Drone-assisted Multi-purpose Roadside Units for Intelligent Transportation Systems

Nico Saputro, Kemal Akkaya, Ramazan Algin and Selcuk Uluagac
Dept. of Electrical and Computer Engineering, Florida International University, Miami, Florida, 33174, USA
{nsapu002, kakkaya, ralgin, suluagac}@fiu.edu

***Abstract*—As drones are becoming prevalent to be deployed in various civic applications, there is a need to integrate them into efficient and secure communications with the existing infrastructure. In this paper, considering emergency scenarios for intelligent transportation applications, we design a secure hybrid communication infrastructure for mobile road-side units (RSUs) that are based on drones. The architecture tackles interoperability issues when Dedicated Short Range Communications (DSRC), wireless mesh, and LTE need to coexist for coordination. Specifically, we propose a novel tunneling protocol to integrate LTE with IEEE 802.11s mesh network. In addition, we ensure that only legitimate users can connect and control the mobile RSUs by integrating an authentication framework built on top of the recent OAuth 2.0 standard. A detailed communication protocol is proposed within the elements of the architecture from vehicles to control center for emergency operations. The proposed secure architecture is implemented in ns-3 and tested for its performance under heavy multimedia traffic. The results indicate that the proposed hybrid architecture can enable smooth multimedia traffic delivery via the mobile RSU.**

***Index Terms*—Drones; ITS; roadside units; IEEE 802.11s, DSRC; Authentication**

I. Introduction

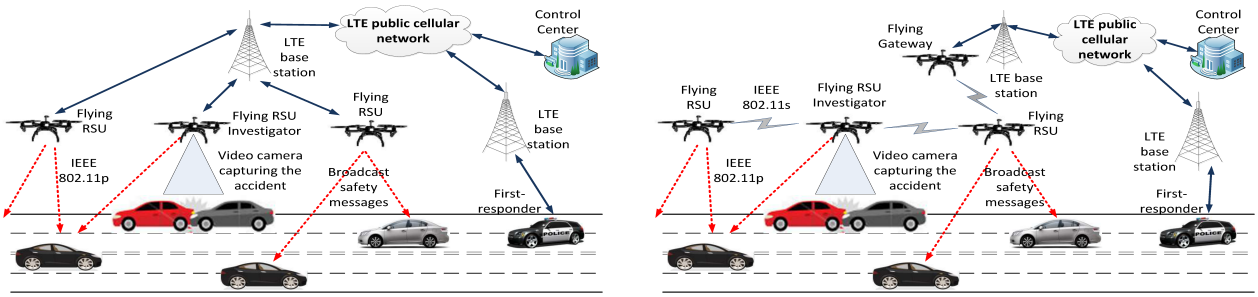
The introduction of Intelligent Transportation System (ITS) to the transportation sector has revolutionized the transportation management and operations [1] [2]. Many approaches (e.g., CCTV for traffic monitoring, load-based dynamic traffic-light cycle, and dynamic message signs located above major roads) have been used not only to enhance the traffic management and control strategies, but also enable drivers to be better informed and make a safer and smarter use of the transportation systems. ITS also has driven the automotive industries to build smarter vehicles by incorporating more and more intelligent devices into vehicles for user's comforts and enable ITS safety applications that may utilize the vehicle-to-vehicle (V2V) and/or vehicle-to-roadside infrastructure (V2I) communications for data exchanges among vehicles and the roadside infrastructure to prevent collision [3].

Within ITS scenarios, vehicles will be equipped with DSRC [4] to broadcast safety messages and talk to infrastructure through road side units (RSU). The deployment of stationary RSUs, which are installed along the roadside, however, is very challenging. In some circumstances, the deployments may not be feasible in terms of cost in rural areas where the vehicle density is very low. Even in the areas with a very high vehicle density, the deployment can still be too costly. In such areas, due to the limited communication range of Dedicated Short-Range Communications (DSRC) technology, stationary RSUs should be densely deployed to ensure maximum spatio-temporal coverage. This may require a large number of stationary RSUs when the area is large. Therefore, there has been some efforts to utilize alternate means to reduce cost, such as cars [5], public transportation (e.g., bus) and fully controllable local government-owned vehicles as mobile RSUs along with the stationary RSUs [6].

