CONTENTS

Message from the MMTC Chair ................................................................. 2

SPECIAL ISSUE ON FUTURE OF THE CONNECTED VEHICLES ............. 3

Guest Editor: Syed Hassan Ahmed ......................................................... 3
Georgia Southern University, USA .......................................................... 3
sh.ahmed@ieee.org .................................................................................. 3

Unmanned Aerial Vehicles as Mobile Roadside Units in Vehicular Environments 4
Carlos T. Calafate, Juan Carlos Cano ..................................................... 4
Department of Computer Engineering, Universitat Politècnica de València, Spain 4
calafate@disca.upv.es, jucano@disca.upv.es ............................................ 4

Named Data Networking for Connected Autonomous Vehicles: ............... 7
Marica Amadeo, Claudia Campolo, Antonella Molinaro .......................... 7
University “Mediterranea” of Reggio Calabria, DIIES Department ........... 7
{marica.amadeo, claudia.campolo, antonella.molinaro}@unirc.it ............... 7

Multi-access Edge Computing for Connected Vehicles .......................... 11
Celimuge Wu, Tsutomu Yoshinaga, Xianfu Chen, and Yusheng Ji ............... 11
Graduate School of Informatics and Engineering, The University of Electro-Communications ................................................................. 11
VTT Technical Research Centre of Finland .............................................. 11
Information Systems Architecture Research Division, National Institute of Informatics .......................................................... 11
{celimuge, yoshinaga}@uec.ac.jp, xianfu.chen@vtt.fi, kei@nii.ac.jp .......... 11

Predicting Vehicular Collisions in Vehicle-to-Vehicle Networks Using Physical Layer Techniques .......................................................... 15
Billy Kihei ................................................................................................. 15
ReachRF LLC ......................................................................................... 15
billy@reachrf.com .................................................................................. 15

Real-Time Computing, Connectivity and Communications for Secure Mobile Transportation Cyber-Physical Systems ........................................ 19
Danda B. Rawat1 and Chandra Bajracharya2, Guy Lingani1 and Sunitha Safavat1 ........ 19
1Data Science and Cybersecurity Center (DSC2), Department of Electrical Engineering & Computer Science Howard University, Washington DC, USA ........ 19
2Department of Electrical Engineering, Capitol Technology University, USA ........ 19
Contact Email: db.rawat@ieee.org .......................................................... 19

MMTC OFFICERS (Term 2018 — 2020) ...................................................... 28
Message from the MMTC Chair

Dear MMTC colleagues and friends,

It is my great honor to serve as MMTC Vice Chair for 2018~2020 term. I would like to wish all of you and your families a very Happy New Year 2019 on behalf of all the MMTC officers. May this year bring you all health, happiness, and prosperity.

I would like to take this opportunity to thank our editorial teams of MMTC Frontiers led by Dalei Wu. MMTC Frontiers provides a timely update on recent developments, hot research topics, and society news in the area of multimedia communications. With the great contribution of Dalei Wu, Danda Rawat, Kan Zheng, Melike Erol-Kantarci, Rui Wang and other editors, the Frontiers is delivering high-quality publications.

I would also like to take this opportunity to thank those who were able to attend the MMTC meeting at Globecom 2018. The Communication Software, Services and Multimedia Applications Symposium (CSSMA) at Globecom and ICC is sponsored by MMTC and I encourage all of you to continue to be actively involved in CSSMA and submit papers there. The next CSSMAs will be at ICC 2019 in Shanghai, China in May 20-24, 2019 and we hope to see you all here.

The MMTC officers would like to encourage members to be actively involved in the TC as well as help recruit new members. Membership is open to all those who are interested, and more information can be found at the TC website, http://mmc.committees.comsoc.org. MMTC provides members the opportunity to actively serve the community by submitting nominations for associate editorship to journals, special issue proposals, conference chairs, and ComSoc distinguished lecturers.

I would like to take this opportunity to invite all of you to attend the MMTC meeting in IEEE ICC 2019 and ICME 2019, both of which will be held in Shanghai in May and July, respectively. I am a main organizer of IEEE ICME 2019. We will review the MMTC activities with recent updates at the meeting. I look forward to seeing you all soon in May and July 2019.

Have a wonderful holiday season. I wish you all the best!

Jun Wu
Vice Chair, Multimedia Communications Technical Committee (2018-2020)
IEEE Communications Society
This special issue of MMTC Frontiers focuses on the research advancements in the connected vehicles and its applications. It is worth noticing that there are various research projects and activities regarding the connected vehicles and we can easily foresee the developments in the near future.

The first paper presents forwarding schemes for the connected vehicles aided with Named Data Networking. Moreover, the authors have also emphasized on the difference between unicast and broadcasting of the Interest packets.

The authors in second paper envision the integration of sub-6 Ghz band, 802.11p, and mmWave communications for enabling Vehicular Networking. In the proposed architecture, Internet connectivity is insured to the vehicles by the vehicles (aka moving gateways) with higher throughput. To bring more efficiency, the authors also used fuzzy logic algorithm to select cluster heads (gateways) among the given neighboring vehicular nodes.

The third paper introduces an interesting idea of using unmanned aerial vehicles (UAVs) as a mobile roadside units. Such roadside units are beneficial to provide connectivity to the wheels on the road at some random points as well as at the most popular areas to avoid congestion.

The fourth paper in this special issue focuses on the utilization of physical layer properties of vehicular connectivity to predict collisions. The author has identified unique techniques to make a proper use of such properties to provide safety applications.

The fifth and final paper focuses on a typical framework for transportation cyber physical systems with its different components for connected vehicles. Authors have presented computing, connectivity, communications requirements for resilient transportation cyber physical systems by considering different parameters such as channel sensing and identifying time, association time, security run time, vehicle density, vehicle speeds, communication range, data rate and size.

Syed Hassan Ahmed (SM’18) is an Assistant Professor in the Department of Computer Science at Georgia Southern University, Statesboro, USA. He is also leading Wireless Internet and Networking Systems (WINS) lab. Previously, he was a Post-Doctoral Fellow in the Department of Electrical and Computer Engineering, University of Central Florida, Orlando, USA. He completed his bachelor’s in computer science from Kohat University of Science & Technology (KUST), Pakistan and Master combined Ph.D. Degree from School of Computer Science and Engineering (SCSE), Kyungpook National University (KNU), Republic of Korea (South Korea). In summer 2015, he was also a visiting researcher at the Georgia Tech, Atlanta, USA. Overall, he has authored/co-authored over 150 international publications including Journal articles, Conference Proceedings, Book Chapters, and 03 books. In 2016, his work on robust content retrieval in future vehicular networks lead him to win the Qualcomm Innovation Award at KNU, Korea. Dr. Hassan's research interests include Sensor and Ad hoc Networks, Cyber-Physical Systems, Vehicular Communications, and Future Internet. He is currently the Member of Board of Governors and IEEE VTS liaison to IEEE Young Professionals society. From the year 2018, he is also an ACM Distinguished Speaker.
1. Introduction

Vehicular networks are currently a hot research topic due to their expected growth in the coming years. By equipping vehicles with on-board units (OBUs) acting as network nodes [1], these connected vehicles can address new challenges related to safety, efficiency, and infotainment. In these environments, communication issues arise due to the high number of networks nodes involved, and due to signal obstruction caused by buildings and other urban artifacts [2]. Unmanned Aerial Vehicles (UAVs), also known as drones, are semi-autonomous or fully autonomous unmanned aircrafts that have embedded sensors, cameras and communication equipment. Originally, UAVs were deployed for military applications. Nowadays, they are being deployed to assist in emergency situations such as search and rescue or disaster scenarios, where they can act as supporting nodes for communications since they can be deployed on demand, and can benefit from a wider communications range, as UAVs have better line-of-sight (LOS) features than ground infrastructures. In addition, UAVs can form a Flying Ad-hoc Network (FANET) [3] to relay information. Combining UAVs and vehicles emerges as an interesting and novel topic with multiple applications in the Intelligent Transport Systems (ITS) area, including remote sensing and disaster assistance operations [4], where UAVs can be used to send warnings to drivers about unexpected danger, or even regulate traffic. This can be especially useful in catastrophic areas, or in areas with minimal or null cellular coverage, where the strategical placement of a few UAVs can quickly reverse the situation.

Moreover, UAVs can enhance the communications between ground vehicles in the scope of ITS applications [5], or they can even be deployed to assist vehicular networks as store-carry-forward nodes [6]. Differently from vehicles that move on the ground, following well-known established routes, UAVs can move freely in a three-dimensional space. Hence, their mobility is not restricted to road layouts or to a two-dimensional space, whether moving randomly as a single UAV or as a UAV swarm [7]. In situations where the communications rely on both UAVs and ground vehicles, their performance can be affected by diffraction from mountains, or by blockage by hilly terrains that will hence experience signal attenuation [8].

