties. By doing so, the risk of downloading malicious software will decrease. Vehicle networks must be designed in such a way that once one ECU's security has been compromised, other parts of the network must be able to work fine and not let the compromised ECU disrupt the whole vehicle network [29].

Digital signatures seem to be a good countermeasure to overcome software vulnerabilities. But the issue of limited resources in the ECU must always be considered as well. Secure software download [29] can be performed by having a trusted center to digitally sign the developed software. The trusted center can use its private key to encrypt the software code and signed code can be sent from the trusted party's portal to the vehicle's appropriate ECU, where the ECU can finally use the trusted center's public key to verify the signature.

Another protection method can be the use of a simple challenge-response mechanism. This method has much less overhead compared to key management mechanisms since the vehicle and

the portal both share a secret key and can run a challenge-response scheme to verify that their shared secrets are identical [29].

3.6.2.1 Embedded Information Security

Regarding embedded data and information security, [32] proposes two fundamental security solutions described below:

- **Tamper-resistant software:** In order to develop tamper-resistant software, there is a small trusted program embedded into a light-weight ECU within the vehicle. This is done by applying trusted computing techniques which combines both trusted software and hardware. The specific ECU will be fully trusted; therefore other parts can be developed with lower trust assumptions at lower costs, while the mentioned ECU will contain the small necessary trusted software.
- **Integrated gatekeeper:** A data security gatekeeper can be a connection point between the different existing networks (e.g. LIN, CAN, and MOST) within a vehicle. From a security point of view, the gatekeeper will be responsible for inspecting and managing the exchanged information passing through the gatekeeper. By secure communication and applications interaction control, the gatekeeper will be able to provide the system with both integrity and confidentiality. In figure 12, there is a data gatekeeper used as a connection boundary between inner and outer vehicle networks.

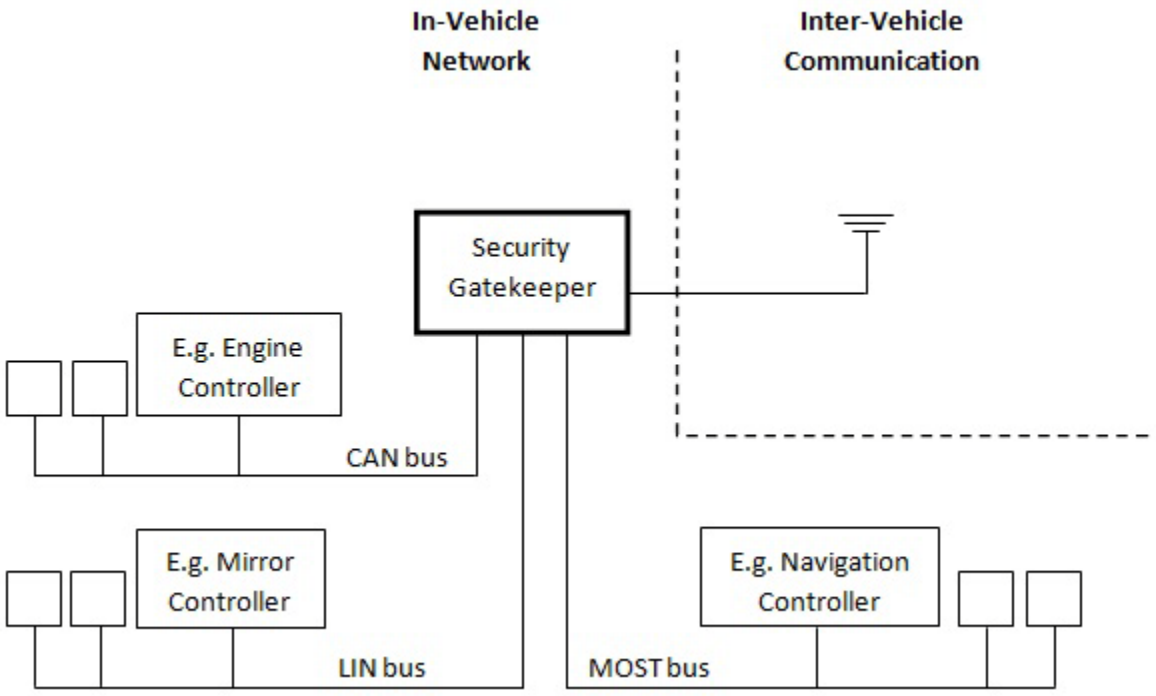

Figure 12. Integrated Data Security Gatekeeper

In order to do this, the gatekeeper must be securely protected with a tamper-proof device. It must also be able to completely protect the cryptographic infrastructure and operations (keys, algorithms, etc.) specifically the signing and verification of messages [32].

3.6.2.2 Intrusion Detection System

Intrusion Detection Systems (IDS) are a common way of protection against malicious behavior and unauthorized access in regular desktop IT systems and with some modifications, they can be used in automotive and vehicular networks as well. Extensive research has been conducted on developing efficient and effective Intrusion Detection Systems. They can become handy when there are no prevention techniques defined for special types of attacks. In this case, intrusion detection systems can alert the driver about the attack so the driver can take appropriate measures. Recently, due to the growing interest in vehicular communications and the need for security mechanisms in such networks, Intrusion Detection Systems are considered as a means to protect vehicular networks.

