sciendo

Transport and Telecommunication, 2020, volume 21, no. 3, 171–180
Transport and Telecommunication Institute, Lomonosova 1, Riga, LV-1019, Latvia
DOI 10.2478/ttj-2020-0013

PERFORMACE EVALUATION OF VEHICULAR COMMUNICATION

Muhammad Naeem Tahir[1], Kari Mäenpää[2],Timo Sukuvaara[3]

Finnish Meteorological Institute (FMI), Arctic Research Centre
Tähteläntie 62, 99600 Sodankylä, Finland
naeem.tahir@fmi.fi

Modern societies are built on good road infra-structure and efficient transport system. Safety is a high-priority consideration in development of road traffic systems. In recent years the weather information has become becomes very vital for road traffic safety because slippery roads are the key source of road accidents in northern regions of Europe, America and Canada as well. In this article we are presenting the test experiences and pilot road weather related services by executing a set of Vehicle to Infrastructure (V2I) communication scenarios by using IEEE 802.11p and 5G test networks. We have made an effort to evaluate the performance of IEEE 802.11p and 3GPP (3rd Generation Partnership Project) 5G test network. We also analyzed the performance of IEEE 802.11p with and without safety feature for secure and reliable vehicular communication. The combination of IEEE 802.11p with 5G test network cellular network makes the traffic system heterogeneous for traffic safety. This heterogeneous system provides the opportunity to exploit the vehicle-based actuators, sensor, and observation data in order to produce the intelligent service platform and up-to-date real time services for vehicles.

In this article we have also made a comparison by using an IEEE 802.11p system having safety feature of SafeCOP (Safe Co-operating Cyber-Physical Systems using Wireless Communication) project. SafeCOP is a European project that aims cyber-physical systems-of-systems relying on wireless communication for safe and secure cooperation. This safety feature will help to decrease the amount of road accidents (Car crashes, injuries and fatalities) by offering safe and secure V2V and V2I co-operation. The fundamental advantage of this kind of performance analysis is that the communication between Vehicle-to-Road Weather station (V2RWS) can be exchanged safely and reliably, at the cost of network resources consumed by a safety feature in IEEE 802.11p. It's clearly presented in this paper, that the use of heterogeneous network and SafeCOP feature for vehicular networking has a clear potential in near future for vehicle's safety and security of vehicular network.

Keywords: V2I, V2RWS, SafeCOP, IEEE 802.11p, 5G Test Network

1. Introduction

The rapid increase in vehicles making road traffic situations become increasingly congested, chaotic and complex. The concept is indeed fascinating for people that the vehicles share information and work collectively to make transport system safe, green, and more pleasant. The vehicles and technologies related to this idea, mutually known as Intelligent Transportation Systems (ITS). Intelligent traffic system plays a pivotal role in traffic management and monitoring by the use of technology to control and overcome these severe traffic issues of today's world. ITS technologies are assisting to develop and augment the way in which infrastructure and transportation systems are used including road traffic supervision, regulation and management. The evolving Wi-Fi standards and other wireless technologies are becoming mature and are suitable for vehicular communication.

Vehicular communication systems are employed with IEEE 802.11p and 3rd Generation Partnership Project (3GPP) cellular networks (Sukuvaara *et al*., 2016, Muhammad *et al.,* 2019). The IEEE 802.11 standard body launched 802.11p standard in 2012, specifically for vehicular communication. The fundamental technology in IEEE 802.11p protocol is Direct Short Range Communication (DSRC). The 802.11p was basically designed to improve the transport system and to make it even safer. It's commonly in use now to make better the public safety applications and traffic flow i.e. Vehicle-to-Vehicle (V2V) and Vehicle to Infrastructure (V2I). The evolving 3GPP standards also provides us the solution for ITS. Vehicular communication (V2V) and (V2I) communication supports Co-operative services and data transfer techniques and can utilize the latest 5G network services by using numerous radio access technologies (RATs) instead of 4G and DSRC (802.11p) (Kim *et al*., 2018, Mir *et al*., 2014). The 5G is a wireless communication technology with good data rate with high latency and is now being used in vehicular environment. Intelligent transport system assisted by IEEE 802.11p or 5G having one the major entity in vehicular communication is Road Weather Station (RWS). RWS are typically installed at the suitable fixed locations beside roads. RWS collect different measurement data and parameters related to

run-time traffic situations and up-to-date forecast information and transferring this data to a single data collection point of the traffic administrator. The information of the RWS network is broadcasted to the public and vehicles through road weather forecasts on internet, radio and TV (Sukuvaara *et al*., 2013).

The major issue in the use of wireless technologies is safety critical systems in ITS. In ITS, developers are trying hard to develop an explicit safety layer relating this evidence with safety arguments for secure V2V and V2I communication. The Co-operative Cyber-Physical System (CO-CPS) has one of the entity in the form of ITS communication environment (vehicles and Road Weather Stations). Safety for Vehicular Co-CPS systems facilitated by wireless communication technologies is a critical characteristic and needs new design methodologies. SafeCOP (Safe Co-operating Cyber-Physical Systems using Wireless Communication) is a European Union (EU) project that aims to a safety assurance methodology, certifying the secure communication within single Cyber-Physical element, as well as Co-CPS. Finnish Meteorological Institute (FMI) has developed one of the SafeCOP use case for vehicular CO-CPS entity, for the road weather station and vehicle interaction. In the SafeCOP project CO-CPS are furnished with extra safety systems derived from the safety standards (Balador *et al.*, 2018, Pisano *et al.*, 2018).