Authors in [9] have conducted extensive simulations to verify the existence of an optimal UAV altitude, and a minimum number of UAVs to guarantee a target connectivity among vehicles. More efforts include creating an inter-connectivity for a disconnected group of cars using UAVs as relays [10], or analyzing the vehicle-to-drone packet delivery delay in VANETs [11]. However, all these researchers performed their experiments using a flat scenario, thus neglecting 3D communication effects.

Hence, there is a need to further investigate on solutions for vehicular networks using UAV-based wireless access in real, challenging scenarios characterized by irregular terrains. This work provides some insight on this topic by proposing, deploying and testing an UAV-based content delivery architecture for vehicular environments.

2. UAVs as Mobile Roadside Units

In this section, we describe an architecture that relies on UAVs to achieve a resilient content delivery solution in vehicular environments.

The envisioned target scenario is one where an infrastructure element is constantly broadcasting some specific content, which can be any sort of multimedia file(s), to vehicles passing by. In our proposed architecture, this content is encoded using RaptorQ. In a previous study [12] it was shown that RaptorQ is indeed a very efficient FEC scheme, and allows a potentially limitless sequence of encoding symbols to be generated. This way, we are able to seamlessly scale content delivery to any number of vehicles in a resource-efficient manner. Within vehicles, the content is received by the driver's smartphone, and the multimedia content is then decoded and played back automatically, without requiring user intervention. Examples of the applicability of our solution includes: (a) location-based security warnings, and (b) touristic advertisements.
Figure 1. Drone-based deployment approach.

Our work differs from the standard approach in that we do not rely on any static infrastructure. Instead, we have a mobile infrastructure element (see Figure 1). We equip Unmanned Aerial Vehicles (UAVs) of the multirotor type with a Raspberry Pi-based broadcasting unit, so that they can become highly flexible and mobile infrastructure elements. The UAVs rely on the ad-hoc wireless networking paradigm to connect to vehicles using the 5.8 GHz band. Since most smartphones do not support this mode of operation, each vehicle is equipped with an on-board unit offering ad-hoc communications at this frequency band. The on-board unit acts as an information relay, conveying the received information to the smartphone on the vehicles by creating a WiFi hotspot in the 2.4 GHz band. The smartphone will receive the RaptorQ-encoded information, playing it back upon successful decoding.

To determine the benefits of UAVs as mobile roadside units in challenging environments, we performed real experiments in a highway located near the municipality of Casinos, Spain, which is characterized by a moderately irregular terrain features causing signal blockages. In addition, UAVs will be used to perform content broadcasting at different altitudes, allowing us to assess the improvements that can be achieved in terms of content delivery efficiency in the presence of such irregular terrain features.

Table 1. Data, time and distance for different altitudes.

<table>
<thead>
<tr>
<th>Altitude (m)</th>
<th>Data (MB)</th>
<th>Time (s)</th>
<th>Distance (m)</th>
<th>Average data rate (kbit/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>0.2</td>
<td>21.68</td>
<td>550</td>
<td>9.7</td>
</tr>
<tr>
<td>25</td>
<td>0.78</td>
<td>74.12</td>
<td>2000</td>
<td>11.0</td>
</tr>
<tr>
<td>60</td>
<td>5.11</td>
<td>231.2</td>
<td>6300</td>
<td>23.2</td>
</tr>
<tr>
<td>90</td>
<td>10.26</td>
<td>285.81</td>
<td>7600</td>
<td>37.64</td>
</tr>
</tbody>
</table>

Table 1 summarizes the results from our experiments, which are further detailed in our upcoming IEEE Internet Computing magazine article [13]. They clearly highlight that standard RSUs, located at about 5 meters above ground, experience a very low coverage range, which will severely limit the size of the contents that can be delivered to vehicles when the terrain is irregular. On the contrary, if relying on UAVs, and flying them at an altitude of 90 meters, the size of the contents to be delivered can benefit from a 50-fold increase, as the coverage range is about 15 times greater; this occurs because terrain obstacles no longer represent significant obstructions to the broadcasted signal, being line-of-sight conditions available most of the time.

3. Conclusion

In this paper, we have proposed an architecture that relies on UAVs as mobile roadside units in vehicular environments, and we studied the performance of this architecture in terms of content delivery effectiveness in a real vehicular testbed. To this aim, our approach adopted a FEC scheme based on RaptorQ to encode contents prior to their broadcasting, which ensures that the data to be transmitted will be received correctly on all devices, even in the presence of channel losses, thereby achieving seamless data integrity.

Tests performed in a road environment with irregular terrains and high vehicular speeds (100 km/h) showed that having a mobile infrastructure deployment based on UAVs can significantly boost content delivery effectiveness compared to static infrastructure deployments since it becomes possible to locate the transmitter at a high altitude (90
meters), a situation that is able to substantially increase the coverage range, and in achieve a 50-fold increase on the size of the contents that can be delivered successfully to vehicles passing by.

References

Carlos T. Calafate is a full professor in the Department of Computer Engineering at the Technical University of Valencia (UPV) in Spain. He graduated with honors in Electrical and Computer Engineering at the University of Oporto (Portugal) in 2001. He received his Ph.D. degree in Informatics from the Technical University of Valencia in 2006, where he has worked since 2002. His research interests include ad-hoc and vehicular networks, UAVs, Smart Cities & IoT, QoS, network protocols, video streaming, and network security.

Juan-Carlos Cano is a full professor in the Department of Computer Engineering at the Technical University of Valencia (UPV) in Spain. He earned an MSc and a Ph.D. in Computer Science from the UPV in 1994 and 2002, respectively. From 1995-1997 he worked as a programming analyst at IBM's manufacturing division in Valencia. His current research interests include Vehicular Networks, Mobile Ad Hoc Networks, and Pervasive Computing.
1. Introduction

The recent advancements in the fields of sensing, computing, communication and networking technologies in the automotive and telecom industries are driving the shift towards more connected autonomous vehicles. Thanks to vehicle-to-everything (V2X) communication technologies, vehicles will be able to interact among each other, with nearby entities, e.g., traffic lights, pedestrians, other vulnerable road users, the roadside infrastructure, edge nodes, and remote entities such as cloud servers and Internet facilities, as shown in Fig. 1. V2X connectivity would overall increase the driving and traveling experience, by enabling a plethora of applications, ranging from safety and traffic efficiency to infotainment and, more recently, cooperative and automated driving. First, localized V2X communications can improve the vehicle’s perception of the surrounding environment and can help it to make more informed decisions, instead of relying only on its onboard, although sophisticated, sensors (e.g., radar, LIDAR, cameras, GPS). As a result, hazard warnings would be promptly disseminated and fatalities on the road reduced, while making transportation safer and smarter. Moreover, connectivity to remote facilities would allow web browsing, files/apps download, social media access, and video streaming for passengers; the access to such applications is considered a “must-have” for new cars, and would become even more relevant with increased penetration of autonomous vehicles, in which also the driver may be engaged in media consumption.

V2X applications foresee the exchange of a big amount of data with different features (e.g., packet size and generation frequency, message dissemination scope) and requirements (e.g., latency, throughput, reliability) among heterogeneous entities. Moreover, communications need to be established under fast-varying and harsh wireless propagation conditions, and possibly intermittent and poor connectivity in rapidly changing network topologies. All in all, such a complex landscape entails the design of novel and potentially disruptive communication and networking technologies.
communicating entities are interested in retrieving content (e.g., road congestion information, weather conditions) regardless of the identity of the node(s) producing it; (ii) most of the content has a spatial and/or temporal scope and validity, and (iii) caching data can help to cope with intermittent vehicles’ connectivity. This work focuses on the role of the forwarding strategy deemed as a crucial component of the NDN paradigm when applied in the V2X context. Related literature is shortly scanned, which addresses the relevant issues, i.e., if, where, when, and how forwarding NDN packets, together with the transmission mode decision (broadcast, unicast) and the priority management.

