Alarming! Security Aspects of the Wireless Vehicle: Review

Sabarathinam Chockalingam
1, Kailash Nagar, First Street, Near Police Colony, Karaikudi – 630002, India.
Sabarathinam14@gmail.com

Harjinder Singh Lallie
University of Warwick, WMG, Coventry, United Kingdom, CV4 7AL.
H.S.Lallie@warwick.ac.uk

ABSTRACT

The auto-mobile industry has grown to become an integral part of our day – to – day life. The introduction of wireless vehicles definitely have to pass through the analysis of potential security threats and vulnerabilities, and robust security architecture should be designed that are able to cope with these threats and vulnerabilities. In this work, we have identified various categories of research in 'Cyber Security of a wireless vehicle' and mainly focused on 'In – Vehicle Network' to identify various potential security threats and vulnerabilities as well as the suitable security solutions. In addition to providing a survey of related academic efforts, we have also outlined several key issues and open research questions.

KEYWORDS

In-Vehicle Network, Security, Threats, Vulnerabilities, Wireless Vehicle.

1 INTRODUCTION

Vehicle manufacturers started incorporating a lot of technological advancements which helps to replace mechanical solutions for vehicle control by software and electronic solutions ([1] and [2]). Nowadays people started demanding wireless internet access even in auto-mobile. They prefer to access internet even while driving on the highway. They also expect high data bit rates to surf the internet, to download files and to have a real time video conference calls through wireless communication similar to the wired communication's data bit rate [1]. Most importantly manufacturers had implemented Vehicular Ad – Hoc Network (VANET) technology which creates mobile network by using moving vehicles as nodes in a network [1]. Importantly, these technological advancements in wireless vehicles brings in a lot of possibility for *Cyber Attacks*. So, we mainly focus on '*Cyber Security of a wireless vehicle'* in this work.

2 LITERATURE REVIEW

In recent times, wires are being replaced by wireless technology in auto-mobile. There are a lot of benefits in removing all the wires within a vehicle and implementing wireless communication in a vehicle. Some of which are,

1. It helps to avoid collision in the vehicle network by issuing an automatic warning which ensures safety ([1] and [2]).
2. It enables users to know about directions, weather reports. Users could also check e-mails, social media, and download files thereby increasing the comfort level of passengers even while travelling ([1] and [2]).
3. Installation cost of wireless technology in auto-mobile is cheaper compared to wired technology.
4. Rapid Deployment, and Mobility [3].

Replacing wires with wireless communication in auto-mobile also brings in a lot of security challenges. '*Cyber security of a wireless vehicle'* is the major concern in recent times which would be discussed in this section by reviewing various research conducted.

2.1 Firmware updates Over The Air (FOTA) and Wireless Diagnostics

Over the past decade there are a lot of research conducted with regard to FOTA and Wireless Diagnostics. FOTA help to save consumers' time and to reduce the labour costs of the manufacturers in service stations. This makes it simpler for manufacturers to fix the bug in a short time.

In 2005, Mahmud et al proposed an architecture for uploading software in vehicle after making a few assumptions such as all the vehicles would be equipped with wireless interface units, company would need to upload software in the vehicle they manufactured, set of keys would be installed in the vehicle at the time of manufacturing [4]. Those keys would ensure the authentic communication between manufacturer and/or software supplier with the vehicle. They had also recommended software suppliers to send at-least two copies of software with a message digest to the vehicle in-order to improve security [4]. But their work is limited as it help to upload software in only one vehicle at a time which means it could be used only for wireless diagnostics where manufacturer would need to fix a particular vehicle which have problems and also their work did not cover the aspects of key management.

In 2008, Nilsson et al proposed a protocol for FOTA which ensured data integrity, authentication, confidentiality, and data freshness [5]. They analysed the security aspects by conducting various experiments. But their work did not address a few major issues like privacy, key management.

In 2008, Nilsson et al assessed the risks that involved with wireless infrastructure and derived a set of guidelines for creating secured infrastructure to do wireless diagnostics and software updates [6]. They identified portal security risks such as *Impersonation and Intrusion*, communication link security risks such as *Traffic Manipulation,* and vehicle security risks such as *Impersonation and Intrusion,* and the consequences of these risks such as *Execution of Arbitrary Code, Disclosure of Information, and Denial of Service* [6].But they did not analyse the risks involved with the Engine Control Unit (ECU). They suggested to explore the use of Intrusion Detection System (IDS) and Firewall in wireless vehicles to improve the security [6].