Nonetheless, these efforts are still not enough to address the problems that may arise under the emergence of unexpected events, which may occur at any place and any time. Specifically, some unforeseen events such as car crashes or natural disasters that block roads (e.g., landslides, floods, bridge collapses, fires, etc.), require the timely response from the relevant first-responders (e.g., firefighter, police, medical team, etc) to reduce its effects to the transportation system (e.g., heavy congestion) and/or users' safety. Vehicles around the area should be continuously notified through the public safety message disseminations from the roadside infrastructure for precautions. A drone, which is also known as unmanned areal vehicle (UAV), is envisioned to be a high potential option to enable the ITS solutions for these cases [2] due to its easy access to the scene and the potential to act as a information dissemination/collection service, i.e., as a mobile RSU.

In this paper, we propose using a swarm of autonomous DSRC-based drones as mobile multi-purpose RSUs for these cases and investigate their effectiveness in terms of providing connectedness to first-responders. To this end, we propose connectivity architectures to enable smooth operations. Specifically, in addition to the DSRC, we propose to equip drones with other types of communications depending on the spot. For instance, LTE is the major communications used between drones and the control center where drones and emergency operations are managed. If LTE is not available due to poor connection, a hybrid wireless mesh (e.g., IEEE 802.11s) [7] and LTE communication architecture is proposed. Basically, the swarm forms a wireless aerial mesh network to cover the LTE blind area and one of the drones which will be placed under the LTE coverage area, will act as the gateway for bridging the mesh and LTE. Consequently, we will have a three-tier architecture where the traffic travels from vehicles to drones and to control center by utilizing DSRC, wireless mesh and LTE respectively. Under this architecture, we address interoperability issues between different standards for smooth end-to-end communications.

978-1-5386-6358-5/18/$31.00 ©2018 IEEE



(a) Drones use LTE when LTE coverage is available

(b) Drones use IEEE 802.11s when LTE coverage is not available

Fig. 1: Drone-assisted mobile RSU Communications Architectures

Another issue in this communication setup is the security of connections made to the mobile RSU. The proposed swarm is expected to support first-responders from multiple organizations. Each of them may have to assess different regions of interest from different point of views that may require the mobile RSU to move to specific directions. In this case, there is a need to enable the first-responders to directly connect/control the drones for their specific purpose. However, allowing multiple parties to have direct access to the mobile RSU may pose security threats since command and control messages that can be used to overwrite the drone autonomous operations are exposed to these parties. Moreover, when an emergency case involves multiple parties that may need to directly control the drones, the hierarchy of commands may also be an issue. Therefore, we also propose a centralized *proxy-based control framework* that acts as the middleman between the first-responders and the swarm. An authorization and symmetric key distribution mechanism based on the OAuth 2.0 framework [8] is incorporated in the framework.

We created the proposed architectures under ns-3 network simulator [9]. The performance of these communication architectures are evaluated under multimedia traffic (e.g., still images and video streaming). The video quality after traversing the hybrid network is also evaluated using the EvalVid framework and tool-set [10]. The simulation results demonstrated the feasibility of the proposed architecture for secure and efficient emergency operations.

The paper is organized as follows. In Section II, we discuss the relevant work. Section III describes the drone communications architectures and the authorization and access mechanism of the proposed system model. Detailed performance evaluation of the proposed model is given in Section IV. Finally, we conclude the paper in Section V.