2. Intelligent Transport System

Recent transport problems i.e. road accidents, traffic jam etc. can no longer be resolved solely by constructing new highways or renovations of existing road infra-structure. In this regard, substantial efforts have been made in the scientific research over the last two decades to resolve the transport system problems by utilizing information technology and communication system resources and novel concepts on how to manage such intricate processes and systems. With the constant growth of urbanization the intelligent transportation system is getting more advanced i.e. smart cars. Intelligent transportation systems (ITSs) provides the solution to ensure the traffic safety, alleviating traffic jamming, decreasing transport emissions and improving the overall transport system operational efficiency. With the implementation and universalization of ITS in the area of transportation system, exclusively in urban traffic system, people are increasingly relying on ITS products (Vinel *et al.*, 2018).

In ITS, the vehicular communication system has a major role between Vehicles and Infrastructure (V2I) and Vehicles (V2V) offers co-operative services facilities related to road safety and weather alerts etc. Vehicles equipped with the advance cameras, processors and sensors are the emerging smart vehicles that have the ability to sense the current road weather condition and environment paving the way to state of the art intelligent transportation systems with great safety and productivity. One of the main developer in ITS venture is Google, who has lately presented their prototype smart vehicles in their promotion. As seen in the Figure 1 Vehicular radio system connects the vehicles, RWS, IoT cloud, infrastructures and other devices with wireless units, for vehicles to get the current global and local information to make decisions in an intelligent mode (Van Dam *et al*., 2018).

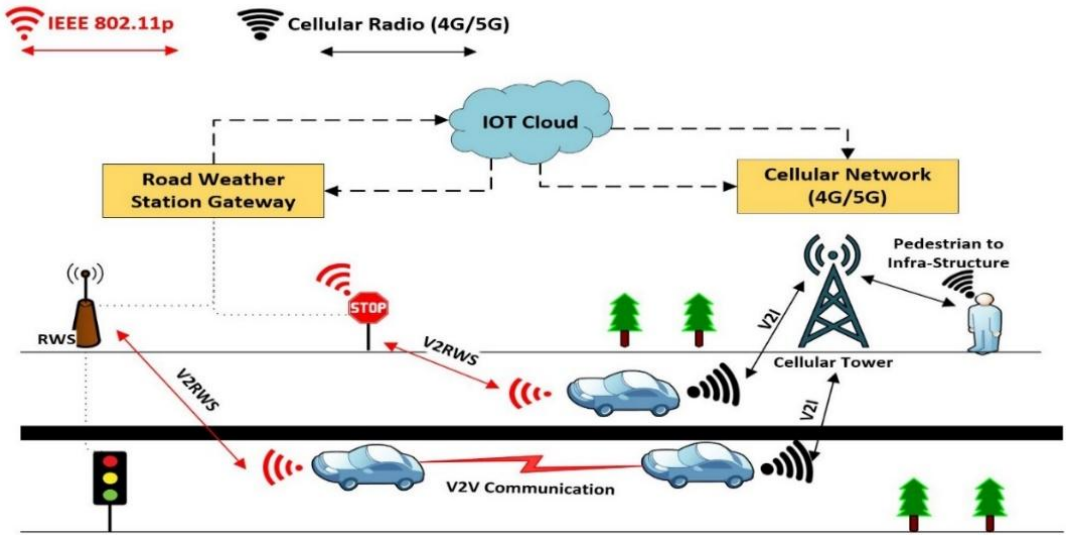

Figure 1. Vehicular Radio Technologies (IEEE 802.11p, 4G (LTE), 5G)

The vehicles use ITS applications and products to fetch up-to-date traffic data, to improve traffic security and traffic safety, such as using smart phone navigation, mobile phones, tablets etc. ITS applications and products are being widely implementing in almost all areas of urban transport system, i.e. traffic safety surveillance, traffic data service, traffic signal mechanism and traffic route guidance. These ITS applications and products directly impacts not only the safety of peoples life positively but also people's quality of living.

Consequently, when ITS applications and products gets faulty i.e. errors or failures, so that it can put the ITS system in an alarming situation because technology needs to be safe before its implementation. The future step might be the integration of safety-assured Road weather information into the road traffic simulations and road traffic prototypes with the utmost anticipated response (Severi *et al.,* 2018).