In 2011, Idrees et al proposed a protocol which guaranteed a secured FOTA in wireless vehicles [7]. They mainly focussed on hardware security mechanism. This helped to improve the standard of security compared to the other systems. Key issue still need to be addressed in FOTA is key management and uploading software in multiple vehicles at the same time securely.

2.2 Digital Forensic Investigation

Digital Forensic Investigation is important in-order to identify the criminal in-case of successful cyber attacks but till now there are only a few research conducted with regard to digital forensic investigation in wireless vehicles.

In 2004, Carrier et al proposed an event – based digital forensic investigation framework [8]. This is used by Nilsson et al as the base for their work. Nilsson et al derived a list of requirements for detection, data collection, and event reconstruction based on the attacker model and digital forensic investigation principles [9]. They have also recommended to use event data recorder which would play a major role in digital forensic investigation, a method to detect events in vehicle, and to trigger an alert about security violation which would help the investigators to initiate the investigation [9]. Storing current state vehicle information in a secured location prove to be one of the important information during digital forensic investigation [9]. Major limitation of this work would be that they did not explore detection techniques which would help digital forensic investigation.

2.3 In – Vehicle Network

In – Vehicle Network play an important role in wireless vehicles. There are a lot of research conducted in this area over the years. In 2003, Mahmud et al analysed blue-tooth and their security issues in wireless vehicles [10]. In 2008, Larsson et al proposed specification based attack detection techniques within the In-Vehicle network [11]. In 2008, Verendel et al proposed a system that make use of honeypot in-order to gather attackers' information [12]. In 2008, Nilsson et al categorised ECUs based on the safety and security characteristics [13]. In 2009, Nilsson, et al analysed FlexRay protocol by simulating attacks [14]. In 2010, Rouf et al evaluated security and privacy of wireless tire pressure monitoring systems [15]. In 2010, Koscher et al summarised the potential risks involved with wireless vehicles after conducting various experiments [16]. In 2011, Kleberger et al categorised the research areas with regard to security aspects of the In-Vehicle Network in wireless vehicles [17]. In 2012, Schweppe et al proposed an architecture that incorporates data flow tracking into In – Vehicle Network which would ensure security and privacy [18]. In 2012, Onishi analysed new risks in the wireless vehicles caused by Carry-In Devices and suggested suitable countermeasures [19]. Detailed analysis of these research would be carried out in Section 3.

2.4 Vehicle – Vehicle Communication

There were many research conducted in Vehicle – Vehicle communication which is one of the important aspects of wireless vehicle. In 2004, Mahmud et al proposed a technique to exchange messages between vehicles securely. They have also analysed about creating secure communication links between vehicles. After analysing, they concluded that this would be possible with the present technology [20]. This technique ensured authentication, authorisation, and data integrity. But they did not focus on the privacy aspect which is one of the important aspects in vehicle – vehicle communication [20].

In 2004, Hu et al analysed the wormhole attacks and they proposed how to detect the wormhole attacks using directional antennas [21].

In 2006, Raya et al analysed the vulnerabilities that exist in vehicular communication such as jamming, forgery, in – transit traffic tampering, impersonation, privacy violation, and on board tampering [22]. After analysing the hardware modules, they have recommended to use Event Data Recorder (EDR), and Tamper Proof Device (TPD) which would improve security. They concluded their work by listing open research problems in vehicular communication such as secure positioning, data verification, and Denial of Service (DOS) resilience [22].

In 2006, Moustafa et al proposed Authentication, Authorization, and Accounting (AAA) mechanism to authenticate vehicles on highways which would ensure secure data transfer between wireless vehicles. They considered Optimized Link State Routing (OLSR) protocol as the base to propose their reliable routing approach [23].

In 2007, Gerlach et al proposed a security architecture for vehicular communication using functional layer, organizational/component, reference model, and information centric views [24]. They suggested that this architecture could be used as a base for prototype implementation. Security level could be also analysed by conducting various practical experiments [24].

In 2008, Larson et al analysed the security issues of vehicle – vehicle communication. They used anti intrusion taxonomy introduced by Halme et al [25] as the base for discussing layers of defence – in – depth paradigm. They have also suggested vehicle manufacturers to adopt Defence – in – Depth approach in the future to improve security level in the wireless vehicles [26].