Since intrusion detection systems basically work by comparing incoming/outgoing messages with predefined patterns, a number of patterns in vehicular networks must be defined as malicious behavior. Three types of patterns which can be used in automotive intrusion detection systems are as follows [26]:

- Increased Message Frequency: Some devices in the vehicle network broadcast CAN messages frequently, therefore, single CAN IDs are sent over the network constantly with fixed frequency. Anomaly in sending such CAN messages can be a sign of unauthorized and malicious access to the network. Hence, this can be defined as a pattern in the intrusion detection system.
- Obvious misuse of Message-IDs: Since authenticity of the message is not supported in in-vehicle networks, an attacker can easily send malicious commands and use a legitimate ECU's ID and be certain that all victim ECUs will receive and act correspondingly. By doing so, fabricated messages will also arrive at the ECU whose ID has been used. Therefore, by adding some IDS functionality to the ECUs, these attacks can be identified and mitigated by the ECUs themselves.
- Low-level communication characteristics: While the two aforementioned patterns will work on link level, CAN networks can be protected on physical layer as well. By analyzing different features such as voltage amplitudes and their stability, the shape of clock edges, propagation delays, signal attenuation, etc. of different manufacturers, a detection mechanism can be developed in order to identify unauthenticated devices which will try to inject messages on the CAN network.

In typical desktop IT environments, Intrusion Detection Systems are categorized as network based or host based IDS. A host based IDS monitors the activities on end systems such as system threads and processes. Network based IDS, on the other hand, monitors and analyzes traffic on the whole network by e.g. packet inspection to find attacks and malicious behavior [33].

Regardless of type, IDS systems must compare its existing data with some reference data in order to be able to perform intrusion detection. In [26], two different approaches to intrusion

detection are presented. In the first approach, Rule-based detection, a number of predefined actions, behaviors and combinations are stored in a signature/rule database and network traffic will be compared with the values in the database. If a match between intrusion database and captured network traffic is found, the IDS will notify the administrator about the possible malicious behavior. The second approach, Anomaly-based intrusion detection, is based on detection of anomalies from the normal behavior. Normal actions are predefined for the IDS and an action will be considered malicious if it is deviating from the normal behavior [33]. Some commercial companies such as Snort [33] have developed hybrid detection mechanism which is basically a combination of rule based and anomaly based detection mechanisms.

When it comes to vehicular network's IDS, certain constraints will be introduced since vehicular networks are a lot different from typical networks in terms of resources, users and the time needed for different actions. An automotive IDS must be designed in such a way that it won't generate a lot of warning messages otherwise it may distract the driver from the road and may cause dangerous incidents. Warning messages must also be categorized into visual, acoustic and haptic groups based on their severity and order of action [33] and different alerts must be communicated to the driver differently.

Since in desktop IT networks IDS systems are usually used by system administrators and experts, generated warning and alert messages will be interpreted in a professional manner and the proper action will be taken. In vehicular networks, on the other hand, alerts and warning messages must be generated in the simplest way possible since some drivers have little or no knowledge of networks and attacks, let alone reacting to IDS messages.

Driver consultation is another important challenge in designing effective vehicular IDS. By introduction of Intrusion Prevention Systems (IPS), some intrusion detection systems will automatically take appropriate measures on the condition of an attack. This may seem a reasonable solution in vehicular networks since the driver won't be bothered with IDS messages and therefore won't be distracted from his main responsibility, driving. But on the condition of a false negative[2] or in special situations like in the middle of a highway, the car must not be able to take an action itself without consulting the driver.

The IDS database must be updated regularly in order to detect new attacks. In a typical computer network, the administrator can easily update the database by either downloading new patches or adding new entries manually. In vehicles, the database must be updated by the authorized manufacturer's service shops. Since vehicles have long maintenance intervals, the IDS database will not be updated regularly which may lead to successful attacks against vehicular networks.

[2] False negative is a condition in Intrusion Detection Systems where the IDS will not detect an active and ongoing intrusion.

3.6.2.3 Digital signatures and Certificates

The lack of two major security primitives namely *Authentication* and *Confidentiality* in the CAN bus, will make in-vehicle networks vulnerable to critical attacks such as manipulations and eavesdropping. Therefore, appropriate security measures must be taken in order to provide the two aforementioned properties. In typical desktop IT systems, authentication and confidentiality are provided by using digital signatures and certificates. With some modifications, they can be applied in vehicular networks as well. There are however some limitations in implementing digital signatures and certificates in vehicular networks such as real-time constraints and bandwidth limitations which must be carefully addressed. Powertrain ECUs' commands and messages must be sent and processed immediately since they perform critical operations in the vehicle and hence they should not wait for authenticity verification and encryption algorithms.

In terms of digital signatures and certificates, two different areas will be discussed in vehicular networks. Recent development in remote software updates have led to the need for a new infrastructure to authenticate the parties which are allowed to generate and send new software patches to vehicles. On the other hand, ECUs within the in-vehicle network as well as the communication bus must be secured against manipulation and eavesdropping as well. In-vehicle protection can be provided by in-vehicle ECU certificates and digital certificates.

A) Digital Signatures and Certificates for Secure Software download

In order to implement digital signatures for secure software downloading to in-vehicle networks, the issuer of the software signs the program code and the control unit in the vehicle verifies it. [29] Suggests six steps from generating the code up to securely downloading it to the control unit. In the first step, the code will be generated and then passed to a trust center in the second step. In the third step, the code is signed by trust center's secret key, passed back and attached to the program object code. Afterwards, in the fourth step the code is stored in a database. The code can now be downloaded to the appropriate control unit. Finally, ECUs can verify the authenticity of downloaded software by using their public keys which are stored in the ECUs (step 6). Figure 13 shows the procedure in more detail.