2. Vehicular NDN Forwarding Strategy
NDN nodes in general, and Vehicular NDN (V-NDN) nodes in particular, maintain three data structures at the Data FPlane, namely: (i) the Content Store (CS), used to cache incoming Data packets, (ii) the Pending Interest Table (PIT), to maintain a soft state about the forwarded Interests that are not consumed by the Data yet, and (iii) the Forwarding Information Base (FIB), used to forward the Interests, see Fig. 2 (right). In particular, each FIB entry may include multiple outgoing interfaces per each named prefix. To cope with the shared wireless medium, while maximizing the probability of content sharing between neighbors, the V-NDN forwarding strategies designed in related works mainly focused on the controlled Interest broadcasting over the IEEE 802.11 interface [4], [5]. Indeed, 802.11 was considered the de facto standard for short-range vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, until a few years ago, when its supremacy was questioned by the novel C-V2X technology. Basically, at the Interest reception, a vehicle first checks in the CS for a matching Data packet to send back. In case of failure, it looks for a matching in the PIT to check if there is an equal Interest packet still pending. If also this check fails, the vehicle has to decide if broadcasting the packet again or not, and if yes, when. Different mechanisms have been deployed to decide if a node can elect itself as forwarder. For instance, in [4] candidate forwarders are only the vehicles that have maximum connectivity time and good link quality with the consumer. In [5], instead, eligible forwarders are only the vehicles in the path towards the data producer, as discovered during a preliminary flooding stage. The eligibility decision is usually coupled with an overhearing mechanism to further limit the packet collisions and the redundancy. A defer time is calculated before each Interest transmission: if the same packet is overhead during the waiting time, the transmission is canceled.

In addition to the decision concerning the timing transmission over the IEEE 802.11 interface, which has been the most investigated V-NDN topic so far, other additional aspects should be considered in the forwarding strategy design:
1. The forwarding strategy must differentiate the delivery of Interest/Data relevant to different V2X applications, e.g., traffic congestion notifications need to be promptly disseminated, while file sharing applications can tolerate longer delays. So far, however, the content type of vehicular applications has not been considered as an input to the NDN forwarding strategy: in the vanilla NDN implementation all vehicles apply the same forwarding rules to all NDN packets.
2. The majority of solutions proposed in the literature relies on broadcasting of Interest and Data packets, however, it could not be the most appropriate choice under some circumstances, and also unicast transmissions should be considered.
3. A few efforts have been devoted to the design of mechanisms for the selection of the best interface(s) where to forward packets: this is conversely an issue considering the multiple radio access technologies (RATs) available on board of recently manufactured vehicular devices, besides 802.11 (e.g., C-V2X, LTE, and

Fig. 2: V-NDN stack and main data structures.
IEEE COMSOC MMTC Communications - Frontiers

In the following, the literature addressing the aforementioned issues is shortly scanned.

2.1. Priority-based forwarding

The Medium Access Control (MAC) layer of the IEEE 802.11p standard defines a prioritization mechanism based on four access categories (ACs), with fixed priority given to voice over video over best effort over background traffic, regardless of the application-layer requirements. This mechanism, where packets of the same AC cannot receive differentiated treatment, is ossified and inadequate for V2X applications. For instance, video packets reporting a congestion event must be prioritized over video packets of an entertainment application.

The V-NDN forwarding strategy, instead, can be designed to closely meet the requirements of vehicular traffic and complement the traffic differentiation capability provided at the MAC Layer.

The work in [6] first argues that hierarchical NDN namespaces should have a globally understood prioritization value that must be used as input in the forwarding decision. The work in [7] leverages this design principle and uses two main name prefixes, /high and /low, to identify the content priority and set accordingly the logic for the defer time calculation before (re)-broadcasting the packet. Specifically, two distinct and adjacent time windows are defined: the Data Defer Window (DDW) and the Interest Defer Window (IDW). Data can be transmitted by randomly calculating a defer timer in the range [0, DDWmax], while Interests can be transmitted in the next time window by randomly calculating a defer timer in the range (DDWmax, IDWmax), to give Data priority over Interests. In addition, to let high-priority Data/Interest packets be prioritized over low-priority ones, DDW and IDW are split into two disjoint sub-windows. In the first sub-window, only high-priority Data/Interests can be transmitted, with a timer randomly chosen in that interval, while low-priority packets are delayed to the second sub-window. The mechanism does not introduce additional overhead: vehicles autonomously compute the timers in a totally distributed way, being also agnostic about the network topology. Moreover, being decoupled from the underlying MAC layer technology, the approach could be easily re-engineered to work for localized V2V transmissions over the PC5 interface of the C-V2X technology [1].

2.2. Unicast Vs. Broadcast forwarding

In [8] a unicast-based forwarding protocol is proposed to avoid the broadcast-related issues of packet redundancy and unreliability due its unacknowledged mode. A controlled flooding is enforced to discover the content source, followed by unicast transmissions of Interest and Data packets according to information about the next-hop stored in the FIB. The solution promptly falls back to broadcast to find a new content provider/next-hop in case of a link failure notified by the MAC layer. This hybrid approach prevents unicast forwarding to suffer from frequent link breakages in highly dynamic vehicular topologies. The benefits of an adaptive context-aware approach adequately combining unicast and broadcast forwarding are also advocated in [9]. Such an approach should be enforced according to application demands and topology dynamics: unicast has to be preferred under high-density road settings, where topology dynamics are not so high, whereas broadcast should be pursued for low-latency safety data dissemination.

2.3. Multi-RAT transmission

The work in [10] first selects the outgoing interface(s) for NDN packets according to the priority of Interest/Data packets, tracked in the content name, as proposed in [7]. More in detail, Interests for low-priority contents are forwarded only over the 802.11 interface. High-priority contents are forwarded by consumers according to a parallel forwarding strategy, i.e., the Interest is simultaneously forwarded on both the 802.11 and long-range cellular interfaces. This is to ensure the low latency and reliable delivery of such sensitive data. Vice versa, vehicles acting as forwarders may decide, according to their own user-defined preferences (e.g., monetary costs), whether to use only the IEEE 802.11 face or also apply the parallel strategy. In case the cellular face is not available for a forwarding vehicle, it can only forward the Interest over the IEEE 802.11 face. The multi-RAT approach in [10] could be extended to the forwarding over 802.11 and PC5 interfaces.

3. Conclusions

In this paper, we discussed the main decisions to be taken by the forwarding strategy of V-NDN nodes. Under such a perspective, representative research efforts have been shortly summarized. The conducted analysis emphasizes the need to treasure such pioneering achievements and to further investigate the topic. The design of more sophisticated priority-based multi-RAT forwarding algorithms is advised to make the best of upcoming V2X communication technologies evolving towards 5G systems and to properly accommodate the increasingly demanding requirements of heterogeneous V2X applications.

http://www.comsoc.org/~mmc/
References

Marica Amadeo is a Postdoc researcher at University Mediterranea of Reggio Calabria, Italy. She received a Bs Degree (2005) and a Ms Degree (2008) in Telecommunications Engineering from the University Mediterranea of Reggio Calabria, and a Ph.D. degree in 2013 from the same University. Her major research interests are in the field of information-centric networking, Internet of Things and wireless ad hoc networks. She served as a reviewer for several international conferences and journals. She also received a best reviewer award by IEEE Communications Letters in 2014 and 2015 and a Best Paper Award nomination at NOF 2011. Contact her at marica.amadeo@unirc.it or marica.amadeo@gmail.com

Claudia Campolo is an Assistant Professor of Telecommunications at University Mediterranea of Reggio Calabria, Italy. She received a Laurea degree in Telecommunications Engineering (2007) and a PhD degree (2011) from the same University. In 2008 she was a visiting PhD student at Politecnico di Torino and a DAAD fellow at University of Paderborn, Germany in 2015. Her main research interests are in the field of vehicular networking, 5G, future Internet architectures. She has received three best paper awards for research in the vehicular networking field and the IEEE ComSoc EMEA Outstanding Young Researcher Award in 2015. She is involved in the organization of many international conferences and she gave tutorials in many IEEE conferences. She was co-editor of the book “Vehicular ad hoc network: standards, solutions and research”, Springer-Verlag 2015, and Guest Editor for special issues on the topic of vehicular networking. Contact her at claudia.campolo@unirc.it

Antonella Molinaro is an Associate Professor of Telecommunications at the University Mediterranea of Reggio Calabria, Italy, and since 2018 she is also a professor at CentraleSupélec, France. She was with the University of Messina (1998-2001) and the University of Calabria (2001-2004) as an assistant professor; with the Polytechnic of Milano as a research fellow (1997-1998); and with Siemens A.G., Munich, Germany as a CEC fellow in the RACE-II program (1994-1995). She graduated in Computer Engineering (1991) at the University of Calabria, received a Master degree in Information Technology from CEFRIEL/Polytechnic of Milano (1992), and a Ph.D. degree in Multimedia Technologies and Communications Systems (1996). Her research mainly focuses on vehicular networks, 5G, information-centric networking. She was co-editor of the book “Vehicular ad hoc Networks: Standards, Solutions, and Research”, Springer, 2015; tutorial instructor and invited speaker on the topic of vehicular networks in several conferences. Contact her at antonella.molinaro@unirc.it
1. Introduction
With the emergence of various vehicular Internet of Things (IoT) applications, such as camera sensor data exchange, driving behavior analysis, speech recognition, real-time traffic information update, and software downloading, a new architecture that can achieve ultra-low delay and high throughput is highly required. The current wireless communication technologies show their incompetence in the throughput performance due to the following two reasons. Firstly, the vehicles could be deployed in a highly dense manner at some urban road segments. Secondly, for rural areas, the current technologies are not designed to support a large number of user terminals. In cellular networks, the spectrum efficiency drops drastically along with the increase of the user density. The vehicular mobile edge computing (MEC) can satisfy this need as it conducts the computational tasks and data caching near the end users, such as the passengers and the pedestrians, by integrating the communication and computational capability of vehicles on the road. In this article, we introduce a vehicular MEC architecture that integrates different types of wireless communication technologies.

