# A Survey of 5G Security Considerations

Michael L. Casey
Ingram School of Engineering
Texas State University
San Marcos, Texas, USA
e-mail: mc74@txstate.edu

Stan McClellan
Ingram School of Engineering
Texas State University
San Marcos, Texas, USA
e-mail: sm65@txstate.edu

***Abstract*—The 5G cellular standard is scheduled to begin the first phase of implementation in 2020. The requirements of new services and, therefore, new security requirements, architectures, and technologies mean the new standard will have a very different appearance relative to the prior standard. This paper surveys some key aspects of the 5G standard, and discusses the effect of security considerations in the context of new 5G features.**

***Keywords - 5G standard; wireless communications.***

## I. INTRODUCTION

THE advent of the 5G cellular standard means new services will become available in addition to conventional voice, text, and data. Many of these services are forecast to be present in the first phase of implementation in 2020 [1], including support for capabilities related to vehicular communications [2], wearables, healthcare, transportation, and the Internet of Things (IoT) [3]. These "vertical services" are a new aspect of 5G networks, which bring a new dimension to the design problem, requiring additional research and pre-planning for deployment. Here, we present a review of current technology and how different aspects of the security features will impact those technologies.

Vertical services are an important aspect of the 5G network. The requirements of these dedicated or industry-specific solutions provide much of the motivation for the transition to 5G-enabled technologies. The eight key verticals addressed by the 5G architecture include the following: Manufacturing, Media/Entertainment, Public Safety, Public Transport, Healthcare, Financial Services, Automotive, and Energy/Utilities markets [4]. Previously, these industries employed dedicated, single-use networks or other industry-specific communications solutions. With the contemporary shift of most activities to data-driven commerce, it is logical that public telecommunications networks would respond with a broad-based and ubiquitous solution such as 5G. However, the disparate requirements of these vertical markets create a number of difficult challenges.

The requirements imposed on the network by the eight key verticals can be viewed in terms of Operational, Functional, and Performance categories [4]. Each of these categories has specific requirements, as listed in Table 1. The approach to achieving these often contradictory or mutually exclusive requirements is via the implementation of dynamic, programmable, segment-specific virtualized subnetworks. These isolated 5G subnetworks are known as "slices" and are implementations of the business model of Networking as a Service (NaaS).

TABLE 1: VERTICAL INDUSTRY REQUIREMENTS FOR 5G

| **Operational** | **Functional** | **Performance** |
|---|---|---|
| Self Managing/Policies | Security | Latency |
| Programming Interfaces | Identity Management | Throughput |
| Service Assurance | Isolation | Reliability/Availability |
| Charging/Billing | | Resiliency |
| Global Operation | | Coverage |

As key enabling concepts in 5G networks, network slices are a drastic paradigm shift from the management of conventional telecommunications networks. Network slices are logical networks implemented on a common, shared infrastructure. They are required to accommodate the large variety of vertical services and the disparate service requirements imposed on the network by each vertical service. In most cases, slices are viewed as an "on demand" meta-service which optimizes Operational, Functional, and Performance requirements for various use cases, service types, and business models. In their most basic form, network slices are groups of functions, resources, and connections, which enable certain types of application services, which bound certain important performance requirements, and which ensure specific service-level agreements between users and providers. In this context, it is clear that one of the most critical aspects of network slicing is the ability of the infrastructure to isolate a multiplicity of slices. Isolation is a key component of the general concept of "security," where the isolated slice benefits from (a) greatly reduced attack vectors, (b) highly segregated internal and operational data, and (c) intelligent limitations on connectivity via restricted architecture.

