# A Framework for Assessing the Security of the Connected Car Infrastructure

Pierre Kleberger*, Asrin Javaheri*†, Tomas Olovsson*, and Erland Jonsson*
*Department of Computer Science and Engineering
Chalmers University of Technology
SE–412 96 Gothenburg, Sweden
Email: {pierre.kleberger, asrin.javaheri, tomas.olovsson, erland.jonsson}@chalmers.se
†Volvo Car Corporation
SE–405 31 Gothenburg, Sweden

***Abstract*—In this paper, a framework for assessing the security of the connected car infrastructure is presented. The framework includes a model of the infrastructure and a security assessment tree. The model consists of a managed infrastructure and the vehicle communication. The managed infrastructure is further divided into five parts; automotive company applications' centre, third party applications' centre, trusted network, untrusted network, and the Internet backbone. The model clarifies the different communication possibilities between the managed infrastructure and the vehicle. Furthermore, the assessment tree defines four categories that need to be addressed in securing vehicular services; the actors, Vehicle–to–X communication technologies, network paths, and the dependability and security attributes. Moreover, we demonstrate the benefit of the framework by means of two scenarios. In this way, the communication in these scenarios are mapped to the model, which makes it possible to analyse the security issues for the scenarios according to the assessment tree. The intention with such an analysis is to identify possible weaknesses of services in the connected car.**

***Keywords*-security assessment; vehicle service; connected car; infrastructure.**

## I. Introduction

In the world of connectivity, almost all applications and systems today are communicating and using the Internet. So far, vehicles have been an exception. The demand for new services are quickly changing this field which makes the vehicle a connected car [1]. However, these new services have to be properly secured for their new communication infrastructure. In this paper, we present a framework for assessing the security of services delivered by the connected car infrastructure.

The connected car is a vehicle equipped with a wireless network gateway connecting the in–vehicle network to an external network. Today, the in–vehicle network consists of 50–100 embedded computers called electronic control units (ECUs), a number which has rapidly been increasing over the last years. With the introduction of wireless access to the vehicle, these ECUs will be exposed to external traffic and the need of securing the vehicle and its communication becomes crucial [2, 3]; it is reasonable to believe that many of the security related problems present on the Internet will be introduced into the vehicle domain.

Protocols developed for traditional vehicular services, such as vehicle diagnostics [4] and software download [5] where a wired connection is used to access the vehicle, as well as new services in development, now have to be adapted for secure remote usage. Furthermore, by introducing a wireless gateway to the vehicle, enabling the vehicle to communicate with mobile devices and other vehicles, the system becomes even more complex. Hence, a model to clarify the communication with the vehicle for conducting security assessment on its services is essential.

The framework presented in this paper consists of a model for the infrastructure of the connected car and a security assessment tree. It will help us understand and evaluate how to implement and secure protocols and applications in different vehicle settings. The connected car will contain a large number of services, communication technologies, and network types, which makes the assessment of security far from trivial [6–8]. The proposed model together with the security assessment tree makes it possible to understand the weaknesses of the system and the existence of threats both when designing new services and when using current ones.

The paper is organized in the following way. After giving an overview of related work in Section II, we present a background to the problem in Section III. In Section IV, we describe in detail the proposed model of the infrastructure, which is further extended with the security assessment in Section V. In Section VI, the security assessment is applied to two services. We discuss the proposed framework and possible future work in Section VII. Finally, Section VIII concludes the paper.

## II. Related Work

Although there is a lot of research going on in vehicular communication (VC) systems [6], there is very little research found referring to models of the connected car and how to assess the security of emerging vehicle services, i.e., remote diagnostics, remote software download, and other Internet services brought into future vehicles.

Nilsson et al. [9] present a model of the connected car. The model is divided into three domains; the *portal*, the *vehicle*, and the *communication link* connecting the vehicle

 ISBN: 978-1-61208-166-3 

to the portal. A risk assessment is conducted for each of the domains and protective security mechanisms are discussed for the identified risks. However, in their model, details of the networks between the portal and the vehicle are not specified, and the possibility of other vehicles and mobile devices to connect to the vehicle is not addressed.