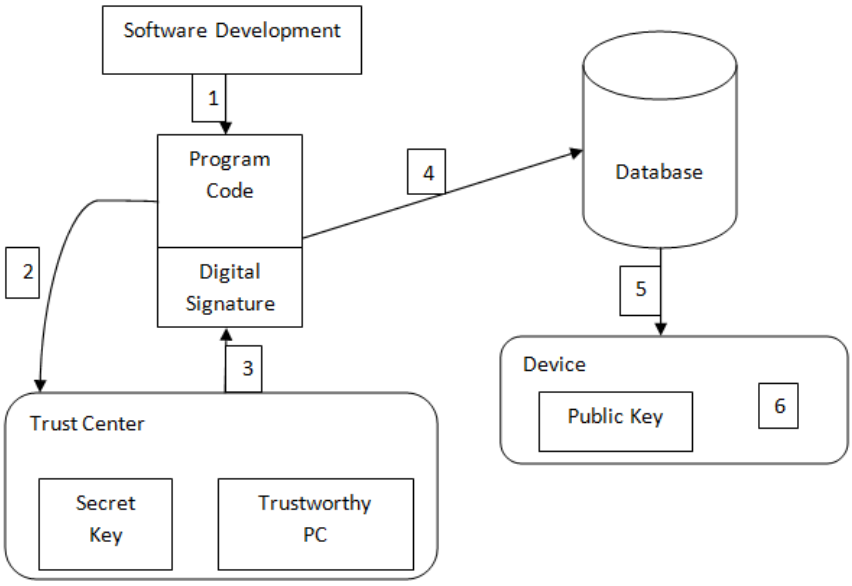

Figure 13. Secure Software Download

Due to the growing interest in remote software updates by both manufacturers and academics, most modern vehicles today are already equipped with software downloading functionality which will make it easier and much cheaper to implement the secure software download mechanism described above. Therefore, only the signature verification needs to be implemented in the vehicles and the rest have to be implemented on the desktop IT and organizational level.

There are a number of drawbacks in implementing secure software download in vehicular networks. First and foremost, the official procedures and organizational bureaucracy issues will emerge. There must be a central authority in charge of distributing secret keys among trust centers which will require a lot of official procedures. There are a large number of vehicle manufacturers, suppliers, content providers, etc. which must all be taken into account in designing such infrastructure. Also, key management and organizational security must be considered in the server side as well. Interoperability to existing infrastructures will also be an important issue which must be addressed carefully [29]. Finally, as mentioned earlier, resource and bandwidth limitations as well as real-time constraints should be taken into account in order to develop a structure with minimum processing and bandwidth overhead for the in-vehicle network.

It should also be mentioned that key management and ECU key protection is a crucial issue. By knowing or having access to the key, an attacker can change the keys and take complete control of the software download procedure and be able to inject his own generated malicious code into the ECU which may be to the detriment of the vehicle or its passengers.

B) Digital Signatures and Certificates for In-vehicle Security

Security in the in-vehicle network is also an important issue which must be considered seriously. As mentioned earlier, since in-vehicle networks were not originally intended for communication with external networks, they lack security measures. As a countermeasure, digital signatures and certificates are suggested to be used within the in-vehicle network. In this suggested countermeasure, ECUs must register themselves inside the network in order to be able to send and communicate with other network nodes, and if not, their messages will be discarded by the rest of the network. Gateway ECUs will be in charge of other ECUs' signature verification and authentication.

Authentication: will guarantee that only legitimate ECUs are able to send messages on the bus; therefore all ECUs having a certificate must authenticate themselves to gateways. According to the system policy all other unauthorized messages will be processed in a different way or will simply be discarded [11].

According to [21], a certificate contains the ECU's identifier, the public key and the authorization of the respective ECU. The list of valid public keys for different ECUs issued by the manufacturer will be kept within the gateway. Each ECU's certificate is then digitally signed with its respective secret key by the original manufacturer. While authenticating, public keys are used by the gateway to verify the validity of ECUs' certificates, the authenticated ECU is then added to the gateway's list of valid ECUs [21]. Each authenticated and valid ECU will then receive a symmetric encryption key which will later be used for encrypted bus communication (bus encryption key) [11].

Encryption: Another possible security consideration is to encrypt the transmitted information between ECUs within the bus system. Since there are some limitations regarding CPU computational power, memory capacity and timing issues in vehicular network systems, a combination of symmetric and asymmetric encryption is needed to achieve the highest degree of security and performance at the same time.

Symmetric encryption mechanisms are mainly used for data encryption and message integrity [31]. Symmetric encryption is the most appropriate mechanism for In-Bus communications since they are fast and require little memory and computational resources therefore are more efficient regarding resource constraints in In-Vehicle networks.

Asymmetric encryption is used for distributing and periodically updating the symmetric encryption key which is shared by all the ECUs within a specific bus system. Acquisition of public keys for newly added ECUs is also done through asymmetric encryption as well [21].

3.6.3 Firewall Gateway

Another solution to further securing in-vehicle communication is to implement a firewall mechanism within network gateways. If message authentication codes (MAC) or digital signatures are used as authentication and authorization between ECUs, firewall rules can be

derived from the authorizations given in each ECU's certificate [34]. On the contrary when there are no MACs or digital signatures used between ECUs, the rules of firewalls can be defined individually, based on each vehicular subnet authorizations.

Therefore, only messages from valid and authentic ECUs will be able to pass through the firewall rules and thus be transmitted on the in-vehicle bus system.

Restricting the access level of different types of networks to other parts of the bus system can be another approach to defining firewall rules. For instance, ECUs of less important networks such as LIN or MOST should not be able to send messages into higher safety relevant and more critical bus systems such as CAN or FlexRay [11].