The use of millimeter wave (mmWave) communications is considered to be one of the main approaches to improve the throughput in 5G. However, there are several challenges to deploy mmWave in vehicular networks. First, mmWave requires a line-of-sight transmission path between the sender and the receiver. Although unlicensed 60GHz mmWave communications can provide up to 2.5Gbps for 1.7Km, the real transmission range in vehicular networks would be much lower as many obstacles such as other vehicles and buildings could block the signals. Second, a directional transmission technology, specifically directional antenna or beamforming, is required to overcome pathloss. The sender node needs to know the information (position etc.) of the receiver in order to design efficient beamforming. The corresponding information can be exchanged with Sub-6 GHz communications which are promising to provide larger transmission range and seamless connectivity.

The main drawback of Sub-6 GHz communications is the limited bandwidth as compared to mmWave. Sub-6 GHz communications include licensed infrastructure-based communications and unlicensed distributed communications. The benefit of using licensed Sub-6 GHz spectrum is the large coverage, and the possibility to ensure strict quality-of-service (QoS) provisioning. IEEE 802.11p [14] is the default standard for distributed vehicle-to-vehicle (V2V) communications. Vehicular ad hoc networks (VANETs) utilizing IEEE 802.11p have attracted tremendous attentions in recent years. In addition to safety applications which can be achieved by V2V communications, VANETs could also be an important part of vehicle-to-cloud communications by integrating IEEE 802.11p-based V2V with other communication technologies.

The integration of Sub-6 GHz with mmWave communications becomes a necessity to ensure QoS in vehicular networks. Recent works on V2V communications mainly focus on the use of IEEE 802.11p or mmWave V2V communications [4][16][1]. There are some studies on collaborative downloading through combining LTE with IEEE 802.11p [18]. However, the integration of licensed Sub-6 GHz, IEEE 802.11p, and mmWave communications has not been extensively in the recent studies. There are two main technical obstacles for the integration of these three communication technologies. Firstly, the selection of gateway nodes should take into account the overall network performance which is determined by both the allocated licensed Sub-6 GHz bandwidth and the V2V throughput. Secondly, the route creation from a vehicle to a gateway is challenging due to the vehicle mobility and the varying node density. The vehicle mobility and inter-vehicle wireless link quality should be taken into account in the selection of the cluster head nodes. For certain hours or road segments, vehicles are densely deployed, and the number of concurrent sending nodes can thus be huge. In IEEE 802.11p, the increase in the number of sending nodes leads to the performance degradation due to the exponential backoff based contention scheme at the MAC layer. Therefore, an efficient information exchange protocol is important for disseminating required control messages with limited bandwidths.

In this article, we first introduce a vehicular MEC architecture that utilizes the computation capability of vehicles, and
IEEE COMSOC MMTC Communications - Future of the Connected Vehicles

then introduce a cluster-based communication protocol by integrating licensed Sub-6 GHz band, IEEE 802.11p, and mmWave communications for the multi-access edge computing in vehicular networks [19]. The protocol employs IEEE 802.11p to exchange control messages among vehicles, and uses mmWave communications to provide high throughput connections to vehicles. We employ a fuzzy logic-based algorithm [20] to select efficient cluster head nodes by taking into account the vehicle velocity, the vehicle distribution, and the antenna height. The clusters are generated in a distributed way with low overhead, which ensures that the required information can be exchanged through IEEE 802.11p link.

2. Multi-access Edge Computing for Connected Vehicles
2.1 Multi-access edge computing architecture
To meet the rapidly increasing need of latency-sensitive vehicular IoT applications, a MEC architecture that can provide an ultra-low latency and high bandwidth is required. Here, we introduce a hierarchical vehicular multi-access edge computing architecture that efficiently utilizes the computational resources of vehicles to perform MEC in order to provide better QoS to end users. As shown in Fig. 1, three different types of communications, namely licensed Sub-6 GHz, IEEE 802.11p, and mmWave, are utilized for information exchange. We define two different types of vehicle edges specifically tier-1 edges and tier-2 edges. Tier-1 edges are used to conduct content caching, data aggregation, and data analysis (such as video analytics). Tier-2 edges are connected to the BS through tier-1 edges. By performing data caching and data aggregation at the Tier-1 edges, a more efficient use of the wireless resources can be achieved. A vehicle edge works either as a tier-1 or tier-2 edge depending on the surrounding environment including available wireless resources and node density.

![Fig. 1 Multi-tier vehicular edge.](image)

2.2 Communication problem definition and protocol overview
We consider the problem of sending data from the cloud to vehicles. More specifically, the problem can be simplified as the transmission from a licensed Sub-6 GHz BS to vehicles. We utilize one-hop mmWave communications while the multi-hop mmWave communication is considered to be impractical due to the complexity of establishing a long path for mmWave communications.

In the protocol, as shown in Fig.2, instead of each vehicle connecting to a BS, only the gateway vehicles utilize Sub-6 GHz interface and communicate with other vehicles through mmWave V2V communications. Control messages are exchanged with IEEE 802.11p V2V communications. The IEEE 802.11p V2V communications could be multi-hop, and could be used for data (content) exchange depending on the network conditions. The gateway nodes are selected using a fuzzy logic-based algorithm considering vehicle mobility, vehicle distribution, and antenna height. The fuzzy logic algorithm ensures that the selected cluster head nodes are stable. The number of gateway nodes is tuned by an adaptive algorithm according to the bandwidth of licensed Sub-6 GHz communication, the node density, and the quality of V2V links.
2.3 Distributed edge (cluster head) selection based on IEEE 802.11p V2V communications

We use an approach where cluster heads are selected in a distributed way. Cluster joining/leaving procedure is conducted with low overhead as we do not use any cluster joining/leaving messages for the maintenance of cluster member information. After cluster heads being determined, each cluster head announces the number of cluster members using the hello messages. We evaluate the suitability of a vehicle acting as cluster head by using a fuzzy logic-based approach. In the evaluation, we take into account three different factors: 1) the moving speed of vehicles, 2) the density of vehicles that are moving toward the same direction as the current vehicle, and 3) the antenna height. The first two factors are used to ensure that the generated cluster heads are stable. The third factor is to fully utilize mmWave communications as high antenna height could improve the line-of-sight distance. We use a fuzzy logic-based approach for the evaluation by combining these three factors.

The cluster heads are selected based on the information shared with hello messages. Each node attaches the information about its velocity and antenna height information. Upon reception of a hello message, each node calculates a competency value (in other words, the value for being a cluster head) for itself and each one-hop neighbor. The node that has the largest competency value in its vicinity declares itself as a cluster head using hello messages.

We generate the cluster heads by considering the connectivity between cluster heads. Each node calculates a competency value for its neighbors which are within the range of $R_{\text{ref}}$ which is smaller than $\frac{R}{2}$ where $R$ is the average transmission range for IEEE 802.11p V2V communications in meters. $R$ is determined by the wireless transceivers installed at vehicles. A vehicle declares itself as a cluster head if its competency value is the largest in the $\frac{R_{\text{ref}}}{2}$ region. This means that there would be at least two cluster head vehicles at $R_{\text{ref}}$ distance, ensuring the reliable connection between two neighboring cluster head vehicles. If the vehicles are uniformly distributed, there would be one cluster head for each $R_{\text{ref}}$ region.

3. Conclusion

We introduced a cluster-based protocol for the content distribution in vehicular networks by integrating licensed Sub-6 GHz band, IEEE 802.11p, and mmWave communications. In the protocol, the licensed Sub-6 GHz communication is used to provide Internet connectivity to the vehicles which serve as gateway nodes providing connections to other vehicles. The mmWave communication is employed to provide high throughput connection between a vehicle and a gateway node. IEEE 802.11p-based V2V communication is used to exchange control messages for an efficient integration of different wireless technologies. We used a fuzzy logic algorithm to generate efficient cluster head nodes by taking into account vehicle velocity, vehicle distribution and antenna height. By conducting efficient clustering and edge-based communications, the protocol can provide a better performance than the existing baselines in various scenarios, especially in low bandwidth and highly dense scenarios.