II. Related Work

A number of hybrid IEEE 802.11p/LTE communications architectures for Vehicular Adhoc Networks has been studied recently. A cluster-based architecture where the vehicular cluster-head acts as the gateway to LTE infrastructure, is used in [11] for an end-to-end multicasting group communications between clusters; in [12] for a cooperative public safety content distribution system; in [13] for the real-time video streaming distribution; and in [14] for the safety message multihop dissemination between clusters. In the vehicular named data networking [15], the interest message and the data messages are conveyed by LTE and IEEE 802.11p respectively. While these works focus on the V2V message exchanges, our work, on the other hand, is concerned with the mobile RSU infrastructure communications with control center/first responders. Moreover, our work also takes into account the end-to-end communications interoperability issue [16], an issue that the previous works did not consider. In [17], the hybrid communications architecture includes an intermediate IEEE 802.11s-based Advanced Metering Infrastructure to support the Vehicle-to-Grid certificate verification. While this work also considers the similar hybrid architecture (i.e., includes IEEE 802.11s), our work is different since we also need to consider the drone mobility, interoperability with LTE, and the heavy multimedia traffic that passes through the network. Finally, we would like to note that none of the previous studies considered authentication issue that is tackled in this paper.

III. Proposed Multi-purpose RSUs

A. System Overview

We propose a drone-assisted multi-purpose RSU, which consists of a swarm of autonomous drones where each autonomous drone can have a different name/role based on the assigned tasks. These are listed as follows: 1) *Flying RSU* for public safety message dissemination; 2) *Flying RSU investigator* which can be assigned to assess any possible damages of the emergency event; and 3) *Flying gateway* that acts as the communication gateway when two different communications technologies are used.

We envisioned that each autonomous drone is supported by the following: (1) a sustainable power source (e.g., energy harvesting devices); (2) adequate computing power for various drone built-in autonomous capabilities; (3) a variety of required sensors and cameras; and (4) multiple communications technologies (i.e., IEEE 802.11p [18] which supports DSRC, LTE [19] which supports wide-area communications, and IEEE 802.11s [7] which is the mesh standard for WiFi) that can be activated/deactivated by the drone based on the sensed environments and its roles in the swarm (e.g., drone deactivates LTE and activate IEEE 802.11s in the non-LTE coverage area when the task is as the *flying RSU*). The next section discusses the communications architectures in more details.

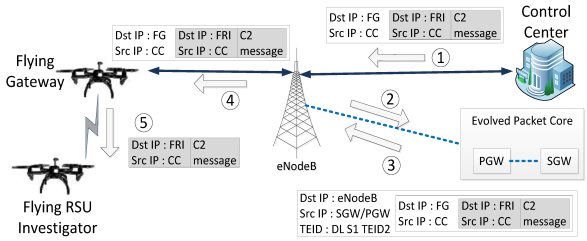


Fig. 2: The proposed downlink traffic tunneling over the public LTE

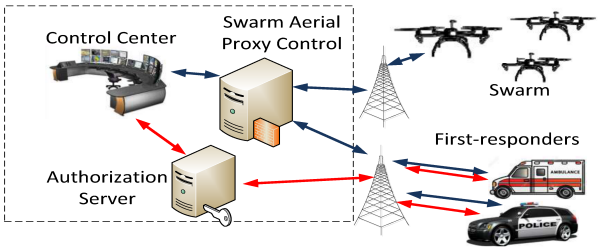


Fig. 3: The centralized proxy-based control framework

B. Drones Communications Architectures using Tunneling

Two proposed drone communications architectures are depicted in Fig. 1. In both architectures, IEEE 802.11p is the core communications technology used by the *flying RSUs* and *flying RSU investigator* for the public safety messages dissemination to vehicles. The availability of a public LTE coverage around the area of interest determines the type of communications technology used. The LTE communications architecture as illustrated in Fig. 1a is used when there is a public LTE coverage in the area of interest. All drones are connected to the control center through the public LTE cellular network. In case the LTE coverage is not available, drones forms an IEEE 802.11s-based multihop mesh network to cover the LTE blank spot area and the *flying gateway* acts as the gateway between the drone aerial mesh network and the public LTE cellular network as shown in Fig. 1b. The *flying gateway* is also the root node of the mesh network, which knows all paths to all other drones by using the default path selection mechanism of IEEE 802.11s (i.e., Hybrid Wireless Mesh Protocol). The uplink traffic (e.g., live streaming video from the *flying RSU investigator*) is delivered multihop inside the mesh network to the *flying gateway* and then to the control center through the public LTE network. Conversely, the downlink traffic from the control center (e.g., C2 messages) reaches the *flying gateway* using the public LTE network, which then delivers the traffic multihop inside the mesh network to the drone end destination.