As explained earlier, Intrusion Detection Systems can also be employed to further enhance the communication and system security. A central gateway equipped with an IDS system will be able to inspect and analyze the exchanged information to detect security-critical anomalies. In case of detected communication misbehavior, based on its type, the IDS can take appropriate countermeasures ranging from raising simple intrusion warning messages to even deactivating the misbehaving ECU.

3.6.4 Honeypots

The vehicle's wireless communication gateway will provide a vulnerable entry point open to attackers. By having wireless access to a vehicle, an attacker will be able to launch cyber attacks, directly targeting the in-vehicle network. Since the most critical and significant operations of a vehicle are performed and controlled by the in-vehicle network, it is of great importance to secure the in-vehicle communication system from being compromised by such attacks. Learning the attacker's behavior, techniques and approaches is an effective method which helps to design and develop highly effective security solutions for in-vehicle communication systems.

Regarding this concept, a honeypot can be used for gathering attacker's information. The basic idea behind honeypots is to provide a vulnerable easy to access target for attackers by intentionally expose system weaknesses toward them and thus analyzing their behavior and techniques. According to [35], honeypots are tools for prevention and early detection of malicious attacks based on studying the attackers' malicious and unauthorized behavior within the system.

In desktop IT systems, a honeypot is usually a regular computer. A honeypot runs a special kind of software which attracts attackers by appearing as valuable and easy to access targets. Once an attacker manages to break into the system, the administrator will be able to analyze his intrusion techniques and behavior. This will help to develop specific security measures for the system and prevent further attacks in future. By some adaptations, honeypots can be implemented in the automotive domain as well, to identify potential threats against in-vehicle networks.

In the automotive domain a honeypot must be *realistic* in order to be able to attract real attackers and also *separated* from the system's main functionality in order to avoid interfering with normal vehicle operation and putting passengers into danger [35]. During its data collection phase, the car equipped with the honeypot will drive along a specific area and record all data which is sent to its gateway affecting the in-vehicle network. Later by analyzing and processing the collected data, attack behavior and scenarios can be identified. Attack commands can also be investigated using reverse engineering techniques to identify their effects on the system. This practical information will be useful for further securing the in-vehicle communication system in future design and implementations.

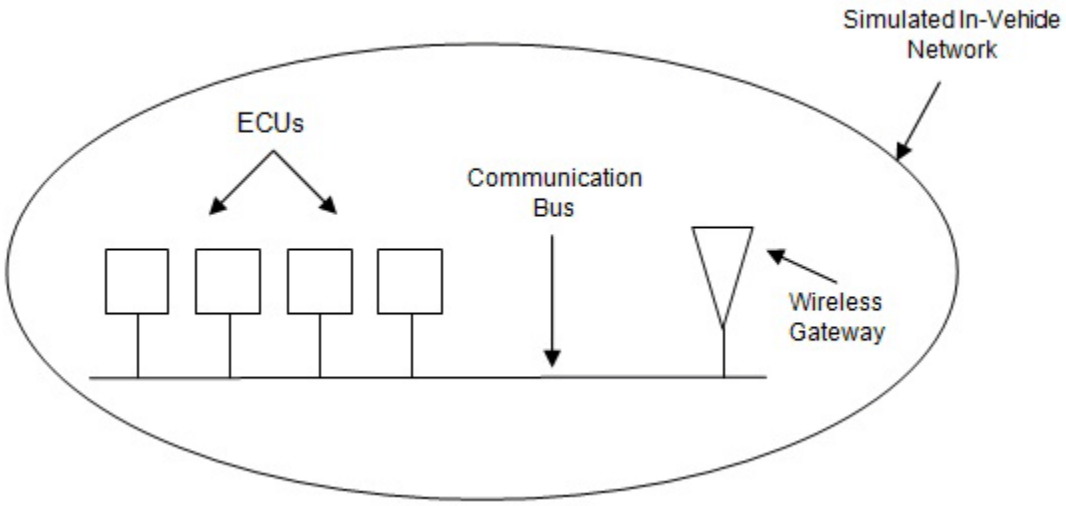

Figure 14. A Simulated In-vehicle Network as a Honeypot

The hotspot of a honeypot is the wireless gateway which provides the inter-vehicle communication and is therefore an entry interface to the in-vehicle network system. In order to look realistic, a honeypot must simulate all ECUs and their functionality exactly as a real in-vehicle network. Tools like CANoe [36] exist to build in-vehicle networks and simulate all ECUs and their functionality [35]. A simulated in-vehicle network which can be used as a honeypot is shown in figure 14.

3.6.5 FlexRay Bus Guardian

The bus guardian in FlexRay protocol is proposed to guarantee the safety and security of the communication channel and protect it against faulty conditions. Implemented on the physical layer of the FlexRay protocol, the bus guardian protects the communication channel from interference caused by any message that is not aligned with the communication schedule [37]. Being implemented on the physical layer, the bus guardian provides very fast and effective error detection and signaling.

There is a bus guardian associated with each communication controller, which independently controls schedules and data to prevent the communication controller from accessing the communication channel outside its pre-allocated slots. As another basic task, the bus guardian must ensure that messages from valid and authentic communication controllers are correctly sent to their destination.

All the aforementioned tasks are done by monitoring timing status of the bus. Once a gap in timing is detected, the bus guardian will send a message to the bus driver preventing it from sending further messages and thus protecting the bus. At same time, it also notifies the error producing node by sending an error message [41].