3. Vehicular Radio Technologies

3.1. IEEE-802.11p

The IEEE 802.11p was initially designed and launched by IEEE in 2012 to provide wireless access in vehicular environments (WAVE). The main purpose of 802.11p is to meet the specifications with the exacting performance. With the passage of time it's being deployed and used at large in vehicular communication scenarios. This technology is more mature and stable, as it was few years ago but gets mostly over-shadowed by the other networking standards i.e. 802.11a/b/g/n. IEEE-802.11p elucidates theWAVE. Its operational range is between 5.85 GHz to 5.925 GHz band for the deployment at increased rate and channelization (Vivek *et al.,* 2014). This technology aims for both vehicle to vehicle and vehicle to RWS/Roadside communication as presented in the Figure 1. The application of this standard protocol includes vehicle safety, in vehicle internet and road bridge tolls. It uses the orthogonal frequency division multiplexing (OFDM) for transmission. It can turn down 3GPP cellular technology in some aspects because it provides the connection with the constantly changing relative speed between transmitter and receiver creating selective transmission channel. The IEEE 802.11p can play a vital role for forthcoming V2x and hybrid communication with cellular technology (Vinel *et al.,* 2018).

3.2. 4G (LTE)

Fourth Generation (4G) and Long Term Evolution (LTE) technology is a 3rd Generation Partnership Project (3GPP) standard. It is the combination of fourth generation and long term evolution for data terminal and mobile devices based on the GSM/EDGE and UMTS/HSPA technologies. It was mainly designed to provide the IP-based voice, multimedia streaming and data at speeds ranging from 100Mbit to 1Gbit per second. 4G LTE is the currently fastest working commercial network technology, providing maximum speeds for downloading and uploading. 4G LTE, unlike earlier generations, uses Internet Protocol (IP) technology and provides mutual protocol for data transfer. This technology is the output of new technological advances in radio technology as a part of 3GPP. LTE will keep growing as a medium of connectivity for enterprises for primary communication medium. It has low latency, low idle to active times, higher spectrum efficiency at higher network capacity and improved cost efficiency. It offers uninterrupted coverage than the other systems such as Wi-Fi that makes users to depend upon the hotspots/access point. 4G LTE may bring a new insight to ITS but it will take few years for gaining the certain standards for supporting the safety related and non-safety related V2x. However constant research is going on the co-existence of current 802.11p and 4G LTE. As the merged form can create heterogeneous network to provide the best outcome in the coming years as seen in the Figure 1 (Wang *et al,* 2017).

3.3. 5G

The Fifth Generation (5G) is also a 3GPP standard and it is the latest cellular technology to till date that is aimed to increase the speed and responsiveness of wireless network also known as next generation networks. The peak estimated data transfer rate in 5G would be 20Gbps that can even exceed the wired line networks speed. 5G is an unfolding platform whose endeavour is to expand the current technology and introduce novel application platforms with low latency and ultra-reliable communication. In future this technology will bring a plethora of benefits to various infrastructure and different types of industries. The ITS might be the smartest approach that will be used by 5G. By utilizing the introduction of 5G wireless network the ITS infrastructure may perhaps start to deliver us with the real intelligent

cities with the application of ultra-low latency network for real time data transfer between vehicles and transport infrastructure (Wang *et al.*, 2017). Moreover, this technology can enable vehicles to transmit data in real-time to make the vehicular system more safe and secure. 5G wireless network can empower the vehicles to be monitored persistently and managed at the same time by traffic management system to ensure their safety as shown in the above mentioned Figure 1. In coming days, this next generation cellular technology would be mostly suitable for most of the V2x communication (Vinel Wang *et al.*, 2017).

4. Test Measurement scenarios for IEEE 802.11p and 5G Test Network

The main focus of this section will be on the V2I data sharing scenarios using IEEE 802.11p and 5G Test Network. The general aim of 5G Test Network (5GTNF) on test track in Sodankyla is to fill the vacant slot between laboratory based 5G network and beyond commercial network installations and testing environments. It provides trialling support and configurations for tailored infrastructure for communication and scientific and industrial community. Meanwhile, the RWS on our test track offers run time weather updates, traffic accident updates and road friction information collected by different vehicles. RWS gathers the observation data from the nearby vehicles (V2I), to be used in different Intelligent Transport System services and applications. RWS distributes the collective weather data to the vehicles (V2I).

In test measurements, two Road weather stations and a vehicle contributed for V2I data exchange using IEEE 802.11p and 5G Test Network. The vehicle drove in a close loop test track (1.7 km long) composed of two RWS's acting as V2I counterpart. The information exchange between the RWS and vehicle was piloted by using Cohda MK5 radio transceivers, compatible with wireless vehicular communication standard IEEE 802.11p. For the IEEE 802.11p test measurements, the SUNIT F-series vehicle user interface is a primary User Interface (UI) in vehicles but also android tablets are being a possible alternate. For the 5G test network measurements Samsung S7 with the SUNIT F-series vehicle user interface is used. For all test measurements we used Iperf software for sending UDP packets to RWS and for the analysis of IEEE 802.11p and 5G test network we are using Wireshark software.

In the first phase, vehicle sending UDP packets to RWS and collecting RWS data in V2I communication mode, to analyse the performance of a particular network during driving on the test track. RWS broadcasted the up to date road weather data to the vehicles, while driving during the test measurements. The Figure 2 (a, b) is showing the connectivity of IEEE 802.11p and Figure 3 showing the connectivity of 5G test network in our test measurements.