The Car 2 Car Communication Consortium (C2C–CC) describes a reference architecture which is divided into three domains; the *in–vehicle*, the *ad hoc*, and the *infrastructure* [10]. The in–vehicle domain is represented by the vehicle, its applications, and mobile devices directly associated to the vehicle. The ad hoc domain is represented by the vehicles and the road–side units (RSUs), where the RSU further can be connected to the infrastructure domain. In their architecture, the access network, the Internet, and possible nodes connected to the Internet are shown as part of the infrastructure domain, but are not further considered. These parts were out of their scope.

An architecture for providing a continuous connection to the vehicle is presented by the CALM Forum [11]. The aim is to make the best possible use out of available external communication media in the vehicle. A nice overview of the network is shown, but the focus is not in securing the communication infrastructure.

Koscher et al. [2] recently showed on the lack of security in the in–vehicle network. By using techniques such as packet sniffing, packet fuzzing, and reverse-engineering, a number of possible attacks toward the in–vehicle network was performed. The focus of their work is on the security of the vehicle. Thus, the communication link with the vehicle is not addressed.

In [3], Brooks et al. discuss a set of automotive applications and they propose and use an adapted version of the CERT Taxonomy for analysing the security of these applications. Among the applications analysed are business related services, which integrates the vehicle into the automotive company, i.e., remote software download, remote diagnostics, and other applications related to the comfort of the vehicle.

Research in a security architecture for VC systems have been performed within the SeVeCOM project [12]. In [13], Papadimitratos et al. present necessary security requirements to provide the services of secure beaconing, secure neighbour discovering, and secure geocasting in VC systems. Certificates are used for securing the communication between vehicles and pseudonyms for addressing the introduced privacy problem of using certificates; the certificate gives the vehicle a unique identity, which makes it possible to trace the vehicle and its driver. In [14], Kargl et al. present implementation details of the security architecture. Furthermore, the integration of mobile devices and different communication technologies into the VC system are briefly discussed.

Two more research project that currently are running are the EVITA project [15] and the OVERSEE project [16]. The aim of the EVITA project is to provide a security architecture for the in–vehicle network and to support secure Vehicle–to–X (V2X) communication. The aim of the OVERSEE project is to develop an open and secure platform for running applications, with the possibility for internal and external communication, in the vehicle.

However, we are still missing a structured approach in assessing the security of services to the connected car, i.e., services from the automotive company or other third party application providers. Thus, a model of the infrastructure for assessing the security of the connected car is needed.

## III. Background

As more and more services are introduced into the vehicle, the complexity of the vehicle is increased correspondingly. Therefore, the work with securing the connected car requires a holistic understanding of the system. In the lack of a model describing the infrastructure, the development of a unified security solution is far from trivial. This may lead to that different security solutions, possibly incompatible with each other, are chosen when applications are implemented in the connected car. Therefore, for a model to be useful for further security analysis, it must be possible to map almost all possible scenarios into it; which actors need to be considered, and which V2X communication technologies and network paths are available. However, a model for mapping services and their corresponding communication protocols, to be used for security assessment, has not been found.

The model proposed in [9] is a simple model which only describes the infrastructure of the connected car and leaves out details about communication links, network entities, and possible communication technologies. The model presented here is an extension of that model and takes into account the different communication technologies, various remote vehicular services, and possible threats and security risks which may exist.

We believe that the use of a framework can help in relaxing some requirements in different situations, e.g., the need of protecting confidentiality in the repair shop when using wireless LAN (WLAN), or the integrity of the diagnostics data while connecting through the Internet. Considering the first example, the same level of security as for a wired connection could be reached.

## IV. A Model of the Infrastructure

In this section, we present a model of the infrastructure of the connected car. This model is shown in Figure 1. We divide the infrastructure into two domains, the managed infrastructure and the vehicle communication. The managed infrastructure is further divided into five regions, automotive company applications' centre, third party applications' centre, trusted network, untrusted network, and the Internet backbone. The vehicle communication describes the possible means of communication with the vehicle. These communication means are classified in two categories, bi–directional and uni–directional.