References

http://www.comsoc.org/~mmc/
IEEE COMSOC MMTC Communications - Future of the Connected Vehicles


Celimuge Wu received his ME degree from the Beijing Institute of Technology, China in 2006, and his PhD degree from The University of Electro-Communications, Japan in 2010. He is currently an associate professor with the Graduate School of Informatics and Engineering, The University of Electro-Communications. His current research interests include vehicular ad hoc networks, sensor networks, intelligent transport systems, IoT, 5G, and mobile cloud computing. He is/has been a TPC Co-Chair of Wireless Days 2019, ICT-DM 2018, a track Co-Chair of many international conferences including ICCCN 2019 and IEEE PIMRC 2016. He is a senior member of IEEE.

Xianfu Chen received his Ph.D. degree in Signal and Information Processing, from the Department of Information Science and Electronic Engineering at Zhejiang University, Hangzhou, China, in March 2012. He is currently a Senior Scientist with the VTT Technical Research Centre of Finland, Oulu, Finland. His research interests cover various aspects of wireless communications and networking, with emphasis on software-defined networking, green communications, centralized and decentralized resource allocation, dynamic spectrum access, and the application of artificial intelligence to wireless communications.

Tsutomu Yoshinaga received the BE, ME, and DE degrees from Utsunomiya University in 1986, 1988, and 1997, respectively. From 1988 to July 2000, he was a research associate of the Faculty of Engineering, Utsunomiya University. He was also a visiting researcher at Electro-Technical Laboratory from 1997 to 1998. Since August 2000, he has been with the Graduate School of Information Systems, The University of ElectroCommunications, where he is now a professor. His research interests include computer architecture, interconnection networks, and network computing. He is a fellow of IEICE, and a member of ACM, IEEE, and IPSJ.

Yusheng Ji received B.E., M.E., and D.E. degrees in electrical engineering from the University of Tokyo. She joined the National Center for Science Information Systems, Japan (NACSIS) in 1990. Currently, she is a Professor at the National Institute of Informatics (NII), and SOKENDAI (the Graduate University for Advanced Studies). Her research interests include network architecture, resource management, and quality of service provisioning in wired and wireless communication networks. She is/has been an Editor of IEEE Transactions on Vehicular Technology, a Symposium Co-chair of IEEE GLOBECOM 2012, 2014, and a Track Co-chair of IEEE VTC2016-Fall, VTC2017-Fall etc. She is a senior member of IEEE.
1. Introduction
The United States averages over 5.6 million car accidents per year, of which, over 1.6 million results in injuries and over 30,000 ends fatally. To improve the lives of motorists, the United States is preparing to mandate all domestically sold vehicles to be equipped with a new technology called: Vehicle-to-Vehicle (V2V) communication [1]. Vehicles equipped with V2V are proven to be able to establish an ad hoc network by exchanging safety messages (SM) with each other to determine if a vehicular collision will occur [2]. V2V has emerged from the study of Mobile Ad Hoc Networks (MANET) which focus on the networking of information through unfixed links between nodes with power constraints. From MANETs, Vehicular Ad Hoc Networks (VANET) focus on the routing of information and collision prevention services in which the nodes move at terrestrial speeds with unlimited power sources. VANETs and V2V have become synonymous, though recently V2V has received more popularity due to the immediate deployment set to happen at the beginning of the next decade. In the United States, Europe and Singapore, the V2V physical layer (PHY) adheres to the IEEE 802.11p standard while communicating in 10MHz channels at the 5.9GHz Intelligent Transportation Systems (ITS) band. The Wireless Access in Vehicular Environments 1609 standards (WAVE-1609), outline the communication stack [3]. Recently, the Third Generation Partnership Project (3GPP) has released a new cellular based PHY known as, Long Term Evolution - Vehicular (LTE-V), employing the PC5 Sidelink [4]. Regardless of the underlying waveform adopted for deployment, the 5.9GHz ITS spectrum is envisioned for use of V2V collision avoidance services. V2V will be the largest deployment of an ad hoc safety related communication system, however, the system relies on two critical requirements: 1) the sender must be trustworthy and 2) the data received must be accurate. Because data contained within the message is necessary for providing safety benefits, the collision avoidance regime is data-centric, in that other vehicles within a 270-375m broadcast range must be equipped with V2V to determine if drivers should be warned of an impending collision or if an autonomous system should be actuated. New physical layer techniques could enable a data-decoupled collision avoidance regime operating as a parallel integrate mode without requiring changes to the existing V2V standards.

2. Background
V2V is architected as a large distributed system which relies heavily on the authenticity and integrity of the SM data to be reliable for collision avoidance. Observing Figure 1, the current paradigm alerts the driver of a potential collision with another vehicle from the application layer, but the new paradigm is to also alert from the physical layer. The application layer is more susceptible to hacking whereas the physical layer is less susceptible.

An on-going topic for V2V is ensuring anonymous SM integrity across several layers of reliability. The first reliability layer
IEEE COMSOC MMTC Communications - Future of the Connected Vehicles

is to secure the hosts raw motion information provided to a V2V radio generated by on-board sensors and securing position information generated by a Global Positioning System (GPS) device. Safety critical on-board sensor data sent to the V2V radio is assumed to be on a safety-critical bus separate from a non-safety data bus that uses a Controller Area Network (CAN) bus, but CAN data is typically bridged with safety critical data such as the auto-unlock mechanisms bridged with the crash detection system. Bridging non-safety systems with safety critical systems is a vulnerability which could provide an adversary access to the safety-critical bus to alter sensor data. On-board GPS receivers are susceptible to spoofing attacks but can mitigate attacks using a common approach that sends registration credentials before acquiring GPS coordinates from satellites and Differential GPS (DGPS) stations. However, once GPS data is validated the GPS data must be routed to endpoints within the in-vehicle CAN network including in-dash navigation systems, telematics services, electronic recording units, and within the safety-critical bus network to the V2V radio. This leaves GPS data susceptible to similar data alteration attacks as on-board sensor data, unless a dedicated GPS unit is used strictly for V2V co-located on the V2V on-board unit (OBU).

Assuming on-board sensor data and GPS data are polled securely, the second reliability layer focuses on encrypting the contents for delivery to near-by vehicles. Network layer security techniques ensure trustworthiness of anonymous SM transmissions using the WAVE 1609.2 standards but anonymizing the data while still meeting time-sensitive delivery requirements for a SM (suggested single-hop delay is less than 100ms) is still an active research area. However, regardless of the encryption method used in V2V, misbehaving nodes could broadcast erroneous SM data either intentionally or unintentionally. Unintentional misbehavior could be the result of equipment malfunction or loss of GPS service. Intentional misbehavior could be caused by malicious software altering SM data either before transmission or after reception. Data integrity is essential for collision avoidance but ensuring data integrity among misbehaving nodes is still a challenge. A misbehavior detection scheme (MDS) can be employed to detect or correct misinformation, but an MDS alone may not be sufficient for driver safety [5]. An MDS with active sensors in line-of-sight (LOS) conditions can correct SM data, but the driver is left vulnerable in non-LOS (NLOS) conditions where accident prevention is needed most. A cooperative MDS leverages other vehicles to identify misbehaving vehicles, but cooperative approaches perform poorly among multiple misbehaving nodes. A decentralized MDS can be made which sizes virtual zones of separation distance relative to the receiver to detect misbehavior, but if the receiver is unknowingly misbehaving (i.e. receiver GPS is compromised), then the zones may be sized incorrectly.

3. PHY-based Alternatives to Data-Centric Collision Avoidance

While the current state-of-the-art contribute towards either securing or correcting the contents of a SM, each approach is either cooperative data-centric or relies on infrastructure. A new paradigm being investigated thanks to the introduction of software defined radio technology, investigates collision avoidance services directly from the radio frequency (RF) front-end. By performing collision avoidance at the physical layer, the safety benefits of V2V could be decoupled from the data contained in a SM. Vehicular accidents are predicted directly from perturbations of the channel, rather than informed solely through application layers where SMs are vulnerable to garbage-in-garbage-out errors. Current V2V literature neglects physical layer (PHY) based collision avoidance applications for drivers, rather the emphasis has been on LOS active sensors integration or cooperative V2V for resolving errors. It is possible that the V2V radio will be the only collision avoidance “sensor” available to most vehicles until active sensor technology becomes more affordable. Therefore, the V2V radio RF front end is being explored for real-time collision prediction, even with 5G communication waveforms [6].

A V2V short-range path loss model was derived from a novel static measurement campaign which captured the effect of vehicle orientation, approach direction, and lane separation [7]. Differences in reported path loss values in the background literature suggest that the vehicle road configuration plays an important role in the signal power response. The model extends the classic power law path model, to include a y-intercept and a path loss exponent as a Gaussian distribution obtained from the static channel measurements. The model is apparently effective at distances less than 100m to fit a variety of dynamic vehicle scenarios. The proposed model leverages the LOS dominance as an opportunity to uncover a detailed realization of the channel, which on average could perform better than the classic power law and two-ray ground reflection models.