Figure 2. (a) Road Weather Station 1 UDP Packet Capture Range (b) Road Weather Station 2 UDP Packet Capture Range

Figure. 3 5G Test Network UDP Packet Capture Range

The marks shown in yellow colour are indicating the positions where the UDP packets were collected from both RWS1 and RWS2 in V2I setup from vehicle. V2V communication data collection was done with 7-8 drives, each drive was almost of 180 sec long. For test, measurements the vehicles driving to the same direction and going across each other in the track.

5. Performance Analysis of IEEE 802.11p and 5G Test Network (5GTN)

For V2I test measurements and comparison purpose, 7 measurements were sufficient to evaluate and analyze the trend in measurements between the IEEE 802.11p and 5G test network.

During of the average 7 measurements of IEEE 802.11p, we can notice from the Table 1 and Figure 4, the considerable number of packets are lost initially as well as at the end of the test drive. That's one of the reason for the initial message latency because it takes time for the initialization of the

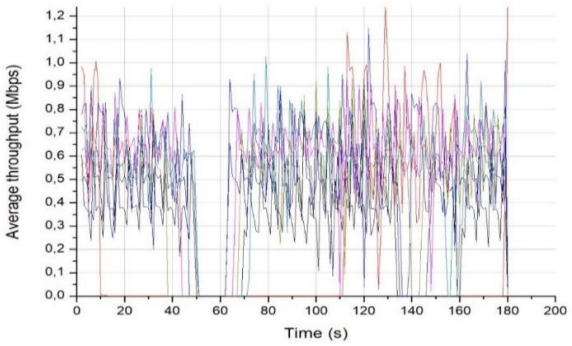

Figure 4. IEEE 802.11p Test Measurements Average Throughput with time

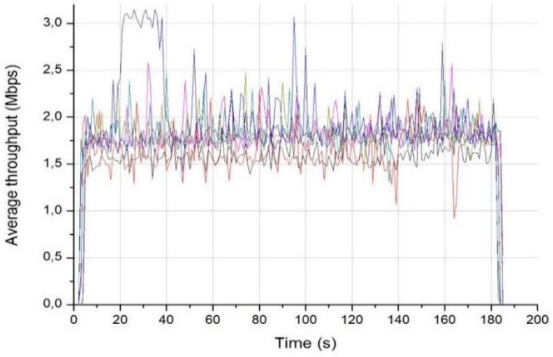

Figure 5. 5GTN Test Measurements Average Throughput with time

connection setup. The initial connection setup in 5G test network takes even more time in comparison of IEEE 802.11p and as a result initial message latency is bit high. Using Iperf and python program the IEEE 802.11p offers data transfer rate of 0.01 second due to obstacles in communication link and 5G test Network has a continuous transmission of packets due to good communication link. The Table 1 also indicates that the jitter also created a difference between IEEE 802.11p and 5G test network because the jitter is quite high in IEEE 802.11p and that can lead to the overall latency. The range of IEEE 802.11p and 5G test network was measured in the test track. It can be seen in the Figure 3 and Figure 5 that the overall coverage, uninterrupted availability and capacity of 5G test network was better than IEEE 802.11p, it can also be seen in the Table 1.

Table 1. Performance Analysis of 802.11P and 5G Test Network

Description	**IEEE 802.11p ((V2I))**	**5 G Test Network (V2I)**
Measurements	7	7
Launched	IEEE in 2010	3GPP (Evolving from 2G-3G-4G-5G)
Tested Frequency Band (GHz)	~5.9	~2.3
Deployment and Scalability	Needs deployment and placement of access points & gateways	Upgraded the existing cellular network infrastructure
Latency (seconds)	0,18	0,65
Data Transfer Rate (s)	0,01	Continuous
Jitter (ms)	14.178	5.20
Average Packet Size (Byte)	925	1510
Average Throughput (Mbit/s)	1,46	5.01
Initial message latency (s)	0,06	0,099
Lost Packet Percentage (%)	20	35.43
Average Packet per Second (s)	693.17	1201.55
Maximum Data Rate (Mbps)	6.664	15

In the Table 1, we can also notice that the lost packets were high in IEEE 802.11p as compared to 5G test network. It perhaps because of the embedded system in our RWS or possibly due to the interruption of long trees in continuous transmission of packets in our test measurements. The IEEE 802.11p performance is immensely sensitive to large vehicle densities, vehicle speed, and heavy traffic

load. It can be seen in the Table 1 and Fig 4, the latency is less in IEEE 802.11p because the IEEE standard is specifically designed for direct communication between vehicles. The latencies with less than 25 milliseconds imitates optimal situation for best vehicular applications i.e. IEEE 802.11p as it can be seen in the Table 1.

The initial message latency in IEEE 802.11p is bit less than 5G test network due to initial connection setup for V2I communication. It might be because 5G test network equipment that is not standardized yet. 5G test network is good in jitter because its high in IEEE 802.11p and high jitter can increase the overall network delay.