In 2008, Anurag et al introduced collision avoidance system using Global Positioning System (GPS). This system would ensure safety in wireless vehicles [27].

In 2010, Tripathi analysed problems that exist in Vehicular Ad-Hoc Networks which mainly focused on basic attacks such as cheating with sensor information, ID disclosure of other vehicles in order to track their location, Denial of Service (DoS), masquerading and also other sophisticated attacks such as hidden vehicles, tunnel, wormhole, and bush telegraph [28]. This work lacks practical analysis.

In 2010, Amirtahmasebi et al discussed about various attacks such as sybil attack, bogus information, Denial of Service, impersonation, alteration attack, replay attack, and illusion attack in vehicular communication as well as various securing techniques such as digital signatures, tamper proof device, data correlation, and WAVE (*Wireless Access in Vehicular Environments - IEEE 1609.2*) [29].

After reviewing various research conducted in *'Cyber Security of a Wireless Vehicle'*, we have identified four important categories of research in this area.

They are:

1. Firmware updates Over The Air (FOTA) and Wireless Diagnostics
2. Digital Forensic Investigation
3. In – Vehicle Network
4. Vehicle – Vehicle Communication

3 IN-VEHICLE NETWORK

In–Vehicle Network is the combination of Engine Control Units (ECUs), and buses. Most common networks are Controller Area Network (CAN), Local Interconnect Network (LIN), Media Oriented Systems Transport (MOST), and Flex Ray ([9], [11], and [13]). CAN play a vital role in communication of safety – critical applications like Anti-lock braking system, and Engine management systems [11]. LIN play a major role in communication of non – safety critical sensors, and actuator systems [13]. MOST is the high speed technology which is used to carry audio, and video data [13]. CAN is being replaced by FlexRay in the recent years. Data is transferred from one network to another using wireless gateways ([9], [11] and [13]). In – Vehicle Network is illustrated in Figure 1 [12].

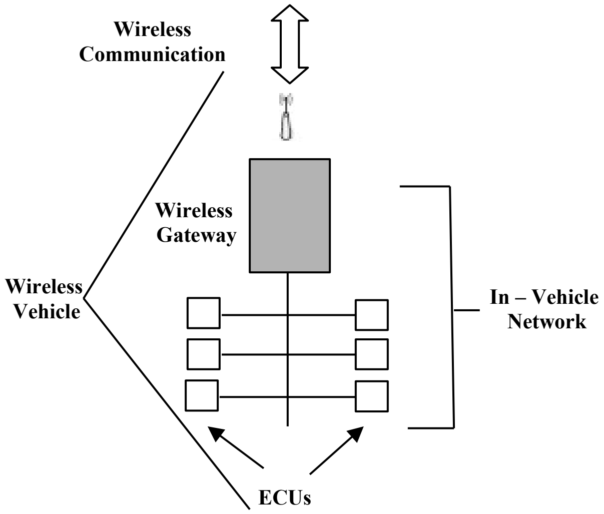

Figure 1. In – Vehicle Network [12]

As discussed earlier in Section 2, there are a lot of research conducted with regard to *'In – Vehicle Network'*. In 2003, Mahmud et al proposed a technique which would help to secure wireless In – Vehicle Blue-tooth networks. Short range communication between closer vehicles would help to avoid collision. This could be achieved using blue-tooth technology. Blue-tooth technology covers 10-100 metres in wireless communication [10]. They have also proposed a security architecture which make use of password protected Network Device Monitor (NDM) [10]. NDM help to activate devices which would want to take part in the wireless communication. It would make use of two different PINs: one for secured communication which should be changed after each session to encounter brute – force attack, and the another one for non – secured communication which is not necessary to change after each session [10]. NDM plays a major role in distributing PINs to devices which would be the suitable countermeasure against Man – in – the – Middle Attack [10]. This architecture could also be implemented at a very low cost. They concluded their work by addressing one of the important question *"what happens if the activated* *device got stolen or lost"?.* They suggested in that case the owner would be able to deactivate that device manually using NDM [10]. But they failed to address *"what happens if NDM malfunctions?"* in their work. As there is no alternate solution, the entire system would be compromised in that case.