### A. Managed Infrastructure

The five regions of the managed infrastructure are further described below.

 ISBN: 978-1-61208-166-3

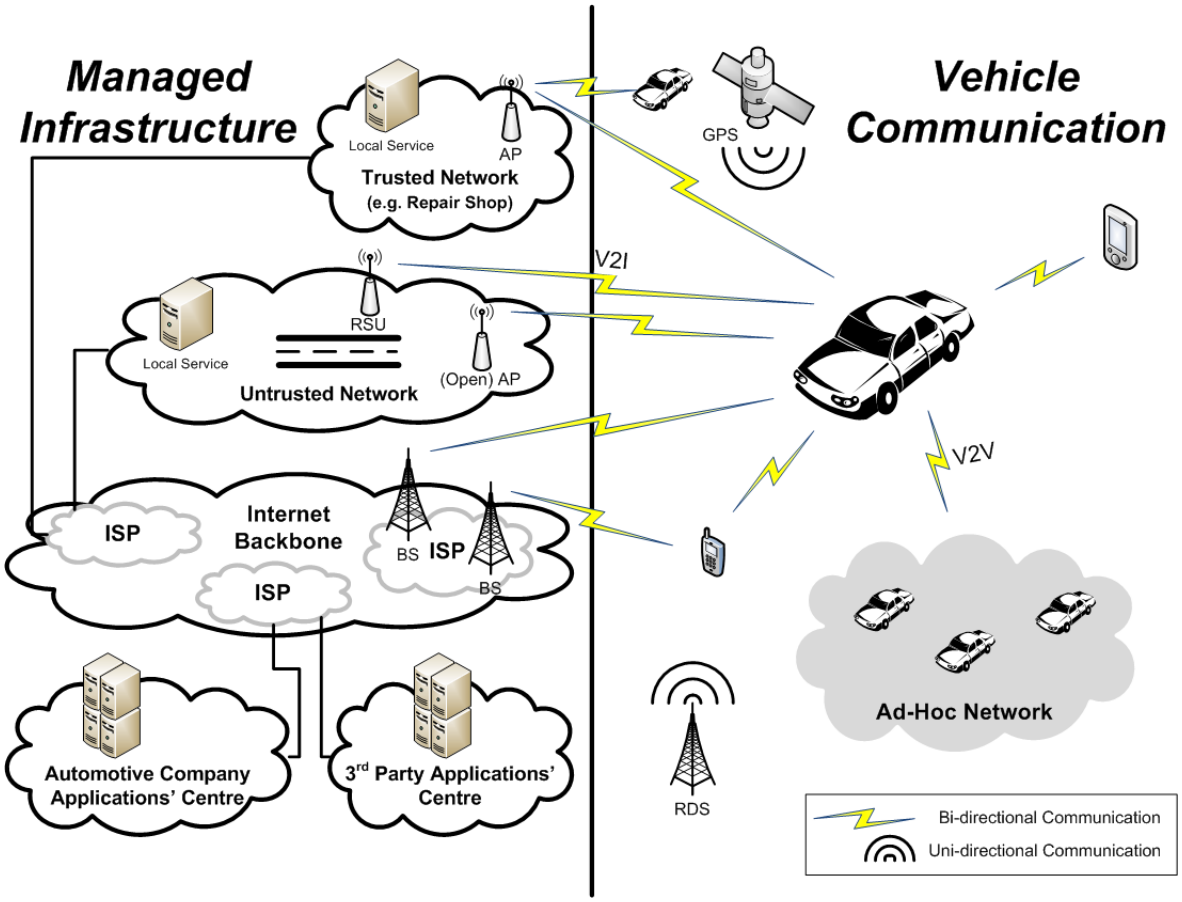


Fig. 1. Model of the connected car infrastructure

*1) Automotive Company Applications' Centre:* In the literature, the automotive company applications' centre have had different names. In [9], it is called *portal*. In [4], the remote diagnostics is performed from a *remote service centre*. To summarise, it consists of a set of servers providing services to their vehicles. It holds necessary information about the vehicle, such as information from previous services (e.g., diagnostics data), configuration data, cryptographic keys, as well as new software available for the ECUs.