The Figure 4, and the Table 1 clearly indicates that the IEEE 802.11p has less data rate and throughput as compared to 5G test network because IEEE 802.11p data rate ranges from 3 Mbps to 27Mbps. Similarly, the average packet per second and average packet size is good in 5G test network in contrast of IEEE 802.11p because of different standards. The Table 1, also indicates that the pilot measurement assessment and investigation gave us 5G as an optimal network with good average throughput. 5G network performance can be a lot better in near future with extensive investigation for its implementation in intelligent traffic system (ITS).

6. SafeCOP Feature Performance Analysis in IEEE 802.11p

In ITS, developers are trying hard to develop an explicit safety layer relating this evidence with safety arguments. The Co-operative Cyber-Physical Systems (CO-CPS) has one of the entity in practice for ITS communication environment (vehicles, Road Weather Station (RWS) and backend systems). Safety for Vehicular Co-CPS systems facilitated by wireless communication technologies is a critical characteristic and needs new design methodologies. SafeCOP (Safe Co-operating Cyber-Physical Systems using Wireless Communication) is a European Union (EU) project that aims to a safety assurance methodology, certifying the secure communication within single Cyber-Physical element, as well as Co-CPS. Finnish Meteorological Institute (FMI) has developed one of the SafeCOP use case for vehicular CO-CPS entity, for vehicle and road weather station interaction. In the SafeCOP project, CO-CPS are furnished with extra safety systems derived from the safety standards as described in the Figure 6 (a, b). In the Fig 6 (a, b), it can be seen that by using the safety layer in SafeCOP, the use case of vehicles and RWS can be piloted in a secure and reliable manner so that the weather service development can trust the unfeigned weather information and the vehicles utilizes RWS service data reliably. The secure latest information can be delivered to the vehicles using different wireless technologies (IEEE 802.11p, 4G (LTE-A), 5G) to avoid vulnerable weather situations and adjust their travelling routes based on weather alerts. The imminent step could be the integration of safety-assured system into the road side infrastructure and road traffic simulations by using IEEE 802.11p and 3GPP latest standards to scrutinize and classify the different aspects of this safety feature (Muhammad *et al.*, 2019).

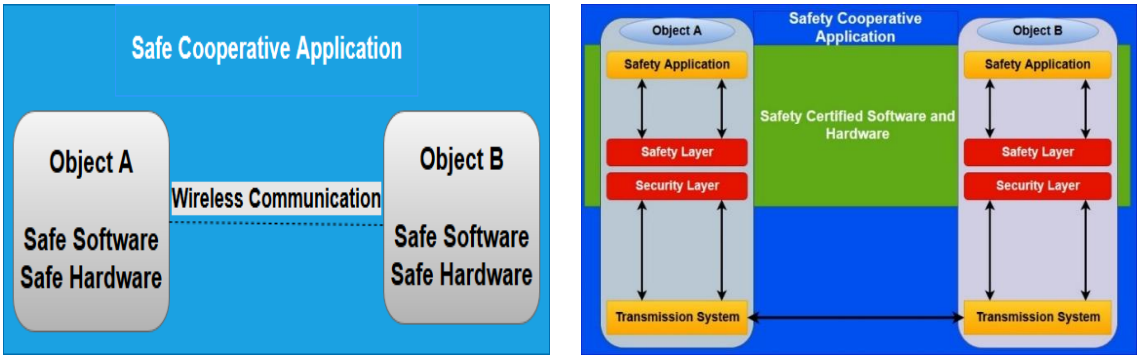

Figure 6. (a) Safety layer Communication Entities in V2I (b) Safety Cooperative Application in V2I

6.1. SafeCOP V2I Communication & Runtime Manager Operation

In the Figure 7, we are presenting V2I communication scenario using SafeCOP feature. The communication processes between vehicle and RWS are defined with green elements, showing different SafeCOP features and functions. In V2RWS communication, the validation processes are introduced in a step-by-step phase to maintain and ensure the safety layer validation. The basic purpose of validation

process is to authenticate the communication entities, so that counterpart did not get any interruption and remains the same throughout the interaction: The validation processes and procedures performed by Run-time-manager are presented in the Figure 7. The SafeCOP safety layer concept is derived from the arsenal of approaches described in EN 50159, i.e. source/destination IDs, time-outs and the time stamps are applied in V2RWS scenario (EN 50159 *et al.*, 2010).

In the safety layer concept, the runtime manager is checking the different entities in V2RWS data exchange, verifying the internal communication. Generally, the safety layer assumes that the information exchange between V2RWS is unsecure and based on this assumption, it produces its own validation and authentication events, i.e. 2 temperature sensors in a parallel process. Consequently, we created the process structures, incorporated with supplementary safety element offered by the SafeCOP utility,