The received signal strength indication (RSSI) within WAVE-1609 and the IEEE 802.11p (WAVE-802.11p) based V2V networks is shown to provide collision avoidance to drivers among misbehaving nodes [8]. Experimental observations reported by this work demonstrated during a collision that RSSI can be differentiated from the RSSI during a no-collision outcome. If the direction-of-arrival (DOA) is available, then false alarms due to multiple vehicles can be reduced. The RSSI collision avoidance technique leverages the relationship between vehicle dynamics and sharpness in the RSSI curvature. By checking the third derivative of a discrete array against zero, the technique does not have to set a specific threshold to define what collision “curvature” is, which could vary for many different channel conditions. Generally, vehicular collisions occur because the relative velocity between two vehicles remains positive. The prediction methodology attempts to detect this
behavior in RSSI among varying channel conditions, whereas the traditional RSS-distance method attempts to guess the varying channel conditions; a much more difficult task to accomplish in practice for vehicular environments.

A collision and driving scenario classification technique based on the Doppler spectral density was presented called: automotive Doppler sensing (ADS), which can decouple the safety benefits of V2V communications from relying on SM content [9]. Machine learning is employed to use Cepstral coefficients for the feature set [10]. As shown in Figure 2, the Doppler profile in V2V networks shows rich data about the vehicles and their environments and can be exploited to potentially provide a reliable collision avoidance service directly from the radio front end. Using the Doppler spectral density, a feature set was described and extracted to numerically represent the time-series data acquired through a large measurement campaign in real-world scenarios. The classification algorithms used in the study, demonstrated a reliable average overall performance of 82.75% detection rate and 9.71% false alarm rate. Compared to other studies, this work was the first to prove incoherent continuous wave signals on non-stationary platforms using omnidirectional antennas could be used in terrestrial V2V for determining the surrounding environment. The Doppler profiles acquired, revealed unique information about the driving scenario between the two platforms, including sub-classification capabilities such as identifying what type of intersection is being approached and what the lateral lane spacing between the radios might be.

4. Conclusion

The safety benefits of V2V communications can be decoupled from relying on SM content. To date, there have been no validated physical layer techniques for V2V that can provide 360° collision avoidance services to drivers in both LOS and NLOS amid misbehaving nodes. The new paradigm of predicting vehicular collisions by using PHY-based observations of the channel are one way to do so by leveraging machine learning. The RSSI and Doppler-based approaches can spur new architectures that provide situational awareness while communicating. An ADS approach performs exceptionally well when given sufficient training data and can be optimized by the adjustable system parameters. Originally intended to help thwart the susceptibility of the V2V link to hacking, the existing V2V standards leave the reliability of the ad-hoc network susceptible to both primitive and intelligent RF attacks. Currently it is assumed that no RF jamming attacks are used during the operation of the PHY-based collision avoidance techniques to be discussed. Mitigating this attack-vector is still an open research area and could be addressed in future investigations by leveraging anti-jamming techniques for V2V communications. Future work would seek to develop these different techniques into a unified system for collision avoidance. Several advancements...
IEEE COMSOC MMTC Communications - Future of the Connected Vehicles

would need to be made in the areas of software defined radio technology which may achievable soon.

References


Billy Kihei received his Ph.D. in electrical and computer engineering from the Georgia Institute of Technology in Atlanta, GA in 2017. He is now an independent researcher for his own consultancy company specializing in wireless communications and intelligent transportation systems. He is also a part-time faculty professor at Kennesaw State University, in Marietta, GA. His main interests include V2X, software defined radio, IoT, and security and reliability strategies for ITS technologies. He is also a member of I Am The Cavalry, a white-hat grassroots movement to bring security awareness to the IoT. He thoroughly enjoys new research collaborations and technology commercialization. Contact him at billy@reachef.com or billy@kennesaw.edu.

Jesus Christ is LORD.
1. Introduction

The successful development and deployment of wireless (Wi-Fi, cellular and sensor) networking technologies and embedded systems over the past decades provide the opportunity to bridge the physical components with cyber-space leading to Cyber Physical Systems (CPS) [1, 2]. Transportation CPS is one of the important CPS systems where vehicles exchange upcoming traffic information and other periodic status messages for both safety and infotainment applications using vehicle-to-vehicle (V2V) or vehicle-to-roadside (V2R) communications [3, 4, 11] and vehicles also process the received data to make informed decision. IEEE 802.11p standard for Dedicated Short-Range Communication (DSRC) for Wireless Access for Vehicular Environment (WAVE) has seven channels (one common control channel and six data communication channels). These channels could be overloaded when high number of vehicles (near traffic light, intersections, urban areas) are communicating at the same time. Vehicles should be able to find other opportunities for timely dissemination of the information when 802.11p channels are busy. Furthermore, vehicles should be able to process the received data in real-time to make informed decision. For instance, for computing, transportation CPS could use clusters of vehicles as a private cloud or offload data to the public cloud depending on the availability of resources and application requirements. Computing, connectivity and communications should be robust so as transportation CPS be resilient to any malicious actions. In this paper, we present building blocks of resilient transportation CPS for computing and communications as well as research challenges and perspectives.

Main motivation of deploying transportation CPS is that the road safety is a growing concern for governments around the world [5]. The US National Highway Safety administration reports that about 15 people die a day in the US highways [5, 6]. Similarly, several million dollars is wasted because of the lost productive-working hours and consumed fuels because of traffic congestions in the U.S. highways. According to US. Patent No. 5613039, “About 60% roadway collisions could be avoided if the operator of the vehicle was provided warning at least one-half second prior to a collision.” Thus, most of the incidents could be avoided if upcoming traffic information and periodic status message are transmitted reliably and in a timely manner. With the automated process in transportation CPS, one could reduce or eliminate accidents and deaths caused by human errors, which currently account for 93% of the approx. 6 million annual automotive crashes. Upcoming traffic information and in-vehicle information should be processed in real-time to make an informed real-time decision. Thus, computing should not introduce any harmful delay and security breach in transportation CPS. Note that for the sake of simplicity, we take an example of road transportation throughout this paper. However, the analysis presented in this paper is directly applicable to other transportation CPS such as rail and air transportsations.

The rest of this paper is organized as below. Transportation CPS framework is presented in Section II where its different components. Section III presents performance evaluation using numerical results. The current status, challenges and perspectives are presented in Section IV. Finally, the paper is concluded in Section V.

2. Framework of Transportation Cyber Physical Systems

A typical framework for transportation CPS is shown in Fig. 1 in which there are three components: cyber (computing with vehicle cluster/cloud and public cloud, communication and networking), physical (vehicles, road, air, water, human/driver, etc.) and system (interaction and control with feedback). In transportation CPS, like in any other CPS, physical components such as vehicles, road and human/drivers interact with each other and with cyber space through computing (public and vehicular private clustered cloud), communication, and control systems. Transportation CPS needs robust computing, information dissemination and control mechanisms for feedback [2,5].

For computation in transportation CPS, vehicles could use their individual processing and computing capacities, form clusters of vehicles as private cloud for cooperative computing and collaborative decision making, public cloud by offloading their data to the public cloud and getting the response back or hybrid cloud (private vehicle cloud and public cloud). The choice of the computation depends on the requirements of transportation CPS. For instance, when huge amount of data is available, individual vehicle could take longer time to process huge amount of data to get the useful information compared to time needed for offloading to the cloud and getting the response with useful information back from the cloud. In this case, offloading data to public or private cloud is suitable to make near real-time decision. Similarly, for communication, connectivity between vehicles in transportation CPS, which depends on number of neighboring vehicles and transmission
range used for communications, is expected to use variety of wireless technologies such as DSRC/WAVE, WiMAX, Wi-Fi, Bluetooth, ZigBee, cellular, satellite, etc. The connectivity plays a major role in feedback process for controlling and maintaining the stability of the systems. Like in any other CPS, computing, communications and networking in transportation CPS are essential parts for automating the system to make the system resilient and intelligent to operate in the presence of the adverbial users.

Fig. 1: Typical framework of Transportation Cyber Physical System.

2.1 Computing for Transportation CPS

In transportation CPS, huge amount of data can be processed by forming private cloud/clusters of vehicles for collaborative processing or hybrid of private vehicular cloud and public cloud as shown in Fig. 1.

i. Private Cloud Computing using Clusters of Vehicles

In transportation CPS, individual vehicles are armed with virtually unlimited power, storage and computing capabilities, they could form clusters to make private clouds for distributed computing on the fly [7, 8]. Individual vehicles could form the clusters based on their travel direction and information needs to share and process the information to make informed decision with resiliency.

ii. Public Cloud Computing

When vehicles cannot process the huge amount of the data in a timely manner to meet near-real-time requirements, they could offload their information to the public cloud in the Internet for processing and aggregation as shown in Fig. 1. Vehicles could offload the data partially or fully depending on how long they will take if they process the data by themselves vs the time needed for offloading, processing and getting the response back from the cloud. Vehicles could also use hybrid cloud (combination of public cloud and private vehicular clouds).