In 2008, Larson et al proposed a technique that help to detect cyber-attacks within the in – vehicle network. They have also suggested the location where the attack detector could be placed. Their work mainly focussed on CAN protocol version 2.0 and CANopen draft standard 3.01 which is used to create protocol – level security specifications [11]. They have also mentioned that the abnormal messages could be detected with the help of communication protocol security specifications and Illegal attempts to transmit or receive messages could be detected with the help of ECU communication parameters [11]. They recommended to place a detector on each ECU because if a detector is placed in CAN it is impossible to detect the source and destination of the message as it would not support unique ECU identifiers [11]. But if we place the detector on each ECU, this would be helpful as the object directory of ECU knows which one to transmit and to receive. They evaluated the attack detector using different attacker actions such as Flood, Read, Replay, Spoof, and Modify [11]. They concluded that still there are some attacks which would be possible even if the attack detector is placed. In-order to make this system effective and complete, they have suggested to implement alternate approach like firewalls to complement the attack detector [11].

In 2008, Verendel et al proposed a technique to gather attackers' information using honeypot which is simulated In – Vehicle network as shown in Figure 2 [12]. This would allow us to analyse the attackers' behaviour thereby we could prevent cyber-attacks. They suggested that honeypot should be placed in the vehicle and gathered information should be processed at the central location. Larson et al have identified the major attacks in the In – Vehicle network. Verendel et al used it as the base to detect the attacks early which would help to ensure safety. But they did not focus on the security of gathered data which would be analysed at the processing centre. This data could be tampered.

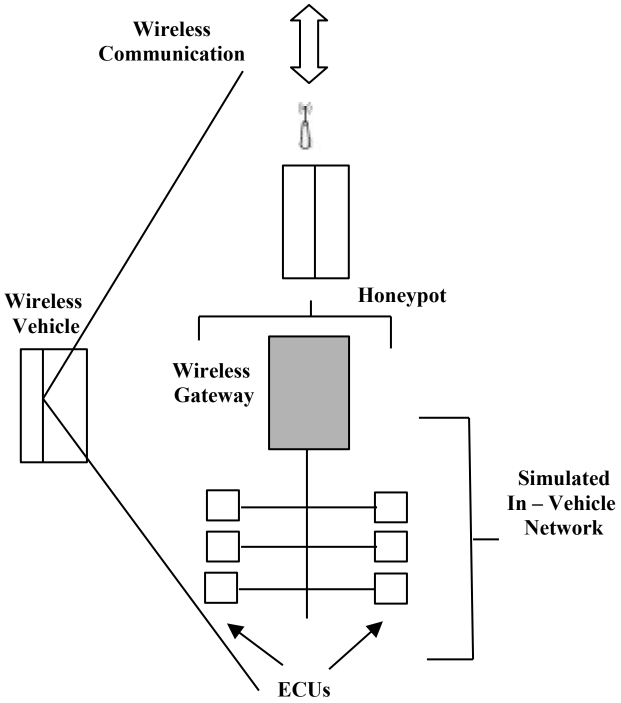

Figure 2. Vehicle Honeypot [12]

In 2008, Nilsson et al classified ECUs into five categories based on the safety and security characteristics. They were Powertrain, Vehicle Safety, Comfort, Infotainment, and Telematics [13]. After analysing the attacker model, they concluded that communication link is the main target for the attackers where cyber-attacks such as eavesdropping, intercepting, modifying, and injecting messages would be possible [13]. They discussed the process of assigning Safety Integrity Levels (SIL) ranging from highest level 4 to lowest level 1 based on their controllability after failure. They assigned highest SIL 4 for powertrain and vehicle safety ECUs. Powertrain category consists of brake system which is highly important to ensure safety. In case of failure, driver would not be able to control the vehicle. Vehicle Safety category consists of tire pressure monitoring, air bag, collision avoidance system which are also highly safety critical. They have also assigned highest safety integrity level as in the case of failure, driver would not be able to control the vehicle [13]. They have assigned level 2 for comfort category as it would not affect the safety immediately. They have assigned level 1 for both infotainment and telematics. Infotainment category consists of audio and video systems, mobile communication is provided by the ECUs of telematics category which were not highly safety critical [13]. This work would help to prioritise the categories which need more protection to ensure safety in the wireless vehicles.