*2) Third Party Applications' Centre:* Apart from services provided by the automotive company, third party services can be provided to the vehicle. We could imagine that large "application stores" for vehicles will be available in the future. These applications can provide any kind of service to the vehicle.

*3) Trusted Network:* Some networks can be considered to be trusted by the applications' centres and the vehicle. For example, a repair shop may be considered to be a trusted network by the automotive company and the vehicle. In delivering a service to this network, it may well be that some requirements in an implementation can be relaxed. Furthermore, other local services can be available in these networks for running the local infrastructure and providing service to the vehicle.

*4) Untrusted Network:* All networks, except for the trusted networks, are considered to be untrusted. In these networks, the services provided to the vehicle have to be adapted to the hostile environment of the Internet. In the same way as for the trusted networks, other local services may also be provided in these networks.

*5) Internet Backbone:* The Internet backbone, with its Internet Service Providers (ISPs), is the core network for connecting the other four regions together. A backbone network is usually well protected and operated by network specialists in a Network Operation Centre (NOC). Therefore, when network traffic has reached the Internet backbone, we assume it is very unlikely that the data will be intentionally modified.

### *B. Vehicle Communication*

The vehicle communication domain includes two possible types of communication means, bi–directional and uni–directional. They are further described below.

*1) Bi–directional Communication:* The bi–directional communication mean includes the possible communication between:

(1) the vehicle and the managed infrastructure,
(2) the vehicle and mobile devices, and
(3) the vehicle and other vehicles.

 ISBN: 978-1-61208-166-3 

We will now go through possible communications within these three groups:

- *vehicle to wireless access point (AP)*. The vehicle can establish a connection to a wireless AP in the managed infrastructure. All open APs (hotspots) are considered to be part of the untrusted network. Furthermore, a protected AP, where the vehicle needs authentication keys, can be available in both the trusted network and the untrusted network. An example of a wireless AP in an untrusted network is one provided by subscription from a telephone network provider; these wireless APs can be considered to be shared with other unknown users in the same way as for open APs.
- *vehicle to RSU*. The RSUs can be used for establishing a connection from the vehicle to the managed infrastructure.
- *vehicle to cellular base stations*. A mobile data network, e.g., 3G, can be used for establishing a connection from the vehicle to the managed infrastructure. In this case, the vehicle connects to a cellular base station in the Internet backbone. This connection requires a subscription to a mobile data network service at a telephone network provider.
- *vehicle to mobile devices*. Mobile devices can be connected to the vehicle. For example, a connection can be established to a mobile phone, a laptop, or a personal digital assistant (PDA). Furthermore, the vehicle can also act as a gateway for the mobile device, so that the mobile device can reach the same network as the vehicle.
- *vehicle to cellular base station via mobile device*. If the vehicle lacks the possibility to connect directly to a cellular base station, another mobile device with a connection to the cellular base station can be used as a gateway. One example is to use the driver's mobile phone. By using the mobile phone, a connection to the managed infrastructure can be created.
- *vehicle to other vehicles*. Finally, the vehicle can connect to other vehicles and create a vehicle ad–hoc network (VANET). This Vehicle–to–Vehicle (V2V) communication will be critical in future traffic- and safety-related services.

It should be noted that the description of the vehicle communication above is based on just one vehicle; any connected car will have the same communication surroundings. This means that the vehicle may possibly reach the managed infrastructure, via other vehicles or other mobile devices acting as gateways.

*2) Uni–directional Communication:* Broadcast devices that only sends signals to the vehicles are classified as uni–directional communication. Two uni–directional communication means have been identified:

- *the global positioning system (GPS)*. The GPS system can be used by services in the vehicle.
- *the radio data system (RDS)*.