According to [38], there are four properties defined for the bus guardian:

- Correct Relay. If a valid and authentic communication controller sends a message, its non-faulty bus guardian relays the message.
- Validity: If a non-faulty bus guardian relays a message, then all correct communication controllers receive the message.
- Agreement: If a non-faulty communication controller receives a message, then all non-faulty communication controllers receive the message.
- Integrity: If a message is received by a non-faulty communication controller, the message must have been sent by another non-faulty communication controller.

Despite of its protection mechanisms, the bus guardian can be considered to be a security vulnerability in the FlexRay protocol. Utilizing this facility, an attacker will be able to send fake error messages to a specific controller and thus completely deactivate it. According to [34], if within one static communication cycle more than α ($\alpha >= n/3$, where n is the number of existing nodes) malicious SYNC messages are posted into a FlexRay bus; it will be possible to perform time based attacks, which will result in deactivating the whole FlexRay network.

3.6.6 Vehicular Security Architecture

One ideal approach to secure the in-vehicle communication is to implement a security module in each and every security-sensitive device within the vehicle. Despite of being effective, this approach will cause a considerable overhead with respect to cost and complexity. In order to avoid implementing a security module for each security-sensitive component, [11] proposes three different security architectures for in-vehicle communication, which are explained in detail below:

Central Security Architecture

In this approach, there is a central security module responsible for security operations of all internal and external ECUs and devices. This security module is commonly a part of the main control unit which implements most vehicular applications and needs to be strongly protected.

Therefore, a central security module will be the main communication point which implements all security-sensitive applications such as software update over the air mechanism. Additionally it

will serve as cryptographic key management unit for other devices in order to support key establishment procedures or authentication.

However, there is no correctness verification possible between the central security module and devices which don't have security functionality on their own. Therefore, only ECUs which implement some own security measures can take part in security-sensitive operations, if not; they won't be able to verify the correctness of the information they send or receive.

Implementing a central security module is simple, easily manageable, rather cheap, flexible and upgradable. On the other hand, the correctness of transmitted information cannot be verified and the central security module will become a single point of failure making the whole network highly vulnerable in case of being the target of an attack.

Distributed Security Architecture

In this architecture, all ECUs and devices take part in shaping the overall security functionality. In this solution, [11] introduces two possible scenarios for implementing such a distributed system:

- *Based on several self-protected security modules*, in which the necessary security functionality is implemented within separate and autonomous protected security modules.
- *Based on collaboration between multiple ECUs*, to provide a subset of devices capable of enabling specific security functionality.

In this distributed security architecture, the correctness of transmitted information between different devices is verifiable, there is no single point of failure which means that a compromised device will not affect the operation of the whole network and finally, due to the distributed characteristic of the system it is hard to attack since there must be several attacks launched.

On the other hand, such architecture requires a complicated cryptographic infrastructure which makes it hard to realize in practice. Implementing security functionality within each individual device will be complex and expensive, making the system less flexible and also hard to upgrade.

Semi-Central Security Architecture

This architecture is a combination of the two aforementioned architectures. In this scenario, there exist a central security module along with some individual self-secured ECUs and devices such as critical sensors and actuators. The ECUs, equipped with autonomous security functionality (which mainly includes secure authentication, communication and storage), will be able to take part in security-sensitive applications, similar to what happens in distributed security architecture explained in the previous section.

By implementing only a few required security functions, other ECUs and devices in the system will be able to benefit from the available security functionality provided by the central security module, similar to what happens in central security architecture.

Implementing a system using semi-central security architecture is practically feasible. In such a system, the correctness of transmitted information is verifiable; there is no single point of failure and the system is reasonably flexible and upgradable. Due to the individual protection mechanisms implemented in each critical ECU and also the inherent distributed characteristics, launching attacks against the system will be sufficiently hard. Bu when compared to a central security architecture, it is not that simple, flexible and easily manageable, moreover it is rather expensive and complex to implement.

4 Discussion

Vehicular networks perform critical functions and must be secured against malicious behavior. As mentioned before, unauthorized access can result in serious financial or physical damage to the vehicle or its passengers. Therefore, the vehicular network framework must be designed with great care and should meet several design challenges. Although security considerations might have different perspectives, there are general security requirements which are common in many embedded systems [27]:

- User authentication, all users must be authorized to use the network. This may also include the case where the owner tries to modify a part of the vehicle to improve functionality or performance without consulting the manufacturer.
- Availability, a vehicular network must always be ready to operate and must be robust against different logical or physical attacks otherwise there might be serious consequences concerning its passengers.
- Secure network access, all nodes must be authorized in order to be able to use the network and send and receive messages to/from other nodes in the network.
- Secure communications, when connecting the vehicular network to an external network (e.g. performing FOTA), the communication channel must be secure in order to prevent unauthorized and malicious access to the data in transfer which might damage the internal vehicular network. Without secure communication channels, attackers may inject unauthorized messages and frames in the network to extract confidential information such as detecting vehicle location or perform unwanted tasks such as modifying the downloaded software to, for example, turn on the brake lights while moving.
- Secure storage, sensitive and valuable information must be securely stored in order to be protected against unauthorized access and requests.
- Secure content refers to protection of all the digital content from cyber attacks.

As shown in the report, vehicular networks do not fulfill the mentioned security requirements and therefore, are open to several attacks. There are a number of suggested countermeasures to secure vehicular networks, both in-vehicle networks and VANETS, against cyber attacks. We are conviced that many of these protection techniques and mechanisms are mainly short-term countermeasures and they are partially effective in securing vehicular networks.