The end-to-end downlink traffic in the hybrid IEEE 802.11s/LTE architecture, however, raises an interoperability issue. In the context of LTE cellular network, which is an IP-based network, a User Equipment (UE) is the LTE end terminal that gets its IP address from the Evolved Packet Core (EPC) network [19]. The *flying gateway* can be seen as a UE with the extended functionality as the gateway to the other network (i.e., IEEE 802.11s/IEEE 802.11p networks) that may have their own IP address assignment scheme. This causes the EPC network not being able to find the corresponding GPRS tunneling protocol (GTP) tunnel identity (TEID) from the downlink traffic since the destination IP address in the downlink traffic is pointing to a *flying RSU* while a TEID is typically mapped to a UE IP address (i.e., the IP address of the *flying gateway*). Providing the UE access list solution to this interoperability issue at the EPC network as in [16], is not be applicable since the network is formed dynamically and LTE network cannot act quickly to update this list. Obviously, this will cause operational delays. Moreover, it requires to expose the swarm internal IP addressing to the LTE provider that raises privacy concerns.

To address this issue, we propose a tunneling protocol over the public LTE network for the downlink traffic between the control center and the *flying gateway*. Fig. 2 illustrates the tunneling operations for the downlink traffic. The control center encapsulates its downlink traffic to the *flying RSU investigator* by adding a new IP header with the IP address of the *flying gateway* as the destination. This way, the EPC network will be able to find the corresponding TEID and deliver this traffic to the corresponding LTE base-station and subsequently to the corresponding *flying gateway*. On receiving this traffic, the *flying gateway* decapsulates the traffic to find the end-destination for the final delivery.

C. Proposed Centralized Proxy-based Control Framework

When multi-purpose RSU is deployed for emergency operations, there is a need to control them centrally and enable first-responders to communicate with them for various control purposes. To this end, we propose a secure control framework. In this control framework, all two-way communications between drones and control center/first-responders are handled by a centralized proxy called the *Swarm Aerial Proxy Control (SAPCon)*. This centralized control is chosen with the aims to hide C2 messages from the third parties; reduce the complexity of the swarm operations related to the first-responders activities (e.g., the need to handle secure connection requests and authentication from multiple first-responders); and the need to deal with the execution priority when C2 messages are received from multiple first-responders and/or control center (i.e., command hierarchy) at almost the same time. The SAPCon handles any drone movement requests from the control center/first-responders when they want to have a more comprehensive assessments from their point of views by moving the drone around any region of interest. Additionally, for efficiency purposes, SAPCon also acts as a storage proxy for the video streaming and all other sensors' reports from the *flying RSU investigator* for any requests from the legitimate interested parties.

To authorize any legitimate first-responders for secure indirect control to the swarm autonomous operations, we propose a security framework that is based on OAuth 2.0 authorization framework. OAuth follows a similar approach to Kerberos authentication system [20] where tokens are issued to third-party clients by an authorization server, with the approval of the resource owner. The third party can then use the access

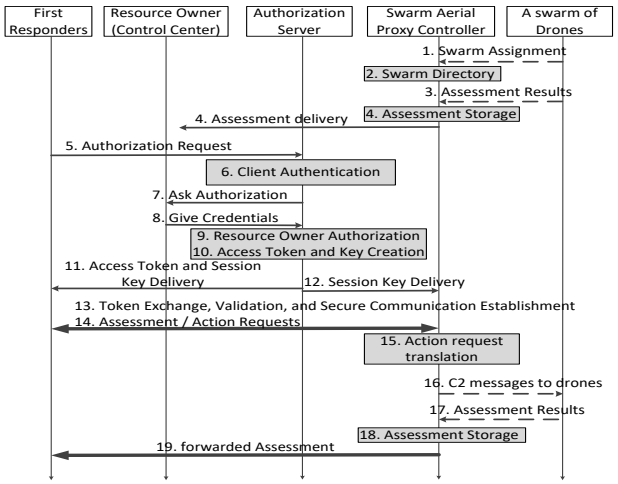


Fig. 4: Proposed Security Framework for the first-responders access to drones and their reports.