## V. Using the Model to Assess the Security of Vehicle Services

From the model of the infrastructure of the connected car, there are different aspects that can be discussed regarding the V2V and the Vehicle–to–Infrastructure (V2I) communication. One of them is the security of the services delivered to the vehicle. Figure 2 presents a brief taxonomy of the security of these services. Four categories are described; the *actors*, the *V2X communication technologies*, *network paths*, and the *dependability and security attributes*. A description of them follows bellow.

- *actors*. Six different actors that can be involved in a service have been identified. Common for them all are that they have interests in how the service is being designed and delivered; the automotive company and the application provider can state requirements, the car owner and the user can have concerns on how the data from a service is processed, the authorities can issue legal requirements, and an attacker can try to manipulate the service in an unwanted way.
- *V2X communication technologies*. A number of communication technologies are available for connecting the vehicle to other devices. Examples of these are listed in this branch. An extended list, including classifications of the communication technologies, can be found in [17].
- *network paths*. The service may be delivered to the vehicle using one of several network paths. The model describes four possible network paths that the service can be delivered through (see Figure 1); the trusted network, the untrusted network, the Internet backbone, and an ad-hoc network.
- *dependability and security attributes*. To deliver the service in a secure and safe manner, the six attributes for dependability and security [18] need to be considered. In this paper, we are mainly focusing on the security attributes.

From these four categories, an analysis can be made to further clarify how a service will work in the infrastructure and also highlight the dependability and security attributes that need to be addressed in providing such a service.

## VI. Conducting Security Assessment on two Services

We will now show the benefits of using the framework for assessing the security of the services delivered to the connected car. We will describe two scenarios to illustrate the approach; a remote diagnostics service and a map service with GPS positioning.

### A. Remote Diagnostics

Remote vehicle diagnostics is one of the emerging vehicle services in the connected car [4, 5]. Thus, work is being performed by the International Standard Organisation (ISO) in defining a standard protocol for performing Diagnostics over IP [19–21].

 ISBN: 978-1-61208-166-3 

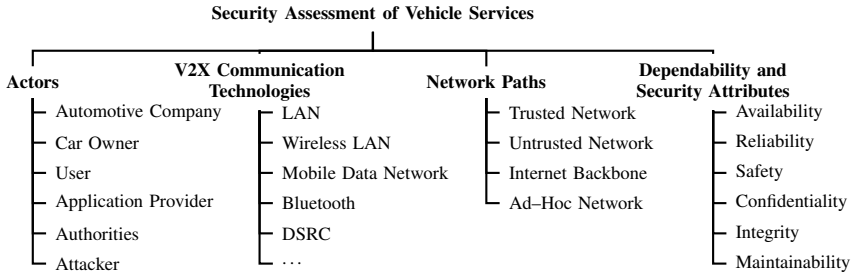


Fig. 2. Security Assessment Tree

In analysing a remote diagnostics service, the first step will be to clarify how the diagnostics will be performed. In the model of the infrastructure (see Figure 1), we find two cases:

(1) *remote diagnostics performed by repair shop*. The vehicle connects to the trusted network at the repair shop through an AP. The diagnostics session is provided as a local service at the repair shop.
(2) *remote diagnostics performed by the automotive company applications' centre*. The vehicle connects to a cellular base station in the Internet backbone. The diagnostics session is performed by the automotive company applications' centre through the Internet backbone and the cellular base station.

To further clarify these cases, the security assessment tree in Figure 2 is used. For case (1), the following question can be derived:

> What is the *automotive company's* concern with respect to the *confidentiality* of the submitted diagnostics data when the vehicle is connected to the repair shop in the *trusted network* using a *wireless LAN*?

This question reflects the following set of aspects from the tree:

> {*automotive company, wireless LAN, trusted network, confidentiality*}

We note that although the network at the repair shop is considered a trusted network, its AP can be shared with other vehicles. Therefore, if the confidentiality requirements of the wireless link is fulfilled, the same level of security might be acquired as if a cable was used.