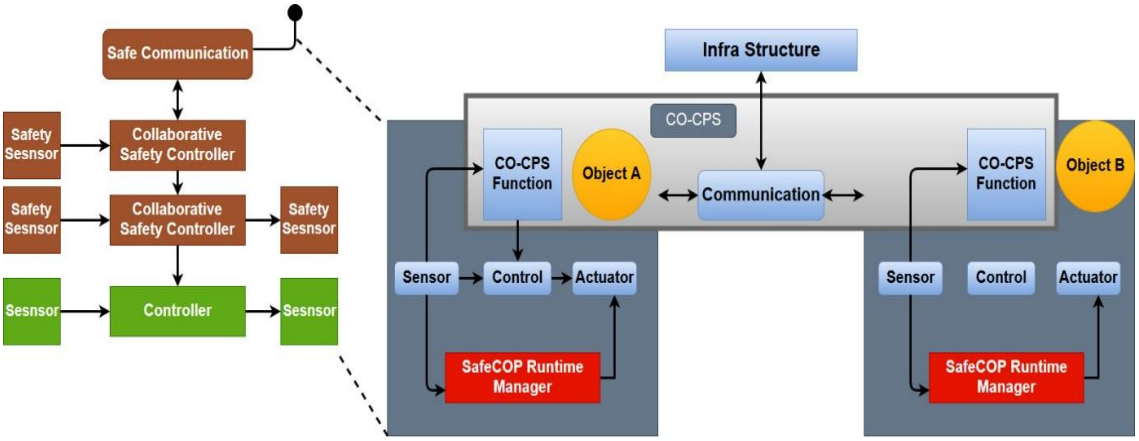

Figure 7. Safety Runtime Manager Concept

combined with the well-defined interface locations. The vehicle and RWS process structures are created in a way that the SafeCOP function and features will be defined as a distinct element. SafeCOP process structure comprised of two communication objects with complete information exchange process and the process structure detail can also be seen in the Figure 7. The aim of the Safety layer process structures explanation in the Figure 7 is to fragment the data exchange procedure into distinct and clear segment, with a probability to investigate, observe and validate the secure communication between V2RWS. The Safety layer process structures explained in the Figure 7 presenting the SafeCOP runtime manager and validation entities individually in green colour. These safety elements representing the initial insertion point(s), where the SafeCOP created entities permitting the secure communication associated to CO-CPS implementation. Runtime Manager in SafeCOP is instigated as a security supervisor for each system, as a distinct computing object.

Table 2. SafeCOP Runtime Manager & Safety layer Validation Objects

Validation Objects	Communication Entities	Validating Sensors/Actuators/Controllers	Sensors/Actuators/Controllers operational description	Validation Technique
Road Surface State	Vehicle	Teconer	Road and friction measurement	Comparison to RWS, Threshold
	RWS	DSC111	Remote road surface state measurement	State Validation
Road Temperature	Vehicle	Teconer	Road and friction measurement	Comparison to RWS, Threshold
	RWS	DST111, 2xDRS511	Remote road surface temperature, State of the surface measurement	Internal Comparison with Thresholds
Air Temperature	Vehicle	Teconer	Road and friction measurement	Comparison to RWS, Threshold
	RWS	2x PT100 (RWS)	Temperature sensor measurement	Internal Comparison with Thresholds.
Road Friction	Vehicle	Teconer	Road and friction measurement	Comparison to RWS, Threshold
	RWS	DRS511, DSC111	State of the surface measurement, Remote road surface state measurement	Temperature Validating Friction thresholds

Safety layer and Runtime manger are working collectively and they are conceptual embedded systems, can't be simply detached from the whole concept and design. Runtime manager is operating as an object continuously observing and monitoring the quality controlling and general functionality of communication data and sensors. Road weather station and mobile friction measurement (Teconer-RCM 411 measuring road temperature, road friction and current state of road) in the V2I set-up comprised of several measurement devices (Co-CPS sensors and actuators) and runtime manager processes this safety critical data. To analyze the efficiency of the system, this data can be used as a reference material with a SafeCOP equipped safety related CO-CPS.

The SafeCOP Runtime Manager/Safety Layer validated and authenticated constraints are listed in the Table 2. For the comparison of sensor, controllers and actuators data from V2RWS (Teconer friction data) is analyzed and compared to standard threshold value. That threshold value is then compared with Teconer sensors/actuators/controllers collected data with highest to the lowest priority.

6.2. IEEE 802.11p Test Measurements and Performance Analysis with & without SafeCOP

The main emphasis of this section will be on the test measurements between Vehicles to Road Weather Station (RWS) data exchange. Vehicles provide road friction data, up to date road weather information to RWS. RWS accumulates and save this observation data collecting from the vehicles (V2I) traveling nearby, to be used in these facilities and services. RWS distributes the collective up to date weather information to the nearby vehicle (V2I). Safe and secure communication is a fundamental feature in this methodology and these V2I scenarios guides us to the solution with collected up to date road weather information and friction data from the vehicles helps to avoid accidents.

For V2I field measurements, two weather stations and a vehicle contributed for test measurements. The vehicle was driving in a closed loop at test track (1.7 km long), comprised of 2 RWS performing as V2I counterpart. The communication between the vehicles and RWS was conducted with Cohda MK5 radio transceivers supporting the wireless IEEE 802.11p vehicular networking standard. Vehicles used SUNIT F-series vehicle PC for user interface (UI) to analyze the performance of IEEE 802.11p. Android tablets can be a possible solution as well depending on our need. In V2I, the road state and road friction data is attained exclusively from the external road friction measurement devices (Teconer RCM 411) installed in vehicles. For transfer of UDP packets, we used Iperf program and for performance analysis of data traffic in V2I mode we used Wireshark.