token to access the services without a need for creating specific authentication protocols for each case. In our case, we assume the authorization server sitting in the control center that will serve the first responders or any vehicles to get access to drones as depicted in Fig. 3. The sequence diagram of the framework is depicted in Fig. 4.

IV. Performance Evaluation

A. Experiment Setup

The two proposed drone communications architectures are implemented in ns-3 version 3.27 and the EvalVid tool-set [10] is used for the video transmission and evaluations over these communication architectures. Three experiment scenarios are designed to evaluate the proposed architectures. In the first scenario, we measured the impact of some background traffic when multimedia traffic is being sent from the *flying RSU investigator* using UDP transport protocol over the LTE public cellular network. We varied the number of active UEs that generate the background traffic to represent the network load as follows: each UE creates a two-way flow traffic (i.e., uplink and downlink traffic) with a server in the Internet, and each UE forms a pair with other UE for the one-way flow traffic. We used the number of UEs, $N_{UE} \in$ [0,10,20,50].

The second scenario is used to evaluate the IEEE 802.11s performance when it is used to cover the blank spot area. We varied the the number of hops between the *flying RSU investigator* and the *flying gateway*, $N_{hop} \in$ [3,4,5,6,7,8] hops.

The third scenario is used to evaluate the impact of the drone mobility around its initial deployment point in response to any first-responders' movement requests on the on-going video transmission. We used a random walk mobility model [9] where each drone moves for a fixed amount of time with a random speed $S \in$ [1,16] m/secs and a random direction D. The area of the drone random walk movement is limited in a square around the initial drone deployment point.

In all scenarios, the **highway** reference video from Evalvid, which consists of 2000 frames, are used as the multimedia traffic. The distance between drones is assumed to be 90m; the height of the drone is varied with the minimum height being 15m; the height of the LTE base-station is set to 30m; and the IEEE 802.11s transmission range is set to 120m.

Our performance metrics were the *end-to-end delay* of data traveling from first-responders to control center and the *percentage of lost frames* when transmitting multimedia traffic.

B. Experiment Results

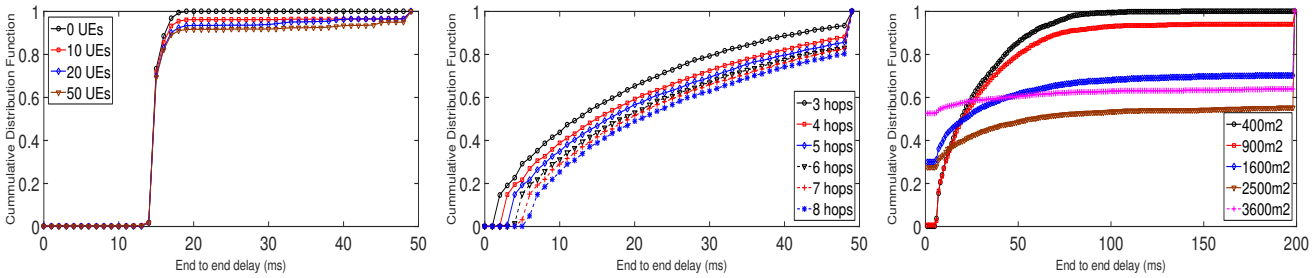
The experiments results for end-to-end delay are shown in Fig. 5. First, we evaluated the impact of active users that may use the public LTE network when the *flying RSU investigator* is sending a live-streaming video. As can be seen in Fig. 5a, when there is no active users, the end-to-end delay is less than 20msecs. As the load of the public network increases, the end-to-end delay also increases, but the increase is still within an acceptable level. More than 90% of the time the end-to-end delay is under 20msecs even when there are 50 active users. Moreover, we also observed the overall percentage of lost frames in the public LTE cellular network since we used UDP transport protocol to carry the video. The percentage is small and constant (0.2%) as indicated in Table I, regardless of the number of active users.

