ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 04, pp.29378-29381, April, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

EMERGING TECHNOLOGY IN CAR-TO-CAR COMMUNICATION

***,[1]Sharvin Pingulkar, [1]Haroondeep Singh Sandhu and [2]Vivek Kataruka**

[1]Electronics and Telecommunication Engineering, Rajiv Gandhi Institute of Technology, Mumbai, India
[2]Computer Science Engineering, Rajiv Gandhi Institute of Technology, Mumbai, India

ARTICLE INFO

Article History:
Received 23rd January, 2016
Received in revised form
15th February, 2016
Accepted 09th March, 2016
Published online 26th April, 2016

Key words:

Car-To-Car Communication,
Driving Information System,
Wireless Communication.

ABSTRACT

This Car-To-Car Communication is a vital information module for driving comfort and safety. It changes the role of automobiles from mere objects used for transportation to smart vehicles capable to talk to each other through wireless communication. The goal is to develop new functionalities for cars and trucks offering driver information system (DIS). Necessary interaction between the driver and automated systems shall be enabled by advanced sensors, cooperative vehicle technologies and adaptive strategies. In this paper we present the potential of future car-to-car and car-to-environment communication systems, introduce the major research challenges in this field, and provide a selection of current research results.

Citation: Sharvin Pingulkar, Haroondeep Singh Sandhu and Vivek Kataruka, 2016. "Emerging technology in car-to-car communication", *International Journal of Current Research*, 8, (04), 29378-29381.

INTRODUCTION

In the last couple of years communication between vehicles has attracted the interest of many researchers around the world. Countries are researching on various technologies for improving road safety and reducing the vehicle crashes. Research projects are being taken up to look into the potential of reducing the accident fatalities by considering the *eSafety Initiative* (e.g. GST, PreVent). This is the story of uplifting this technology in the research oriented countries like USA and Japan. Car-to-car communication (C2CC), often referred to as *vehicular ad hoc networks (VANETs)*, enables many new services for vehicles and creates numerous opportunities for safety improvements. Communication between vehicles can be used to realize driver support and active safety services like collision warning, up-to-date traffic and weather information or active navigation systems. Abruptness can be detected through various sensors thus providing the user complete information about the arriving vehicle and he can ensure his safety through precautionary measures. In order to make roads safer, cleaner and smarter, sensor and communication technologies are increasingly considered in research, standardization and development.

****Corresponding author: Sharvin Pingulkar,***
Electronics and Telecommunication Engineering, Rajiv Gandhi Institute of Technology, Mumbai, India.

While today's vehicles are already able to sense the surrounding environment, we expect that future cars will communicate with a roadside communication infrastructure and with each other. Connected vehicles create a fundamental building block of intelligent transport systems (ITS) and can provide numerous application services to improve safety and comfort of driving. How much time do we spend in cars on an average? Americans spend around 26 days a year in cars. How about Egyptians? They spend around 1000 hours which comes to around 40 days a year in automobiles. Considering the following numbers, it is of utmost importance for vehicles to be safe. Vehicle to Vehicle (V2V) Communication is an emerging technology which uses dynamic exchange of data between the vehicles providing each other with necessary information about the corresponding vehicles such as safety warnings, traffic updates and abruptness in driving.

On a grass route level there are many challenges faced by the research team which are very difficult to overcome. Message integrity, time and bandwidth constraint as well as full proof testing in automobiles are the main areas where the safety is rendered mute. While the development of vehicular communication technology based on IEEE 802.11p has considerably progressed in the past years, the introduction and wide-scale deployment of such a system has not been decided yet. In a purely vehicular communication system, i.e. without roadside access points, a minimum market penetration of equipped vehicles is required for applications to work. This

can at best be achieved a few years after an initial commercial roll-out. To accelerate the revenue of such investment, a roadside infrastructure could be installed along major road across a country. However, costs for purchase, installation and maintenance represent a major investment and in turn can be an obstacle for a successful.In this paper, we propose and analyze a hybrid architecture that combines vehicle-to vehicle communication and vehicle-to-roadside sensor communication. From the wide range of possible use cases, we have chosen accident prevention and post-accident investigation, which we regard as important future services. For accident prevention, roadside sensor nodes measure the road condition at several positions on the surface, aggregate the measured values and communicate their aggregated value to an approaching vehicle. The vehicle generates a warning message and distributes it to all vehicles in a certain geographical region, potentially using wireless multi-hop communication. For post-accident investigation, sensor nodes continuously measure the road condition storing this information within the WSN itself. If an accident occurs, data stored over a sufficiently long duration can be used for forensic reconstruction of road accidents. In contrast to the accident prevention service, such a liability service needs to be restricted to a specified group of users, e.g. insurance companies or the road patrol.