Initially, the measurement starts on the test track by driving the vehicle and transferring the latest road weather state and friction data in a V2I communication mode. RWS delivered the up to date road weather information to the vehicles, while passing. The outcome of our test measurement is that, we had practically continuous networking during the tests with some natural interruptions.

V2I communication data collection was done with almost 8-9 drives on a test track, vehicle was moving in a clockwise direction and passing the information to the RWS. The time span in seconds presented in the Table 3 showing the time taken to transfer average UDP packets for the test drives.

Table 3. 802.11p with and without SafeCOP feature

Test number	Radio	Jitter (ms)	Time span (s)	Average (PPS) (s)	Average packet size (Bytes)	Average Throughput (Mbps)
1-8	IEEE 802.11p without SafeCOP	51,2899	816.923	578.2	925	4.278
1-8	IEEE 802.11p with SafeCOP	45.624	1021.986	91.9	1031	0.753

In the second phase of IEEE 802.11p measurements, we took measurements in V2I mode having a system armed with a security feature (SafeCOP). Authentication and validation of the objects defined in the Table 2 was considered for analysis. The jitter, time span, average packet per second, average packet size and average throughput of these test measurements is presented in the Table 3. For transfer of UDP packets, we used Iperf program along with python script and for performance analysis of data traffic in V2I mode we used Wireshark. In V2I communication with SafeCOP feature, for vehicle data packets we used very simple data format, just enough to deliver relevant road weather and friction information. We can see that the average throughput in IEEE 802.11p with SafeCOP feature considering V2I mode is quite less than without SafeCOP feature. It might be because of embedded system and lost packets in our vehicular networking measurements. Measurements taken in a closed loop of test track perceptibly leads to positions where the communication link between vehicles and RWS is very low that leads to rapid

fluctuations in the Figure 8. It is because of random obstacles between the V2I as well as 802.11p network degradation can be because of nearby Wi-Fi networks sharing the same 5.9 GHz ISM band.

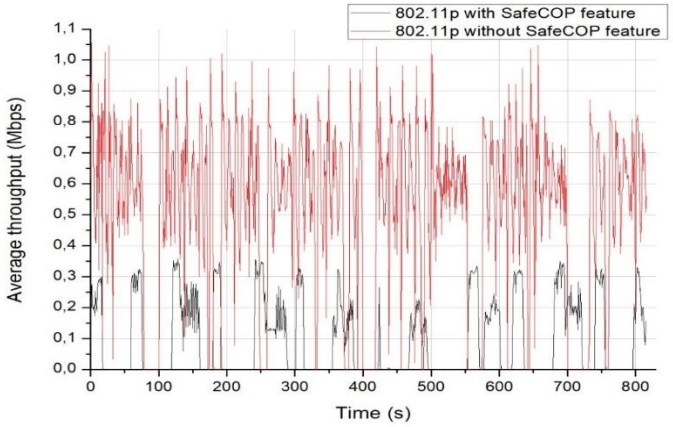

Figure 8. IEEE 802.11p Performance Analysis with & without SAFECOP feature

The performance analysis between IEEE 802.11p with and without safety layer for V2I scenario was piloted by comparing jitter, time span, and average packet/second, average packet size and average throughput. We conducted 8-9 drives for test measurements to compare and analyze the behavior and performance of IEEE 802.11p network with and without SafeCOP. These pilot measurements were sufficient to evaluate and analyze the trend in measurements with and without safety feature. The Figure 8 presenting the weather information for V2I scenario, allowing direct comparison graphs between IEEE 802.11p with and without SafeCOP. The data packet sent from the V2I to the RWS with SafeCOP feature is 1031 bytes that is quite large in contrast to without safety feature in IEEE 802.11p. This might be because of python script combined with Iperf, so that the packet is not fragmented in to different chunks. This fragmentation helps to increase the performance and efficiency of network and it ultimately results in the form of better average throughput of IEEE 802.11p without SafeCOP feature and it can be seen in the above Table 3 and the Figure 8. In the pilot measurements the data packets were sent by using UDP protocol and the UDP protocol is more robust against losing data packets and the loss of a packets can be improved and controlled by the chosen program.

The average throughput is also low with safety feature because of validation process and messages. In the Figure 8 the throughput comparison in V2I with SafeCOP features disabled and enabled can be seen in terms of average throughput.

During the pilot measurements with SafeCOP features, the jitter is bit low but low packets/s that leads to high packets loss at the beginning and at the end of the test drives. The initial message latency in IEEE 802.11p without SafeCOP features is due to the initial connection setup but with safety feature the IEEE 802.11p take a while to establish a connection and that might lead to escalate the lost packets. The average packet/s is also quite high without SafeCOP feature as well as the time span to send UDP packets compared to SafeCOP feature. The average packet/s and time span eventually effects the average throughput and that's the reason the average throughput without safety feature is quite good. The graph shows only the data exchanged between vehicle and RWS.