TABLE I: Frame Lost for the three experiment scenarios

active UEs	Frame Lost	Hop Count	Frame Lost	Cov. Area	Frame Lost
0	0.2%	3	0.05%	400m2	0.05%
10	0.2%	4	0.05%	900m2	0.70%
20	0.2%	5	0.05%	1600m2	28.85%
50	0.2%	6	0.05%	2500m2	31.05%
		7	0.05%	3600m2	52.10%
		8	0.05%		

In the case when there is no public LTE network coverage in the area, our experiments with the used of IEEE 802.11s wireless mesh network to cover the LTE blank spot area also provided promising results. While the end-to-end delay is increased as the number of hops increases, around 80% of the time, the end-to-end delay is under 48msecs regardless of the number of hops as seen in Fig. 5b. This is because, when IEEE 802.11s is used, there is some overhead due to the periodic path selections and mesh connectivity attempts. However, this overhead does not have an impact on the video quality. The overall percentage of lost frame is even smaller (0.05%) as indicated in Table I as well, regardless of the number of hops taken by the multimedia traffic.

With respect to the drone maneuverability around its initial deployment point, our experiments indicate that when the public LTE network is present, a drone can maneuver around a large area (e.g., up to $3,600m^2$ area around the initial deployment point) without any impact to the video transmission quality since the *flying RSU investigator* is directly connected to the LTE base station. However, when IEEE 802.11s is employed, the drone maneuverability is somewhat limited. As indicated in Table I and Fig. 5c, the frame lost and delay increase significantly when the coverage area is greater than $900m^2$ due to the increase in the link failures that may



(a) Background traffic impact on delay (b) Number of hops impact on delay (c) Drone maneuverability impact on delay

Fig. 5: End-to-end Delay performance under different conditions

occur when drones move away from each other to exceed the transmission range of 120m. In this case, these drones cannot hear each other and thus are unable to maintain the mesh pairing, which eventually causes the link failures.

V. Conclusion

In this paper, we proposed to use a swarm of autonomous drones as the multi-purpose RSU that can assist first-responders to carry out some initial assessments in ITS scenarios. We also considered the security issue of the first responders on accessing the swarm and proposed a security framework to ensure the confidentially and limited access to the drone. The feasibility of our proposed approaches are evaluated in ns-3.

The results indicated that the background traffic in the public LTE network does not have a significant impact to the effort to provide a real-time video streaming to the control center/first responders with the minimum frame loss. The use of IEEE 802.11s in the LTE blank spot area also shows promising results with a small percentage of frame lost, while adding some end-to-end delay to the multimedia traffic as the hops increases. The drone maneuverability however, may cause a significant frame lost when IEEE 802.11s is used in a wide area, while LTE is less susceptible to the drone movements.

For future work, we plan to investigate the path selections mechanisms used in the wireless mesh network to reduce end-to-end delay.

Acknowledgment

This work is supported by Qatar National Research Fund (QNRF) under the grant number NPRP-9-257-1-056.

References

[1] M. Alam, J. Ferreira, and J. Fonseca, *Introduction to Intelligent Transportation Systems*. Springer International Publishing, 2016, pp. 1–17.

[2] H. Menouar, I. Guvenc, K. Akkaya, A. S. Uluagac, A. Kadri, and A. Tuncer, "Uav-enabled intelligent transportation systems for the smart city: Applications and challenges," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 22–28, March 2017.

[3] S. Greengard, "Automotive systems get smarter," *Commun. ACM*, vol. 58, no. 10, pp. 18–20, Sep. 2015.

[4] X. Wu, S. Subramanian, R. Guha, R. G. White, J. Li, K. W. Lu, A. Bucceri, and T. Zhang, "Vehicular communications using DSRC: challenges, enhancements, and evolution," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 399–408, 2013.