In 2009, Nilsson et al focused on FlexRay protocol. Their work answered the question '*why CAN is being replaced gradually by FlexRay over the years?'*. FlexRay is different and effective in various aspects compared to CAN. Some of which were: FlexRay support different topologies, higher data rates, and continuous communication [14]. They also considered security properties such as data confidentiality, data integrity, data availability, data authentication, and data freshness to evaluate the security of FlexRay protocol [14]. They used Nilsson – Larson attacker model as their base and focussed on attacker actions such as read, and spoof. Read attack is possible due to lack of confidentiality, and Spoof attack is possible due to lack of authentication in FlexRay. They concluded their work by simulating these attacker actions. The major limitation of this work was that they did not provide any prevention techniques for these attacks [14]. This work could be further expanded by identifying a few more attacker actions, providing detection, and prevention techniques for these attacks which would guarantee secured FlexRay protocol [14].

In 2010, Rouf et al evaluated wireless Tire Pressure Monitoring System (TPMS). Air pressure inside the tires could be measured using TPMS continuously which would help to alert driver in-case of under inflated tires [15]. They have discussed about the security risks involved such as tracking auto-mobiles, and spoofing. They have also analysed TPMS experimentally and found out that the messages could be received up to 40m away from the car with the help of low noise amplifier [15].

They have also discussed about TPMS architecture as shown in Figure 3 [15] which consists of TPM sensors fitted in each tire, TPM ECU/receiver, a TPM warning light at the dashboard, one or four antennas, and receiver is connected to the antennas. They have recommended to follow reliable software design for the software that run in the TPMS ECU which would help to prevent displaying false readings, to encrypt packets. Packet format should be improved in-order to limit eavesdropping, and spoofing attacks [15]. Eavesdropping is the major issue which need to be addressed in the future research to make this system effective. In future, this system could also be shielded to ensure that there is no chance of eavesdropping, and spoofing attacks.

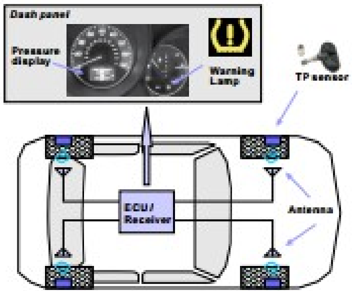

Figure 3. TPMS Architecture [15]

In 2010, Koscher et al used two wireless vehicles of same make and model which was manufactured in 2009 to evaluate the issues of wireless vehicle by conducting various experiments [16]. They have conducted experiments in three different settings [16].

1. They extracted the hardware components and analysed them in lab [16].
2. They elevated the car on jack stand and conducted various experiments to ensure safety [16].
3. They drove the wireless vehicle on decommissioned airport runway and conducted various experiments to ensure safety [16].

They have also summarised the results of various experiments. Also they have discussed about the key security challenges in CAN such as broadcast nature, fragility to Denial of Service, no authenticator fields, and weak access controls [16]. In future, this work could be used as the base to design prevention techniques that would help to improve the security of wireless vehicles.

In 2011, Kleberger et al have reviewed various research related to 'in – vehicle network' and identified five categories of research. They were problems in the In – Vehicle network, architectural security features, Intrusion Detection Systems (IDS), Honeypots, and Threats and attacks [17]. They identified problems in the In – Vehicle network such as lack of sufficient bus protection, weak authentication, misuse of protocols, poor protocol implementation, and information leakage. They suggested to investigate IDS for FlexRay because both specification based and anomaly based IDS have been suggested for CAN [17]. This research did not provide any security solutions but this could be used as the base for designing security solutions for the In – Vehicle network.

In 2012, Schweppe, and Roudier proposed a system with taint tracking tools that would help to monitor data that flows between ECUs in the In – Vehicle network. Using taint tracking tools in auto-mobile guarantees privacy and security [18]. This system could be used with Rouf et al wireless Tire Pressure Monitoring System (TPMS) to prevent spoof attacks thereby ensuring security, and safety of that system.