2.2 Communications for Transportation CPS

In transportation CPS, vehicles could use V2R communication to exchange the information with each other via roadside units such as cellular towers, Wi-Fi access points, WiMAX, DSRC/WAVE and satellite links. When vehicles communicate with each other using roadside infrastructures to forward information, they face high latency or delay [9]. Because of the delay introduced by the roadside units, it is not feasible technically for transportation CPS where decision needs to be made in a real-time manner.

Next, vehicles could form an ad hoc network to communicate directly using a single-hop or multihop V2V communications to exchange the information in transportation CPS. Using 802.11p based DSRC/WAVE standard vehicles could use the
transmission range upto 1000 meter (equivalently 32dBm of power). When information is exchanged between vehicles using V2V communication, delay will be much lower than that in V2R based communication. Lower delay is suitable for exchanging time critical information between vehicles. Furthermore, V2V communication is also applicable for emergency evacuations when all other communication infrastructures are overloaded or not available due to the disasters.

Furthermore, in transportation CPS, vehicles have seven dedicated wireless channels (1 for common control channel and 6 data communication channels) in IEEE 802.11p DSRC/WAVE standard. However, these channels could be easily jammed because of adversaries or large number of vehicles using these limited number of channels. With the advancements with cognitive radio technology and dynamic spectrum access, vehicles could choose the wireless technology depending on their application that the transportation CPS is envisioned to support. If a given vehicle has options to use different wireless networks, it should be able to choose the best network suitable for exchanging information over the network [5,11]. As per the DSRC/WAVE requirement in road transportation, each vehicle is required to broadcast its periodic status information (such as speed, acceleration, geolocation, direction, etc.) periodically to inform neighbors. This periodic status information could include the dynamic spectrum access information for opportunistic communications using channels other than DSRC/WAVE channels. Based on the sensed channel status, vehicles could find idle channels individually or in a collaborative way tune to a suitable idle channel and establish a connection, and exchange the information in transportation CPS [5, 9]. In this case, the time duration for successful communication can be expressed as

\[
\text{Total time} = \text{sensing-plus-processing time} + \text{association time} + \text{time for security} + \text{cluster time} + \text{data exchange time}.
\]

(1)

Sensing time includes the delay introduced by channel sensing other than 902.11p channels and identifying idle channels by vehicles individually or in a collaborative manner. Association time denoted time taken to set up the communication link between vehicles and time for security is the delay introduced because of implemented security mechanisms in CPS vehicles. When vehicles use 802.11p DSRC/WAVE channels, sensing-plus-processing time is zero. Two different scenarios exist V2V communications: i) Scenario 1: one-way-traffic where vehicles move in the same direction with almost zero relative speed; and ii) Scenario 2: two-way-traffic, i.e., vehicles move in both directions with high relative speed. In Scenario 2, there will be short overlapping time duration for vehicles for sensing, connection setup and information exchange.

### 2.3 Connectivity in Transportation CPS

To maintain the connectivity among vehicles, transmission range and power should be adapted based on number of neighboring vehicles (also known as local vehicle density), traffic flow and network conditions. When fewer (or more) vehicles are present around its proximity, transmission range is increased (decreased). The transmission range (Tr) based on the estimated local vehicle density can be calculated as [9]

\[
T_r = \min \left\{ R \left( 1 - D \right), \sqrt{\frac{R \log R}{D}} + \beta R \right\}
\]

(2)

where \( \beta \) is a constant from traffic flow theory, R is the length of the road segment over which the vehicle estimates its local vehicle density, and D is the local vehicle density for a given vehicle which is calculated as the ratio of the actual reachable number of vehicles on the road that are present within its transmission range based on periodic status message interaction to the total possible number of vehicles that can be present on the road for current transmission range, travel speed and safety separation distance on the road. This transmission range is used to estimate the overlap time duration between vehicles for exchanging their information.

### 2.4 Typical Characteristics of Transportation CPS

Transportation CPS has many typical characteristics such as: i) network topology in transportation CPS changes dynamically with the fast-moving vehicles and road structure; ii) driver or human behavior affects the network topology based on drivers’ travel destination; iii) location determines the number of vehicles such as urban areas expected to have more vehicles compared to rural areas; iv) most of the traditional wireless technologies are not designed for fast moving vehicles in transportation CPS; v) vehicles in transportation CPS have virtually unlimited power, storage, and computing capabilities unlike other wireless networks; vi) low latency for safety applications in transportation CPS is the most important feature to forward emergency messages in a timely manner; vii) infotainment multimedia contents are bandwidth hungry and those transportation CPS application could be suffered in low bandwidth wireless networks; and viii) transportation CPS needs tighter combination of security, computing, communications and control systems.
3. Performance Evaluation and Discussions

This section evaluates the performance for connectivity, computing and communications in transportation CPS. We also look into how resiliency can be achieved in case of adversarial activities in transportation systems. When vehicles travel, their relative speed determines the connectivity, computing and communication time period. Note that the road-side unit is considered to be vehicle with speed 0 miles/hour. For a relative speed \( v \) of two vehicles with overlap transmission range \( T_r \), the time period \( t_p \) available to those vehicles could be expressed as

\[
    t_p = \frac{T_r}{v}
\]

By simulating a network of vehicles for transportation CPS, we plotted the variation of time period for different relative speed of vehicles and overlap transmission range as shown in Fig. 2. When vehicles move in same direction, their relative speed is small or zero leading to a long (or infinite) overlap time. However, when vehicles move in opposite directions, their relative speed is very high that leads to short overlap time period as shown in Fig. 2. Note that the overlap time period in Fig. 2 is used for sensing, setting up wireless connection, running security approaches, and data exchange in transportation CPS. We noted that the total time period is higher for lower relative speed for given transmission range and vice versa. Similarly, the time period is higher for higher transmission range for given relative speed and vice versa as shown in Fig. 2.

![Fig. 2: Expected overlap time period for different transmission range and relative speeds for vehicles in transportation CPS.](image-url)

Next, when total time for channel sensing, association and running security techniques was one second and four seconds, we plotted the variation of time period available for actual data communication as shown in Fig. 3 and Fig. 4 respectively. We observed in Fig. 3 that when relative speed is greater than 110 miles/hour (vehicles moving 55 miles per hour in opposite directions) and transmission range is 50 meters, vehicles have no time left when they take about 1 second for successful association. When vehicles’ relative speed is 110 miles/hour, they have about 22.73 milliseconds left for data exchange as shown in Fig. 3. Similarly, vehicles have no time left for data exchange when relative speed is greater than 20 miles/hour for a range of 50 meter as shown in Fig. 4. When vehicles’ relative speed is 20 miles/hour for transmission range of 50 meters, they have about 1.625 seconds for data exchange as shown in Fig. 4.
Fig. 3: Expected overlap time period for different transmission range and relative speeds for vehicles in transportation CPS when channel sensing, association and running security techniques was 1 second.

Fig. 4: Expected overlap time period for different transmission range and relative speeds for vehicles in transportation CPS when channel sensing, association and running security techniques was 4 seconds.
Next, in Fig 5, we plotted the variation of expected data size exchanged between vehicles using 27 Mbps link which is the max. data rate of IEEE 802.11p DSRC/WAVE standard and 200 Mbps which is a typical data rate in IEEE 802.11n standard for different transmission ranges and relative speeds when vehicles take 4 seconds (worst-case scenario in terms of time) for channel sensing, association and running security techniques. For higher relative speed of vehicles, the data size exchanged was smaller and vice versa as shown in Fig. 5. Higher the data rate, the larger the data size exchanged among vehicles for given range and relative speed as shown in Fig. 5.

Fig. 5: Variation of expected data size exchanged between vehicles using 27 Mbps link (max. data rate of IEEE 802.11p DSRC/WAVE standard) and 200 Mbps (IEEE 802.11n) for different transmission ranges and relative speeds in transportation CPS when channel sensing, association and running security techniques was 4 seconds.