[5] O. K. Tonguz and W. Viriyasitavat, "Cars as roadside units: a self-organizing network solution," *IEEE Communications Magazine*, vol. 51, no. 12, pp. 112–120, December 2013.

[6] D. Kim, Y. Velasco, W. Wang, R. N. Uma, R. Hussain, and S. Lee, "A new comprehensive rsu installation strategy for cost-efficient vanet deployment," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 4200–4211, May 2017.

[7] "IEEE standard for information technology–telecommunications and information exchange between systems–local and metropolitan area networks–specific requirements part 11: Wireless lan medium access control (MAC) and physical layer (PHY) specifications amendment 10: Mesh networking," *IEEE Std 802.11s-2011*, pp. 1 –372, 10 2011.

[8] E. D. Hardt, "Rfc 6749 - the oauth 2.0 authorization framework," October 2012. [Online]. Available: https://tools.ietf.org/html/rfc6749

[9] ns 3, "ns-3: network simulator 3," Release 3.27, 2017. [Online]. Available: http://www.nsnam.org/

[10] J. Klaue, B. Rathke, and A. Wolisz, "Evalvid – a framework for video transmission and quality evaluation," in *Computer Performance Evaluation. Modelling Techniques and Tools*, P. Kemper and W. H. Sanders, Eds. Springer Berlin Heidelberg, 2003, pp. 255–272.

[11] R. Sivaraj, A. K. Gopalakrishna, M. G. Chandra, and P. Balamuralidhar, "Qos-enabled group communication in integrated vanet-lte heterogeneous wireless networks," in *2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2011, pp. 17–24.

[12] R. Atat, E. Yaacoub, M.-S. Alouini, F. Filali, and A. Abu-Dayya, "Delay-sensitive content distribution via peer-to-peer collaboration in public safety vehicular ad-hoc networks," *Ad Hoc Networks*, vol. 16, no. Supplement C, pp. 182 – 196, 2014.

[13] E. Yaacoub, F. Filali, and A. Abu-Dayya, "Qoe enhancement of svc video streaming over vehicular networks using cooperative lte/802.11p communications," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 1, pp. 37–49, 2015.

[14] S. Ucar, S. C. Ergen, and O. Ozkasap, "Multihop-cluster-based ieee 802.11p and lte hybrid architecture for vanet safety message dissemination," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 4, pp. 2621–2636, 2016.

[15] A. Bazzi, B. M. Masini, A. Zanella, C. D. Castro, C. Raffaelli, and O. Andrisano, "Cellular aided vehicular named data networking," in *2014 International Conference on Connected Vehicles and Expo (ICCVE)*, Nov 2014, pp. 747–752.

[16] N. Saputro, K. Akkaya, and S. Tonyali, "Addressing network interoperability in hybrid IEEE 802.11s/LTE smart grid communications," in *IEEE 41st Conference on Local Computer Networks (LCN)*, Nov 2016, pp. 623–626.

[17] N. Saputro, S. Tonyali, K. Akkaya, M. Cebe, and M. Mahmoud, "Efficient certificate verification for vehicle-to-grid communications," in *Future Network Systems and Security*, R. Doss, S. Piramuthu, and W. Zhou, Eds. Springer International Publishing, 2017, pp. 3–18.

[18] "Ieee standard for information technology– local and metropolitan area networks– specific requirements– part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 6: Wireless access in vehicular environments," *IEEE Std 802.11p-2010*, pp. 1–51, July 2010.

[19] 3GPP, "Evolved universal terrestrial radio access (E-UTRA) and evolved universal terrestrial radio access network (E-UTRAN)(3GPP TS 36.300, version 8.11. 0 release 8), 2009," *ETSI TS*, vol. 136, no. 300, 2011.

[20] B. C. Neuman and T. Ts'o, "Kerberos: an authentication service for computer networks," *IEEE Communications Magazine*, vol. 32, no. 9, pp. 33–38, Sept 1994.