In 2012, Onishi focussed on potential risks involved with wireless vehicles and assessed their severity using Common Vulnerability Scoring System (CVSS) [19]. They have identified that Carry – In – Devices (CID) creates major risks in wireless vehicles because virus, and malware could invade the system [19]. They have suggested to use certification - authority which would help to verify the content of CID and issue certificates for CID without any malicious contents [19]. They have summarised the limitations of ECU such as low computational power, low memory, and online software update issues. They suggested that it is difficult to monitor CID always due to low computational power. But a few years back Nilsson et al prioritized ECU categories based on their Safety Integrity Level (SIL) which could be used with this research. Protecting powertrain and vehicle safety ECUs from virus, malware ensures vehicle to be in controllable state even if virus, malware invades infotainment ECUs. Onishi suggested to send warning alerts to driver if virus, malware invades highly safety critical ECUs which would help to prevent major accidents [19].
We have identified several key issues by exploring various research conducted in '*In – Vehicle Network'*. They are:

➔'Securing Gateway ECU' as it is the entry point for attackers. Successful attacks would give an opportunity for attackers to gain full control of the vehicle.
➔ 'Securing Communication Links' which could help us to prevent attacks like eavesdropping, interception, and modifying messages.
➔ 'Ensuring confidentiality, and privacy' in the system.
➔ 'Securing attackers' information at the processing centre' as the information gathered using honeypot to be analysed at the processing centre lacks security.
➔ 'Monitoring Carry – In – Devices always' to ensure safety and security of the wireless vehicle.

We have also identified several open research questions. They are:

➔ 'How to configure firewall in the wireless gateway?'
➔ 'How to improve the security of CAN, FlexRay?'
➔'How to implement Intrusion Detection System in the In – Vehicle Network?'
➔'How to monitor Carry – In – Devices always in wireless vehicle?'
➔ 'How to shield the communication link from attacks?'

4 CONCLUSION

After reviewing various research conducted in 'Cyber security of a Wireless Vehicle', we have identified four categories such as *'Firmware updates Over The Air (FOTA) and Wireless Diagnostics, Digital Forensic Investigation, In – Vehicle Network, and Vehicle – Vehicle Communication'.* We focussed on *'In -Vehicle Network'* and identified several key issues by reviewing various research conducted. It is evident that security lacks in the *'In – Vehicle network'* from this work. We have also identified various research problems that have not been adequately addressed. This work could be used as a starting point in the future to address the identified open research questions and improve security in the *'In –Vehicle Network'* as it highlights various security problems.

5 REFERENCES

1. C. Ribeiro, “Bringing Wireless Access to the Automobile: A Comparison of Wi-Fi, WiMAX, MBWA, and 3G”, *21st Computer Science Seminar*, pp. 1–7, 2005.

2. A. Gandhi, and B.T. Jadhav, “Role of Wireless Technology for Vehicular Network,” *International Journal of Computer Science & Information Technologies (IJCSIT)*, Vol. 3, No. 4, pp. 4823–4828, 2012.

3. P. Parikh, M.G. Kanabar, and T.S. Sidhu, “Opportunities and Challenges of Wireless Communication Technologies for Smart Grid Applications,” *IEEE Power and Energy Society General Meeting,* pp. 1-7, July 2010.

4. S.M. Mahmud, S. Shanker, and I. Hossain, “Secure Software Upload in an Intelligent Vehicle via Wireless Communication Links,” *Proceedings of the IEEE Intelligent Vehicles Symposium*, pp. 588–593, 2005.

5. D.K. Nilsson, and U.E. Larson, “Secure Firmware Updates over the Air in Intelligent Vehicles,” *Communications Workshops, 2008. IEEE International Conference on*, pp. 380–384, May 2008.

6. D.K. Nilsson, U.E. Larson, and E. Jonsson, “Creating a Secure Infrastructure for Wireless Diagnostics and Software Updates in Vehicles,” *Proceedings of the 27th international conference on Computer Safety, Reliability, and Security*, Vol. 5219/2008, pp. 207–220, 2008.

7. M.S. Idrees, H. Schweppe, Y. Roudier, M. Wolf, D. Scheuermann, and O. Henniger, “Secure Automotive On-Board Protocols : A Case of Over-the-Air Firmware Updates,” *Proceedings of the third International Workshop on Communication Technologies for Vehicles,*Vol. 6596, pp. 224–238, 2011.

8. B.D. Carrier and E.H. Spafford, “An Event-Based Digital Forensic Investigation Framework*,” *Digital Forensic Research Workshop*, pp. 1–12, 2004.

9. D.K. Nilsson and U.E. Larson, “Conducting Forensic Investigations of Cyber Attacks on Automobile In-Vehicle Networks,” *International Journal of Digital Crime and Forensics*, vol. 1, no. 2, pp. 28–41, 2009.