The drawback in short-term countermeasures is that attackers and malicious users will always try to discover and exploit new vulnerabilities. Especially in case of in-vehicle networks, they are open and vulnerable to many known attacks; therefore, by applying short-term countermeasures, these networks will only be temporarily protected against cyber attacks and manufacturers must proactively discover new threats and constantly update the software in their manufactured vehicles which will be both time consuming and expensive.

On the other hand, this approach will also be frustrating for owners as well since they must have their vehicles serviced and updated more frequently by taking them to authorized service shops.

Even if applying Firmware update Over the Air (FOTA), manufacturers will still have to invest a lot of money in research and development of new countermeasures.

Furthermore, not all known countermeasures will work effectively in vehicular networks since vehicular networks have limited resources and computational power compared to regular IT systems and as a result, all the existing countermeasures will not work properly in vehicular networks and they have to be tailored and modified in order to be able to work effectively.

Apart from the mentioned problems in providing short-term countermeasures, there are a number of technical and non-technical constraints in designing proper defense mechanisms in vehicular networks due to their difference from regular IT systems. Technical constraints include computing and communication resources, physical conditions as well as limitations in the input and output devices [29] and non-technical constraints mainly include particular organizational and legal constraints as well as special maintenance conditions [29].

Vehicular networks usually require real-time processing and capabilities in order to deliver specific tasks. Therefore, vehicular networks need special requirements in terms of complexity, memory size and runtime efficiency [29]. Protection mechanisms must be designed and implemented in the simplest way possible with the least possible overhead on the network. Furthermore, complex encryption/decryption algorithms as well as resource-consuming infrastructures in the communication channel may add processing delays in the ECUs which will lead to failures in delivering messages on-time.

In case of using an intrusion detection system which is counted as a short-term countermeasure [26], an important issue regarding the receiver of the generated messages must be considered. In the case of regular IT systems, the generated message from the intrusion detection system will be displayed to the network or security administrator which is an IT professional. However, in vehicular networks, when a malicious behavior is detected, the message will be shown to the driver who may not be an expert in IT systems. Also, not all the messages should be communicated to the driver since they might be distracting and cause the driver to lose his/her attention and lead to an accident. Thus, messages which are communicated to the driver also need to be altered so that they won't confuse the driver. In [20], different levels of criticality are presented. There is no need to inform the driver about every message. Only safety-critical messages should be shown to the driver so that he can make an informed decision. The vehicle network should be able to handle safety-related and non safety-related cases to some extent. Driver consultation must always be considered in vehicular IDS. An example would be automatic braking in case of a detected problem by the IDS system. If the intrusion detection system incorrectly detects a malicious activity and independently decides to stop the car in the middle of a highway, this may result in terrible consequences.

Based on all the mentioned limitations and problems, there must be a number of long-term countermeasures in securing vehicular networks against attackers and malicious users which will

be to the benefit of both manufacturers and owners. Therefore, more sophisticated protection mechanisms must be designed and implemented in order to cover the security vulnerabilities of vehicular networks. Since most of the attacks in the automotive domain originate from unauthorized users who inject invalid messages to the network, an authentication and registration mechanism seem like a promising approach in securing vehicular networks. Digital signatures can be used to authenticate all the users in the network and as a result, in the event of an attack, the source can be identified.

Implementing digital signature infrastructures and certificate authorities will be one of the non-technical constraints in securing vehicular networks. To have a thorough and secure infrastructure, a complex and expensive organizational structure must be established in order to manage vehicles' identities and authorized key distribution centers. The organization must be globally known and must be accepted by all the manufacturers throughout the world. On the other hand, the organization will also need a quite expensive IT infrastructure in order to be operational in such level.

Apart from being organizationally complex and expensive, organizing all the current and future involved parties to work with each other and developing a common standard for different parties to work together will be an issue as well. Currently there are a lot of manufacturers which produce vehicle parts and they are increasing in number every day.

Long service-periods in vehicles compared to computer systems will also be a considerable issue which will limit the manufacturers. A computer system can be easily serviced and updated through the Internet or other means which will be much cheaper compared to a vehicle. A car cannot be taken for service every month since reliability is an important issue among both vehicle manufacturers and customers. Therefore, the security infrastructure for vehicular networks must be designed so that it will need the least updates and services during a vehicle's lifecycle.

As a result, due to the mentioned attacks and constraints in securing and protecting against such cyber attacks in vehicular networks, we can conclude that most of the existing countermeasures and solutions are only partially effective in providing security for vehicular networks. From the inter-vehicle networks point of view, lack of a proper authentication mechanism will make it possible for malicious users to inject false information into the network and mislead the nearby vehicles. In addition, in-vehicle networks are also vulnerable to several attacks and ECUs in the in-vehicle networks lack serious security protection mechanisms and are not robust against attacks.

Hence, due to the existing problems and threats which will endanger the vehicle and its passengers, the need for a whole new infrastructure seems reasonable which will be to the benefit of both manufacturers and customers. By implementing a new infrastructure from scratch and by considering all possible security threats and vulnerabilities, a long-term and fully-functional

solution could be introduced which would be a remarkable improvement in vehicular networks. This suggestion might seem expensive to implement, but considering its characteristics and advantages, it will be to everyone's benefit in several ways.

First and foremost, a new architecture designed for security will be a long-term solution to vehicular networks security vulnerabilities with all the threats considered and prevented. This means that there will be no need to be concerned about introducing short-term countermeasures to overcome the security threats temporarily.

Moreover, it will reduce the cost of research and development dramatically. By having a thorough and secure infrastructure where there will be no need for constant introduction of new security countermeasures, R&D costs will ultimately decrease. Therefore, research can focus on improving the infrastructure in terms of cost reduction, bug detection and performance enhancement which will result in an ultimate solution to securing vehicular networks.