For case (2), another question can be derived:

> What is the *automotive company's* concern with respect to the *integrity* of the diagnostics data transmitted between the vehicle and the automotive company applications' centre when the vehicle is connected to the *Internet backbone* using a *mobile data network*?

This question reflects the following set of aspects from the tree:

> {*automotive company, mobile data network, Internet backbone, integrity*}

In this case, we see that by fulfilling the integrity requirement, modified diagnostic codes sent by an attacker will not pose any security risk to the vehicle.

### *B. Map with GPS Positioning*

A possible service in a vehicle is a map provided by an Internet service (e.g., Google Maps) with positioning using the vehicle's built–in GPS. A further add–on to this service may be to get local traffic conditions from the road authorities. This service leads to three sources of information that need to be provided to the vehicle, the map, the GPS-coordinates, and the current traffic condition in the area. We will now analyse this service with respect to the model of the infrastructure and the security assessment tree.

The first step will be to clarify how the map is provided to the vehicle. From the model in Figure 1, four suitable links between the vehicle and the managed infrastructure can be found;

(1) vehicle to RSU,
(2) vehicle to AP,
(3) vehicle to cellular base station, and
(4) vehicle to cellular base station via a mobile device.

These four links are located in the untrusted network and the Internet backbone, which are further connected to the third party applications' centre providing the map to the vehicle. Furthermore, for the GPS-positioning, the data is retrieved from the GPS-satellites. A security analysis of the retrieved data is not considered here. However, for the current traffic condition, the service needs to be mapped into the model of the infrastructure to clarify its communication. The same four links as above can connect the vehicle to the managed infrastructure. The current traffic condition is provided by the two networks, untrusted network and the Internet backbone, which are further connected to the road authorities (in the third party applications' centre).

To further clarify the security issues of delivering the map to the vehicle, the second step is to inspect the security assessment tree in Figure 2. For the map service, several questions can be derived with respect to the different possibilities to deliver the map to the vehicle. To illustrate the concept, only one question will be highlighted;

> What is the *user's* concern with respect to the *confidentiality* of the data submitted (i.e., GPS-coordinates) to the map service when communicat-

 ISBN: 978-1-61208-166-3 

ing with the server over the *mobile data network* through the *Internet backbone*?

This question reflects the following set of aspects from the tree:

{*user, mobile data network, Internet backbone, confidentiality*}

The question above is relevant if the user does not want any other party, except for the server, to be able to identify the user's current location by eavesdropping on the transmitted data.

For the traffic conditions, the following question can be derived:

What is the *user's* concern with respect to the *integrity* of the data distributed by the road authorities, when the data passes the *Internet backbone* and the *untrusted network*, and the vehicle is connected to the RSU in the *untrusted network* over a *Dedicated Short–Range Communication (DSRC)*-link?

This question reflects the following set of aspects from the tree:

{*user, DSRC, (untrusted network, Internet backbone), integrity*}

In this case, the user is not concerned about whether any other party can eavesdrop on the traffic condition information, but rather that the *correct* information is delivered to the vehicle.

## VII. Discussion and Future Work

We believe that in analysing some scenarios and solutions with respect to security, it might be that some of the security requirements could be relaxed. One such example is: if the confidentiality of the communication link between the vehicle and the AP in the trusted network can be properly established; will security of the link then be comparable with that of a wired cable? If so, a service can, as a first step, easily be introduced also for this wireless link without any modification. This will reduce the time for adapting already established services, and save cost for developing new ones. However, for other scenarios the service might need to be modified.

The security assessment tree helps us state questions regarding the security of the services delivered to the vehicle. In the future, we would like to investigate how to extended this security assessment tree to cover more aspects, e.g., security mechanisms. A complete security analysis of a vehicle service is also an important next step.