10. S.M. Mahmud and S. Shanker, “Security of Wireless Networks in Intelligent Vehicle Systems,” *Proceedings of 3rd Annual Intelligent Vehicle Systems Symposium*, NDIA, pp. 83–86, 2003.

11. U.E. Larson, D.K. Nilsson, and E. Jonsson, “An approach to specification-based attack detection for invehicle networks,” *IEEE Intelligent Vehicles Symposium*, pp. 220–225, June 2008.

12. V. Verendel, D.K. Nilsson, U.E. Larson, and E. Jonsson, “An Approach to using Honeypots in In-Vehicle Networks,” *68th IEEE Vehicular Technology Conference*, pp. 1207–1211, 2008.

13. D.K. Nilsson, P.H. Phung, and U.E. Larson, “Vehicle ECU Classification Based on Safety – Security Characteristics,” *Proceedings of 13th International Conference on Road Transport and Information Control (RTIC)*, pp. 1–7, 2008.

14. D.K. Nilsson, U.E. Larson, F. Picasso, and E. Jonsson, “A First Simulation of Attacks in the Automotive Network Communication Protocol FlexRay,” P*roceedings of the International Workshop on Computational Intelligence in Security for Information Systems (CISIS'08),* Vol. 53, pp. 84-91, 2009.

15. I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, “Security and Privacy Vulnerabilities of In-Car Wireless Networks : A Tire Pressure Monitoring System Case Study,” *Proceedings of 19th USENIX Security Symposium*, pp. 323 – 338, 2010.

16. 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,” *IEEE Symposium on Security and Privacy*, pp. 447–462, 2010.

17. P. Kleberger, T. Olovsson, and E. Jonsson, "Security aspects of the in-vehicle network in the connected car," *IEEE Intelligent Vehicles Symposium (IV)*, pp. 528–533, June 2011.

18. H. Schweppe and Y. Roudier, "Security and privacy for in-vehicle networks," *1st IEEE International Workshop on Vehicular Communications, Sensing, and Computing (VCSC)*, pp. 12–17, June 2012.

19. H. Onishi, "Paradigm Change of Vehicle Cyber Security," *Proceedings of 4th International Conference on Cyber Conflict (CYCON)*, pp. 1-11, 2012.

20. S.M. Mahmud, S. Shanker, and S.R. Mosra, "Secure Inter-Vehicle Communications," *Proceedings of SAE World Congress*, pp. 8-11, 2004.

21. L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," *Proceedings of Network and Distributed System Security Symposium (NDSS)*, pp. 1 - 11, 2004.

22. M. Raya, P. Papadimitratos, and J. Hubaux, "Intervehicular Communications – Securing Vehicular Communications," *IEEE Wireless Communications*, Vol. 13, No. 5, pp. 8–15, 2006.

23. H. Moustafa, G. Bourdon, and Y. Gourhant, "Providing Authentication and Access Control in Vehicular Network Environment," *Proceedings of IFIP TC-11 21st International Information Security Conference (SEC)*, Vol.201, pp. 62–73, 2006.

24. M. Gerlach, A. Festag, T. Leinmuller, G. Goldacker, and C. Harsch, "Security Architecture for Vehicular Communication," *Proceedings of International Workshop on Intelligent Transportation (WIT)*, pp. 1 – 6, 2007.

25. L.R. Halme, and K.R. Bauer. "AINT Misbehaving: A taxonomy of anti-intrusion techniques," *Proceedings of 18th National Information Systems Security Conference*, pp. 163–172, 1995.

26. U.E. Larson, and D.K. Nilsson, "Securing vehicles against cyber-attacks," *Proceedings of the 4th annual workshop on Cyber security and informaiton intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead – CSIIRW*, pp. 1 – 3, 2008.

27. D. Anurag, S. Ghosh, S. Bandyopadhyay, "GPS based vehicular collision warning system using IEEE 802.15.4 MAC/PHY standard," *8th International Conference on ITS Telecommunications (ITST)*, pp.154-159, 2008.

28. K.P. Tripathi, "An Essential of Security in Vehicular Ad hoc Network," *International Journal of Computer Applications*, Vol. 10, No. 2, pp. 11-16, 2010.

29. K. Amirtahmasebi and R.S. Jalalinia, "Vehicular Networks – Security , Vulnerabilities and Countermeasures," *Master of Science Thesis in the program Networks and Distributed Systems, Chalmers University of Technology*, pp. 1–55, June 2010.