Vis-a-vis the mentioned vulnerabilities, attacks, countermeasures and solutions in the report, once again we would like to emphasize that the solution we strongly propose is the need for a new infrastructure to be designed and developed for both Vehicular Ad hoc Networks and in-vehicle networks. We are of the utter conviction that current infrastructure for vehicular networks will never be fully protected against cyber attacks and new vulnerabilities will always be identified in the field. The new infrastructure might be time-consuming and might seem expensive to implement, but once designed and developed, it will solve the security problems of vehicular networks and make problems appearing in the future possible to manage at the time needed.

5 Conclusion

In this thesis work, different vulnerabilities and attacks as well as a number of countermeasures in the vehicular networks domain are discussed. We argue that implementing a whole new infrastructure which has fully considered all security issues known today will be the best way to overcome the mentioned security vulnerabilities in vehicular networks. Although implementing a new infrastructure will seem like the ultimate solution to overcome security vulnerabilities in vehicular networks, manufacturers will try to resist developing such infrastructure due to a number of issues. It will be costly to implement and in addition, compatibility of the new infrastructure with current existing technologies must be considered. Therefore, we believe a compromise between the ultimate solution and current situation can solve security problems to some extent.

As an alternative solution, we would like to suggest securing critical ECUs, i.e. powertrain ECUs, against cyber attacks. By providing full protection in powertrain ECUs, attackers won't be able to eavesdrop or inject messages destined for such ECUs and as a result, critical components can be protected. We are conviced that fully securing gateway ECUs which are connected to powertrain ECUs will be the best possible scenario. By doing so, powertrain gateway ECUs will monitor bus traffic and drop any malicious or malformed frame.

To implement such solution, new gateway ECUs with more computational power and resources must be developed and replaced by current gateway ECUs. By doing so, a number of security protection mechanisms and countermeasures which couldn't be used before, can be applied to these ECUs and will ultimately guarantee the security of critical, e.g. powertrain, ECUs.

Although this solution will not cover all security issues of vehicular networks, it will be to the benefit of manufacturers and consumers in several ways. An advantage of this alternative is its compatibility with current technologies since it is basically implemented on the top of existing infrastructure. Therefore, no fundamental changes will be necessary and all previously manufactured vehicles can be equipped with the new ECUs and new security policies eventually.

Securing powertrain ECUs will also be much less expensive compared to implementing a new infrastructure from scratch. Such a new infrastructure will require extensive research and a lot of resources in order to be developed and implemented successfully. As a result, we believe that manufacturers will not be likely to go through such an expensive option.

As our final word, once again we would like to emphasize the need for security countermeasures in vehicular networks. Unsecure vehicular networks will have terrible consequences which will be to the detriment of vehicles, passengers and manufacturers as well. Hence, due to recent improvements in connecting vehicles to external networks, proper security mechanisms must be developed in parallel to reduce the risk of malicious and unauthorized behavior in the vehicular network domain.

6 References

[1] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, “Securing Vehicular Communications - Assumptions, Requirements, and Principles,” in Workshop on Embedded Security in Cars (ESCAR) 2006, 2006. [Online]. Available: http://icapeople.epfl.ch/panos/escar-secure-vehicular-communications-fundamentals.pdf

[2] P. Golle, D. Greene and J. Staddon, “Detecting and correcting malicious data in VANETs.” in Proceedings of the first ACM workshop on Vehicular ad hoc networks, (2004), ACM Press, pp 29–36.

[3] 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), 2005. [Online]. Available: http://lcawww.epfl.ch/Publications/raya/RayaH05C.pdf

[4] B. Parno and A. Perrig, ”Challenges in Securing Vehicular Networks,” in Proceedings of the Workshop on Hot Topics in Networks (HotNets-IV), 2005.

[5] F. Dotzer, F. Kohlmayer, T. Kosch, M. Strassberger, “Secure communication for intersection assistance.” In Proceedings of the 2nd International Workshop on Intelligent Transportation, Hamburg, Germany (2005)

[6] R. Panayappan, J. Trivedi, A. Studer, and A. Perrig, “VANET-based approach for parking space availability,” in Proc. of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks (VANET 2007), Montreal, Quebec, Canada, pp. 75-76, Sept. 2007.

[7] T. Leinmüller, E. Schoch, C. Maihöfer, “Security requirements and solution concepts in vehicular ad hoc networks,” in Proceedings of the 4th Annual Conference on Wireless on Demand Network Systems and Services, 2007, pp. 84–91

[8] H. Mustafa, Y. Zhang, “Vehicular Networks, Techniques, Standards and Applications,” Auerbach publications, 2009

[9] K. O’Neill and J. Y. Halpern, ”Anonymity and information hiding in multiagent systems,” Proceedings of the 16th IEEE Computer Security Foundations Workshop, 2003.

[10] K., Lemke, “Embedded security: Physical protection against tampering attacks.” In: Lemke, C.P.K., Wolf, M. (eds.) Embedded Security in Cars, ch. 2, pp. 207–217. Springer, Heidelberg (2006)

[11] Marko Wolf 2009, Security Engineering for Vehicular IT Systems, Vieweg+Teubner, Bochum, Germany

[12] M. Raya and J.-P. Hubaux, “Security Aspects of Inter-Vehicle Communications.” In Swiss Transport Research Conference(STRC) 2005, March 2005.