## VIII. Conclusion

There is a clear trend of offering remote services, third party applications, and critical information exchange between various entities in the connected car. Even though there has been a lot of research conducted in the field of securing VC systems, not much work has been done in assessing the security of these services for the connected car. We believe that, by using our proposed framework, scenarios such as remote vehicle diagnostics, remote software download, multimedia streaming, Internet browsing and the exchange of information between vehicles and the infrastructure can be discussed and assessed from a security viewpoint.

## References


[1] P. Papadimitratos, A. d. La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, "Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation," *IEEE Communications Magazine*, vol. 47, no. 11, pp. 84–95, 2009.

[2] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," in *Proc. of the 31st IEEE Symposium on Security and Privacy*, 2010, pp. 447–462.

[3] R. Brooks, S. Sander, J. Deng, and J. Taiber, "Automobile Security Concerns," *Vehicular Technology Magazine, IEEE*, vol. 4, no. 2, pp. 52–64, Jun. 2009.

[4] S. You, M. Krage, and L. Jalics, "Overview of Remote Diagnosis and Maintenance for Automotive Systems," in *2005 SAE World Congress*, Detroit, MI, USA, 2005.

[5] M. Shavit, A. Gryc, and R. Miucic, "Firmware Update Over The Air (FOTA) for Automotive Industry," in *14th Asia Pacific Automotive Engineering Conference*. Hollywood, CA, USA: SAE, 2007.

[6] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions," *IEEE Communications Surveys & Tutorials*, no. 99, pp. 1–33, 2011.

[7] T. L. Willke, P. Tientrakool, and N. F. Maxemchuk, "A Survey of Inter-Vehicle Communication Protocols and Their Applications," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 2, pp. 3–20, 2009.

[8] M. L. Sichitiu and M. Kihl, "Inter-Vehicle Communication Systems: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 2, pp. 88–105, 2008.

[9] D. K. Nilsson, U. E. Larson, and E. Jonsson, "Creating a Secure Infrastructure for Wireless Diagnostics and Software Updates in Vehicles," in *Proc. of the 27th International Conference on Computer Safety, Reliability, and Security (SAFECOMP '08)*. Newcastle upon Tyne, UK: Springer-Verlag, 2008, pp. 207–220.

[10] *C2C-CC Manifesto*, v1.1 ed., CAR 2 CAR Communication Consortium, Aug. 2007. [Online]. Available: http://www.car-to-car.org/. 2011-08-06.

[11] *The CALM Handbook*, v3 (060326) ed., The CALM Forum Ltd., 1 Beverly Hall, Halifax, West Yorkshire, HX2 6HS, UK, Mar. 2006. [Online]. Available: http://www.isotc204wg16.org/pubdocs/The CALM Handbookv6-070301.pdf. 2011-08-06.

[12] "Secure Vehicle Communication (SeVeCOM)." [Online]. Available: http://www.sevecom.org/. 2011-08-06.

[13] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communication Systems: Design and Architecture," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[14] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 110–118, Nov. 2008.

[15] "E-safety Vehicle Intrusion Protected Applications (EVITA)." [Online]. Available: http://www.evita-project.org/. 2011-08-06.

[16] "Open Vehicular Secure Platform." [Online]. Available: https://www.oversee-project.com/. 2011-08-06.

[17] K. Dar, M. Bakhouya, J. Gaber, M. Wack, and P. Lorenz, "Wireless Communication Technologies for ITS Applications," *IEEE Communications Magazine*, vol. 48, no. 5, pp. 156–162, 2010.

[18] A. Avižienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, 2004.

[19] *ISO/DIS 13400-1: Road vehicles – Diagnostic communication over Internet Protocol (DoIP) – Part 1: General information and use case definition*, ISO Std.

[20] *ISO/DIS 13400-2: Road vehicles – Diagnostic communication over Internet Protocol (DoIP) – Part 2: Network and transport layer requirements and services*, ISO Std.

[21] *ISO/DIS 13400-3: Road vehicles – Diagnostic communication over Internet Protocol (DoIP) – Part 3: IEEE802.3 based wired vehicle interface*, ISO Std.


 ISBN: 978-1-61208-166-3 