Fig. 6: Variation of expected data size exchanged between vehicles using 27 Mbps link (max. data rate of IEEE 802.11p DSRC/WAVE standard) and 200 Mbps (IEEE 802.11n) for different transmission ranges and relative speeds in transportation CPS when channel sensing, association and running security techniques was 4 seconds and 200 vehicles shared the same link.
Finally, about 200 vehicles are assumed to be sharing a given link (27 Mbps link) to exchange their information using CSMA/CA where total time for sensing, association of devices and time needed for securing the communication was 4 seconds. In this case, per-vehicle data rate is lower which results in lower per-vehicle data size. Variation of per-vehicle data size for different ranges and relative speeds is plotted in Fig. 6. The data size exchanged by individual vehicles is smaller when relative speed is higher for a given transmission range as shown in Fig. 6. Furthermore, the data size exchanged by individual vehicles is higher for higher transmission range for a given relative speed as shown in Fig. 6.

4. Transportation CPS Challenges and Perspectives

CPS systems are in early stage of development and implementation. However, there have been some advances in design, development, implementation and evaluation of CPS systems [1, 5, 6, 10]. There are several challenges to realize the full potential of CPS. Typical challenges and perspectives in transportation CPS are discussed below:

- **Cybersecurity Challenges and Perspectives in transportation CPS**: Since CPS systems have networked subsystems for controlling and automating the overall operations of the systems, security vulnerabilities come with the connectivity. However, resiliency is critical to transportation CPS to provide uninterrupted services in the presence of adversaries since it is related to life and death of involved parties. Adaptive security techniques need to be developed for transportation CPS which meet its specific requirements such as least delay, adaptive to operating environment, privacy/confidentiality of the users, availability of the information to the right users and integrity of the information. When internet was designed, security was not considered, and security solutions have been implemented as patches and updates. However, CPS is in the early stage of development, thus developers have opportunity to include security as one of the important components from the beginning of CPS design.

- **Privacy Challenges and Perspectives in transportation CPS**: In transportation CPS, private information of the people is linked with vehicles which results in potential privacy violation of the involved parties by adversaries. Security mechanisms designed for transportation for CPS should consider the privacy of the users which can appropriately work with sensitive and personal information of the owner/drivers of the vehicles.

- **Communication Technologies with Least delay**: Traditional wireless access technologies are not build for highly mobile users that require least amount of delay. However, communication systems used in transportation CPS should have delay/latency in microsecond so as to feed back the controlling information to vehicles to stabilize the overall system in real-time.

- **Economic Challenges**: One of the major challenges is the cost of CPS software. Transportation CPS like other CPS relies on embedded systems (software and hardware) in which cost of the CPS vehicle would increase significantly. For instance, about 25% of the total cost in aeroplanes consists of cost of software that operates the planes and it is expected to double in a couple of years foe new planes.

- **Interoperability and Platform Independency in Transportation CPS**: Most CPS including transportation CPS are expected to run automatically with the help of computing, communication and feedback processes. It is challenging to design a universal technique to work for all CPS systems with different systems requirements that could interoperate across systems with complex tasks and operation environment. One approach could be a hierarchical approach so that certain features can be tuned or untuned depending on the CPS specific needs.

- **High Speed Connectivity in Transportation CPS**: Fibre optics can offer high speed connectivity for backhaul or in-vehicle communications. However, most of the inter-vehicle communications are expected to be done through wireless access for feedback and information dissemination. Existing wireless technologies could offer limited data rate such as IEEE 802.11p DSRC/WAVE standard for vehicular communications offers only up to 27 Mbps. Transportation CPS requires high data rate to have least delay for feedback process to control the CPS in real-time. Transportation CPS urgently needs a high data rate wireless access technology.

All in all, we have an opportunity to consider all challenges while designing resilient transportation CPS from the beginning of its development that can provide reliable and robust operations could interoperate across systems with complex tasks and operation environment.

5. Conclusion

This paper has presented a typical framework for transportation CPS with its different components. Furthermore, we have presented computing, connectivity, communications requirements for resilient transportation CPS by considering different parameters such as channel sensing and identifying time, association time, security run time, vehicle density, vehicle speeds, communication range, data rate and size. These parameters have impact in feedback mechanism for automating
and controlling transportation CPS. This paper has presented some of the major challenges and perspectives in transportation CPS.

Acknowledgements
This work is supported in part by the National Science Foundation (NSF) under grants CNS-1650831 and HRD-1828811. Any opinion, finding, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of NSF.

References

Dr. Danda B. Rawat (S’07, M’10, SM’13) is an Associate Professor in the Department of Electrical Engineering & Computer Science, Founding Director of the Data Science and Cybersecurity Center (DSC2), Graduate Program Director of Howard-CS Graduate Programs, Director of Graduate Cybersecurity Certificate Program and Founding Director of Cyber-security and Wireless Networking Innovations (CWiNs) Research Lab at Howard University, Washington, DC, USA. Dr. Rawat is engaged in research and teaching in the areas of cybersecurity, machine learning and wireless networking for emerging networked cyber-physical systems, Internet-of-Things, smart cities, software defined systems and vehicular networks. He has secured over $3 million in research funding from US National Science Foundation, US Department of Homeland Security, and private Foundations. Dr. Rawat is the recipient of NSF Faculty Early Career Development (CAREER) Award in 2016, the US Air Force Research Laboratory (AFRL) Summer Faculty Visiting Fellowship in 2017, Outstanding Research Faculty Award (Award for Excellence in Scholarly Activity) at GSU in 2015, the Best Paper Award from BWCCA 2010 and Outstanding PhD Researcher in 2009. He has delivered over 10 Keynotes and invited speeches at international conferences and workshops. Dr. Rawat has published over 200 scientific/technical articles and 9 books. He has been serving as an Editor/Guest Editor for over 30 international journals. Dr. Rawat is a Senior Member of IEEE and ACM, a member of ASEE, and a Fellow of the Institution of Engineering and Technology (IET).
Dr. Chandra Bajracharya (S’10, M’14) is an Assistant Professor in the Department of Electrical Engineering at Capitol Technology University, USA. Her research interests include Internet of Things, cyber physical systems, power electronics, alternative energy, communication systems, numerical electromagnetic, UWB antenna design and signal/image processing. She has published over 20 peer reviewed journal articles and conference papers. She has been serving as a TPC member for several international IEEE conferences.

Mr. Guy Lingani (S’18) is a research member of Data Science and Cybersecurity Center (DSC²) as well as member of Cyber-security and Wireless Networking Innovations (CWiNs) Research Lab at Howard University. He is a PhD student, under the supervision of Dr. Danda B. Rawat, in the Department of Electrical Engineering and Computer Science (EECS) in the College of Engineering and Architecture at Howard University. His research interests include smart transportation systems, Internet of Things, cyber physical systems, deep learning, machine learning and video/image processing.

Ms. Sunitha Safavat is a research member of Data Science and Cybersecurity Center (DSC²) as well as member of Cyber-security and Wireless Networking Innovations (CWiNs) Research Lab at Howard University. She is a PhD student, under the supervision of Dr. Danda B. Rawat, in the Department of Electrical Engineering and Computer Science (EECS) in the College of Engineering and Architecture at Howard University. Her research interests include cybersecurity, vehicular ad hoc networks, mobile edge computing, Internet of Things, cyber physical systems and intelligent transportation systems.
IEEE COMSOC MMTC Communications - Frontiers

MMTC OFFICERS (Term 2018 — 2020)

CHAIR
Honggang Wang
UMass Dartmouth
USA

STEERING COMMITTEE CHAIR
Sanjeev Mehrotra
Microsoft
USA

VICE CHAIRS
Pradeep K Atrey (North America)
Univ. at Albany, State Univ. of New York
USA

Wanqing Li (Asia)
University of Wollongong
Australia

Lingfen Sun (Europe)
University of Plymouth
UK

Jun Wu (Letters&Member Communications)
Tongji University
China

SECRETARY
Shaoen Wu
Ball State University
USA

STANDARDS LIAISON
Guosen Yue
Huawei
USA

MMTC Communication-Frontier BOARD MEMBERS (Term 2016—2018)

Dalei Wu Director University of Tennessee at Chattanooga USA
Danda Rawat Co-Director Howard University USA
Melike Erol-Kantarci Co-Director University of Ottawa Canada
Kan Zheng Co-Director Beijing University of Posts & Telecommunications China
Rui Wang Co-Director Tongji University China
Lei Chen Editor Georgia Southern University USA
Tasos Dagiuklas Editor London South Bank University UK
Shuai Shuai Guo Editor King Abdullah University of Science and Technology Saudi Arabia
Kejie Lu Editor University of Puerto Rico at Mayagüez Puerto Rico
Nathalie Mitton Editor Inria Lille-Nord Europe France
Zheng Chang Editor University of Jyväskylä Finland
Dapeng Wu Editor Chongqing University of Posts & Telecommunications China
Luca Foschini Editor University of Bologna Italy
Mohamed Faten Zhani Editor l’École de Technologie Supérieure (ÉTS) Canada
Armir Bujari Editor University of Padua Italy
Kuan Zhang Editor University of Nebraska-Lincoln USA