[13] Lo, N.-W., Tsai, H.-C.: Illusion Attack on VANET Applications - A Message Plausibility Problem. In: IEEE Globecom Workshops, pp. 1–8 (2007)

[14] M. Raya and J. P. Hubaux, “Securing vehicular ad hoc networks”, Journal of Computer Security, Vol. 15, No. 1, pp. 38-68, 2007

[15] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, “Secure vehicular communications: Design and architecture,” IEEE Communications Magazine, vol. 46, no. 11, pp. 100–109, November 2008.

[16] Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE Std. 1609.2, 2006.

[17] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho and X. Shen, “Security in vehicular ad hoc networks”, IEEE Communications Magazine, to appear

[18] A. Rao, A. Sangwan, A. Kherani, A. Varghese, B. Bellur, and R. Shorey, “Secure V2V Communication With Certificate Revocations,” 2007 Mobile Networking for Vehicular Environments, pp. 127–132, 2007

[19] Dennis K. Nilsson, Phu Phung, and Ulf E. Larson.Vehicle ECU Classification Based on safety-Security Characteristics. In Proceedings of the 13th International Conference on Road Transport and Information Control (RTIC), 2008.

[20] Frank Kargl, Zhendong Ma, and Elmar Schoch. Security engineering for vanets. In 4th Workshop on Embedded Security in Cars, escar 2006, Berlin, Germany, November 2006.

[21] M. Wolf, A. Weimerskirch, and C. Paar, “Security in Automotive Bus Systems,” in Workshop on Embedded IT-Security in Cars, Bochum, Germany, November 2004.

[22] D. K. Nilsson, U. E. Larson, F. Picasso, and E. Jonsson, A First Simulation of Attacks in the Automotive Network Communications Protocol FlexRay, in Proceedings of the First International Workshop on Computational Intelligence in Security for Information Systems (CISIS). Springer, 2008, pp. 84.91.

[23] Karl H. Johansson, Martin Törngren, and Lars Nielsen, Vehicle applications of controller area network, in Handbook of Networked and Embedded Control Systems, William S. Levine Dmiitris Hristu-Varsakelis, and, ed., Birkhauser, 2005.

[24] Dennis K. Nilsson and Ulf E. Larson A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure. Journal of Networks (JNW), Special Issue on Security of Wireless Communication Systems, June, 2009. Academy Publisher.

[25] R. Miucic and S. M. Mahmud, .An In-Vehicle Distributed Technique for Remote Programming of Vehicles' Embedded Software,. Electrical and Computer Engineering Department, Wayne State University, Detroit, MI 48202 USA, Tech. Rep., 2005.

[26] T. Hoppe, S. Kiltz, and J. Dittmann. Security threats to automotive CAN networks practical examples and selected short-term countermeasures. In Proc. of the Int'l Conf. on Computer Safety, Reliability and Security (SAFECOMP), pages 234–248, 2008.

[27] Srivaths Ravi, Anand Raghunathan, Paul Kocher, Sunil Hattangady, "Security in embedded systems: Design challenges", In proceedings of ACM Transactions on Embedded Computing Systems (TECS), August 2004, pp 461-491

[28] Nilsson, D.K., Larson, U.E.: Simulated Attacks on CAN Buses: Vehicle virus. In: Proceedings of the Fifth IASTED Asian Conference on Communication Systems and Networks (ASIACSN) (2008)

[29] Wolf, M., Weimerskirch, A., Wollinger, T.: State of the Art: Embedding Security in Vehicles. EURASIP Journal on Embedded Systems 2007, Article ID 74706, 16 (2007)

[30] Manfred Broy. Challenges in Automotive Software Engineering. In *ICSE '06: Proceedings of the 28th International Conference on software Engineering*, pages 32–42. ACM Press, 2006.

[31] Paar, Christoph: Embedded IT- Security in Automotive Application – An Emerging Area. In Embedded Security in cars. Springer Verlag. ISBN 978-539-28374-3. 2006

[32] Huaqun Guo, Lek Heng Ngoh, Yongdong Wu, Lian Hwa Liow, Choon Hwee Kwek, Feng Tao, and Jun Jie Ang, "Embedded Info- Security Solutions for Vehicular Networks," in Proc. *Third International Conference on Communications and Networking in China (CHINACOM'08)*, Hangzhou, China, August 25-27, 2008.

[33] Tobias Hoppe, "Applying Intrusion Detection to Automotive IT- Early Insights and Selected Short Term Countermeasures", 2009

[34] M. Wolf, A. Weimerskirch, and C. Paar, "Secure In-Vehicle Communication," in Embedded Security in Cars, K. Lemke, C. Paar, and M. Wolf, Eds. Springer, 2006, pp. 95–109.

[35] V. Verendel, D. K. Nilsson, U. E. Larson, and E. Jonsson, .An Approach to using Honeypots in In-Vehicle Networks,. in *Proceedings of the IEEE 68th Vehicular Technology Conference (VTC2008-Fall)*, 2008.

[36] Vector Informatik, "CANoe and DENoe 6.1," http://www.vectorworldwide. com/vi canoe en.html, 2007.

[37] G. Sung, C. Juan, C. Wang, “Bus Guardian Design for automobile networking ecu nodes compliant with FlexRay standards,” in Proceedings of IEEE International Symposium on Consumer Electronics, pp. 1-4, Apr. 2008.

[38] Bo Zhang. On the Formal Verification of the FlexRay Communication Protocol. Automatic Verification of Critical Systems (AVoCS’06), pages 184 –189, 2006.

[39] http://www.fujitsu.com/global/services/microelectronics/technical/flexray/index_p10.html, accessed April 2010.