7. Conclusion

1. In this article, we have made a performance analysis between IEEE 802.11p and 5G test network considering vehicular networking.
2. We have also made a system level performance analysis of IEEE 802.11p with and without safety feature (SafeCOP).
3. In our vehicular communication test scenarios, the jitter is reasonable that satisfies maximum of the application requirements. Because as the load on the network increases (network congestion, inappropriate queuing, number of vehicles), and we experienced an upsurge trend in the delays.
4. As for IEEE 802.11p wireless standard, it offers adequate performance with typical communication frequencies in sparse network typologies with limited mobility coverage as well as the SafeCOP feature influenced the system working efficiency because of embedded computer system in Cohda MK5 radio.

5. The feasibility of IEEE 802.11p with embedded SafeCOP feature evidently offers us the improved results and constant safety assurance model for cooperative systems in contrast of the ordinary systems without security. This safety feature can also be implemented in cellular networks in future.
6. The main goal of this article is to develop and improve the road traffic safety and information security by using heterogeneous networking tailored vehicular environments.
7. Finally, we can conclude that 5G technology offers some benefits over IEEE 802.11p in several aspects but still it need to sometime till its final release.

References

1. Sukuvaara, T., Mäenpää, K. and Ylitalo, R. (2016) Vehicular-networking- and road-weather-related research in Sodankylä. Geoscientific Instrumentation, *Methods and Data Systems*, 5(2), pp.513-520.
2. Tahir, M N. Maenpaa, K and Sukuvaara, Timo. (2019) IEEE C-Code 2019. Evolving Wireless Vehicular Communication System level comparison and analysis of 802,11p, 4G 5G. 48-52.
3. Kim, D., Yeom, I. and Lee, T.-J. (2017) Mitigating tail latency in IEEE 802.11-based networks. *International Journal of Communication Systems*, 31(1), p.e3404.
4. Hameed Mir, Z. and Filali, F. (2014) LTE and IEEE 802.11p for vehicular networking: a performance evaluation. *EURASIP Journal on Wireless Communications and Networking*, 2014(1).
5. Sukuvaara, T., Mäenpää, K. and Ylitalo, R. (2016) Vehicular-networking- and road-weather-related research in Sodankylä. Geoscientific Instrumentation, *Methods and Data Systems*, 5(2), pp.513–520.
6. Balador, A., Kouba, A., Cassioli, D., Foukalas, F., Severino, R., Stepanova, D., Agosta, G., Xie, J., Pomante, L., Mongelli, M., Pierini, P., Petersen, S. and Sukuvaara, T. (2018) Wireless Communication Technologies for Safe Cooperative Cyber Physical Systems. *Sensors*, 18(11), p.4075.
7. Pisano, Paul. (2018) Integrated Modeling for Road Condition Prediction (IMRCP). No. FHWA-JPO-17-602. United States. Dept. of Transportation. Road Weather Management.
8. Vinel, A., Lyamin, N. and Isachenkov, P. (2018) Modeling of V2V Communications for C-ITS Safety Applications: A CPS Perspective. *IEEE Communications Letters*, 22(8), pp.1600–1603.
9. Bissmeyer, N., Van Dam, J.-F., Zimmermann, C. and Eckert, K. (n.d.). *Security in Hybrid Vehicular Communication based on ITS-G5, LTE-V, and Mobile Edge Computing*. [online]
10. Severi, S., Härri, J., Ulmschneider, M., Denis, B. and Bartels, M. (2018). Beyond GNSS: Highly accurate localization for cooperative-intelligent transport systems. www.eurecom.fr, [online] pp.1–6.
11. Vivek, N., et al. (2014) On field performance analysis of IEEE 802.11 p and WAVE protocol stack for V2V & V2I communication. International Conference on Information Communication and Embedded Systems (ICICES2014). *IEEE*, pp. 1-6.
12. Vinel, A., Lyamin, N. and Isachenkov, P. (2018) Modeling of V2V Communications for C-ITS Safety Applications: A CPS Perspective. *IEEE Communications Letters*, 22(8), pp.1600–1603.
13. Wang, M., Winbjork, M., Zhang, Z., Blasco, R., Do, H., Sorrentino, S., Belleschi, M. and Zang, Y. (2017) Comparison of LTE and DSRC-Based Connectivity for Intelligent Transportation Systems. [online] *IEEE Xplore*.
14. Vinel, A., Breu,J., Luan, T.H. and Hu, H. (2017) Emerging Technology For %g-Enabled Vehicular Network kms.shanghaitech.edu.cn,[online] 24(6).
15. Muhammad Naeem Tahir & Kari Maenpaa & Dr.Timo Sukuvaara (2019) Analysis of SafeCOP Features in V2I and V2V Communication. In: *Proceedings IEEE 89th VTS Spring 2019 Kualalumpur Malaysia*.
16. Jan, T. and Lubor, B. (2009) 354567 The Architecture of GNSS Local Elements in Railway Safety Related Applications Safety, Technical Session). The Proceedings of International Symposium on Seed-up and Service Technology for Railway and Maglev Systems : *STECH*, 2009(0), p._354567-1_-_354567-5.