Choice of technology and services

Vehicular Ad Hoc Networks (VANETs) have grown out of the need to support the growing number of wireless products that can now be used in vehicles. These products include remote keyless entry devices, personal digital assistants (PDAs), laptops and mobile telephones. As mobile wireless devices and networks become increasingly important, the demand for Vehicle-to-Vehicle (V2V) and Vehicle- to-Roadside (VRC) or Vehicle-to-Infrastructure (V2I) Communication will continue to grow. VANETs can be utilized for a broad range of safety and non-safety applications, allow for value added services such as vehicle safety, automated toll payment, traffic management, enhanced navigation, location-based services such as finding the closest fuel station, restaurant or travel lodge and infotainment applications such as providing access to the Internet.

Quality of Service (QoS)

The term Quality of Service (QoS) is used to express the level of performance provided to users. High levels of QoS in traditional networked environments can often be achieved through resource reservation and sufficient infrastructure, however, these cannot be guaranteed in dynamic, ad-hoc environments, such as those used in VANETs due the VANETs inherent lack of consistent infrastructure and rapidly changing topology. Most QoS routing strategies aim to provide robust routes among nodes and try to minimize the amount of time required to rebuild a broken connection. However, factors such as node velocity, node positioning, the distance between nodes, the reliability of and delay between links can seriously affect the stability of a particular route. Simulations were carried out in both highway and urban environments with varying vehicle density and speed to determine the upper performance bound for connection duration, packet delivery ratio, end-to-end delay, and jitter for unicast communication in typical highway and urban VANET environments. According to their results, delay and jitter in VANETs were adequate for most of the envisioned unicast-based applications, whereas the packet delivery ratio and connection duration may not meet the requirements for most unicast-based applications. The various research was achieved by simulating vehicles in an urban environment to analyze the performance of a multipath routing protocol and its impact on global QoS metrics. Their simulations show substantial improvement in performance compared to no multipath, only gateways multipath, only nodes multipath and all multipath when considering global QoS metrics in vehicle-to-vehicle and vehicle-to-infrastructure communications.

Security Issues

The security of VANETs is crucial as their very existence relates to hazards in the life at a very critical rate. It is obvious that vital information cannot be inserted or fidgeted by a malicious person. The system must be able to determine the liability of drivers while still maintaining their privacy as well as maintain the important information related to the sending and receiving process of the desired technology. These problems are difficult to solve because of the network size, the speed of the vehicles, their relative geographic position, and the randomness of the connectivity between them. An advantage of vehicular networks over the more common ad hoc networks is that they provide ample sources for transmitting the desired data. The types of attacks against messages, can be described as follows: “Bogus Information”, “Cheating with Positioning Information”, “ID disclosure”, “Denial of Service”, and “Masquerade”. The reliability of a system where information is gathered and shared among entities in a VANET raises concerns about data authenticity. For example, a sender could misrepresent observations to gain advantage (e.g., a vehicle falsely reports that its desired road is travelling at a speed it is not and distributing false data to the vehicles nearby, thereby making the other vehicle drivers feel unsafe while taking the route). More malicious reporters could impersonate other vehicles or road-side infrastructure to trigger safety hazards. Vehicles could reduce this threat by creating networks of trust and ignoring, or at least distrusting, information from untrusted senders. Threats to availability, authenticity, and confidentiality Attacks can be broadly categorized into three main groups: those that pose a threat to availability, those that pose a threat to authenticity and those that pose a threat to driver confidentiality.

The following sections present threats posed to each of the areas of availability, authenticity, and confidentiality.

Threats to availability

The following threats to the availability of vehicle-to-vehicle and vehicle-to-roadside communication (including routing functionality) have been identified:

- Denial of Service Attack*: DoS attacks can be carried out by network insiders and outsiders and renders the network*

unavailable to authentic users by flooding and jamming with likely catastrophic results. Flooding the control channel with high volumes of artificially generated messages, the network's nodes, onboard units and roadside units cannot sufficiently process the surplus data.

- Broadcast Tampering: *An inside attacker may inject false safety messages into the network to cause damage, such as causing an accident by suppressing traffic warnings or manipulating the flow of traffic around a chosen route.*
- Malware*: The introduction of malware, such as viruses or worms, into VANETs has the potential to cause serious disruption to its operation. Malware attacks are more likely to be carried out by a rogue insider rather than an outsider and may be introduced into the network when the onboard units and roadside units receive software and firmware updates.*
- Spamming*: The presence of spam messages on VANETs elevates the risk of increased transmission latency. Spamming is made more difficult to control because of the absence of a basic infrastructure and centralized administration.*
- Black Hole Attack*: A black hole is formed when nodes refuse to participate in the network or when an established node drops out. When the node drops out, all routes it participated in are broken leading to a failure to propagate messages.*

Threats to authenticity

Providing authenticity in a vehicular network involves protecting legitimate nodes from inside and/or outside attackers infiltrating the network using a false identity, identifying attacks that suppress, fabricate, Vehicular ad hoc networks (VANETS): status, results, and challenges alter or replay legitimate messages, revealing spoofed GPS signals, and impede the introduction of misinformation into the vehicular network. These include:

- ***Masquerading*:** Masquerading attacks are easy to perform on VANETs as all that is required for an attacker to join the network is a functioning onboard unit. By posing as legitimate vehicles in the network, outsiders can conduct a variety of attacks such as forming black holes or producing false messages.
- ***Replay Attack*:** In a replay attack the attacker re-injects previously received packets back into the network, poisoning a node's location table by replaying beacons. VANETs operating in the WAVE framework are protected from replay attacks but to continue protection an accurate source of time must be maintained as this is used to keep a cache of recently received messages, against which new messages can be compared.
- ***Global Positioning System (GPS) Spoofing*:** The GPS satellite maintains a location table with the geographic location and identity of all vehicles on the network. An attacker can fool vehicles into thinking that they are in a different location by producing false readings in the GPS positioning system devices. This is possible through the use of a GPS satellite simulator to generate signals that are stronger than those generated by the genuine satellite.
- ***Tunneling*:** An attacker exploits the momentary loss of positioning information when a vehicle enters a tunnel and before it receives the authentic positioning information the attacker injects false data into the onboard unit.
- ***Position Faking*:** Authentic and accurate reporting of vehicle position information must be ensured. Vehicles are solely responsible for providing their location information and impersonation must be impossible. Unsecured communication can allow attackers to modify or falsify their own position information to other vehicles, create additional vehicle identifiers (also known as Sybil Attack) or block vehicles from receiving vital safety messages.
- ***Message Tampering*:** A threat to authenticity can result from an attacker modifying the messages exchanged in vehicle-to-vehicle or vehicle-to-roadside unit communication in order to falsify transaction application requests or to forge responses.
- ***Message Suppression/Fabrication/Alteration*:** In this case an attacker either physically disables inter-vehicle communication or modifies the application to prevent it from sending to, or responding from application beacons.

Threats to confidentiality

Confidentiality of messages exchanged between the nodes of a vehicular network are particularly vulnerable with techniques such as the illegitimate collection of messages through eavesdropping and the gathering of location information available through the transmission of broadcast messages. In the case of eavesdropping, insider and/or outsider attackers can collect information about road users without their knowledge and use the information at a time when the user is unaware of the collection. Location privacy and anonymity are important issues for vehicle users. Location privacy involves protecting users by obscuring the user's exact location in space and time. By concealing a user's request so that it is indistinguishable from other users' requests, a degree of anonymity can be achieved.

Selected Search Results

Telematics Service Platforms

Many of the aforementioned services need some kind of OBU and a supporting backend infrastructure. This platform concept should be standardized between multiple vehicle manufacturers to generate a mass market and ease the market entry for new service providers. A standardization approach for a system platform has been developed within the European Project GST backed by the major car manufacturers. In Figure 1 the open high level platform architecture is shown, detailing the system entities and their interactions. Security SW & HW in each GST Node Secure Communications & Distributed Algorithms Public Key Infrastructure Vehicle End User Client System Control Center Center Service Payment Center Registration Authority Certificate Authority Figure 1 - The GST high level architecture diagram Security is a crucial aspect for a platform concept, especially if commercial services are included and subscription and billing have to be conducted over the platform. In (18) the security concepts of the GST platform are presented in detail. The trust is based on

a PKI with certificates. In addition, each entity is equipped with a hardware security module which is tamper proof. This module is the key component for all security related operations, since it stores, handles, and uses the keys and certificates. 4.2 Security in Vehicular Ad Hoc Networks As mentioned above, in the decentralized MANETs, the use of a PKI and certificates to introduce trust is not an obvious choice. Especially the continuously changing connectivity to different neighbors and the not guaranteed access to an Internet gateway node make the use of certificates a challenge. Our security framework LKN-ASF is a first approach using certificates to secure VANETs. The performance evaluation proved the feasibility of the approach. However, simply installing a PKI to introduce trust is not sufficient. A certificate management is needed which can validate and revoke certificates. With the limited access to the Internet and hence the PKI backend servers, this management is difficult to realize in VANETs. Both a conventional certificate revocation list approach and a concept using validation tickets proved to be quite efficient for the certificate management in distributed network environments. Many solutions have been published concerning secure routing protocols.

Conclusion

Car-to-car communication is an interesting and challenging new field in communication network research. While many creative and powerful new solutions have already been proposed, still many open issues exist.

Car-To-Car Communication is an interesting field in the subject of Telecommunication and Innovative Research. There is huge research facility set up in Massachusetts Institute of Technology, USA where Researchers and Scientists are setting up experiments for the emerging scientific development in this field. VANETs will only become a commercial and technological success as long as its services and capabilities are of high value to potential users during all phases of the introduction phase. Quality of Service (especially concerning latency) and security for VANET systems are crucial aspects of car-to-car communication that need to be integrated to ensure the success of this promising technology.

REFERENCES

Andreas Festag, Alban Hessler, Roberto Baldessari "Vehicle-to-vehicle and road-side sensor communication for enhanced road safety", Proceedings on ITS World Congress and Exhibition, New York, USA, November 2008.

Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges" Telecomm Syst DOI 10.1007/s11235-010 -9400-5.

Stephan Eichler#, Christoph Schroth§ and Jörg Eberspächer, Institute of Communication Networks, Technische Universität München, München, Germany, "Car To Car Communication".

****