 ISBN: 978-1-61208-623-1

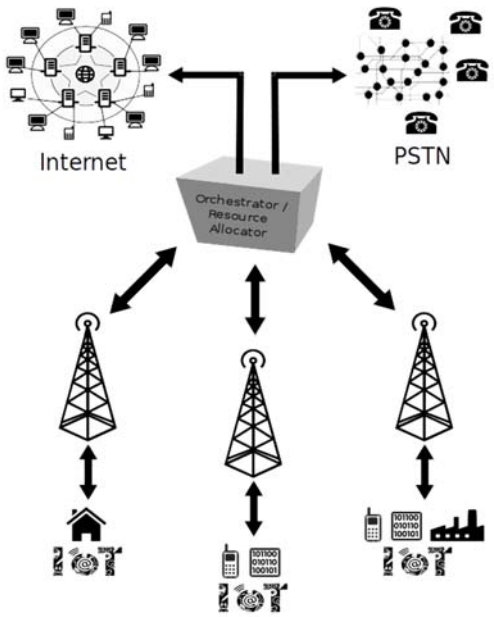


Figure 1: Illustration of network slices

Figure 1 presents a simplified perspective of three different network slices. The Internet and Public Switched Telephone Network (PSTN) are connected in the 5G network. Each tower represents a connection with different network needs. The tower on the left side of the figure needs data connectivity for IoT activities in a suburban setting. The tower in the middle of the figure needs multiple resources for mobile units. The tower on the right side of the figure has mixed needs. In all cases, the network resources needed for the subnetworks addressed by each tower are different. Each tower needs the ability to create its own Virtual Private Network (VPN) in order to serve the connected mobile units or other equipment. This VPN constitutes a slice of network resources. The slice could involve multiple service providers, e.g. a server for cloud storage, a company supplying the physical infrastructure, and a voice network. These different service providers have their own respective domains within the network structure. The subdivision of the slice among the different service providers must be designed carefully to delineate where liability and security needs for one service provider end and liability and security needs for another service provider begin. The slices and their subdivisions need to be isolated from one another since the security needs are different for different slices as well as the subdivided domains.

An important component in Figure 1 is the Orchestrator / Resource Allocator (ORA). The ORA is responsible for creating end-to-end realizations of services, which are requested by network-resident applications. Such applications request network services, which may span multiple operating domains and may be expressed in abstract fashion, via a common Application Programming Interface (API). A primary function of the ORA is to translate abstracted service requests into resource requests to be handled by controllers in the various domains. Additionally, the ORA maps SLA requirements and Quality of Service (QoS) requirements into formats to be managed by domain-specific controllers. The three slices seen in Figure 1 are likely to change with respect to time; therefore, the changing needs will mean a new instance of a slice will need to be managed by the ORA. Since the concept of "security" in the 5G network is logical rather than physical, the ORA will also have to be virtualized, and the complexity of the ORA will be quite substantial.

The remainder of this paper explores the highlights and important aspects of the Functional Requirements in 5G networks, or the extended concept of "security." The intent is to introduce the reader to tradeoffs, architectures, and considerations which may pervade ongoing implementations and standardization efforts. This discussion is undertaken in the context of requirements for the several vertical markets, and illustrates how security concerns arise in certain cases. For example, vehicular communications are an important "vertical service" in the 5G standard which contain a number of different and considerably complex scenarios [1][2]. Connected cars will be expected to interface seamlessly with the 5G network, just as many cars already connect easily to the 4G/Long-Term Evolution (LTE) network. Additionally, this discussion is undertaken in the context of technologies that are addressed by 5G implementations. For example, integration of IoT systems is an important set of technologies, which will be challenging in the development and deployment of 5G networks [3]. IoT systems will impact canonical network layers (e.g. MAC, PHY) and other vertical services, and will drastically alter the security landscape of the overall network. A brief historical perspective is discussed based upon [5], which was written for 5G Public Private Partnership (5GPPP) and [3] which was written for 3GPP. Also included in the discussion are use cases and performance evaluation models from 5GPPP, and issues related to IoT from 3GPP. While many of the 5G requirements are not globally unique, certain aspects may be designed and adapted to fit local geography, specific use cases, or regulatory requirements. From these aspects and other architectural concerns, it is clear that new security mechanisms, architectures, and technologies are required to manage various aspects of the 5G network.

Section II reviews the features of the security protocol for 5GPPP. Section III reviews the security implications for vehicular communications. Section IV review security implications for IoT. Section V reviews the beginning of the design of the security protocol from the 3GPP perspective. Section VI concludes the paper.

## II. 5GPPP SECURITY LANDSCAPE

Security risks in modern network communications are of utmost importance. Developing 5G networks are no different, and security aspects of 5G include issues such as: unauthorized usage/access, weak slice isolation, traffic embezzlement, service level agreement (SLA) compliance,

 ISBN: 978-1-61208-623-1 

slicing versus neutrality, trust management, service provider lock-in, and insufficient technology readiness levels (TRL) [2]. Each of these items is briefly discussed below.

**Unauthorized usage/access**: Unauthorized usage/access of assets has several security risks clearly identified. One known risk is that of identity theft or cloning. Subscriber credentials may also be stolen or cloned. The desired seamless interworking between different domains, e.g. a vertical slice or a core slice, may expose the 5G security level to new threats. Another identified risk is that of allowing appropriate security measures for massive IoT deployments while still accounting for necessary security of non-IoT services. The security features must account for all of these requirements, which will likely produce a heterogeneous access security protocol.

**Weak slice isolation**: If the isolation of the slices is weak, then side channel attacks are a distinct possibility as a security risk. Likewise, management of sensitive data in one security domain may be exposed in another security domain due to a different set of security requirements. Monitoring and management of security protocols across all the security domains implies substantial additional complexity in the interfaces between various slices.

**Traffic embezzlement**: The specific security risk in traffic embezzlement lies in the weakness of third parties being able to capture or alter control plane data or user plane data without detection. The heart of this risk lies in the inconsistency between three logical segments: the Orchestrator abstraction, the software defined network (SDN) abstraction, and the physical and network resources. This weakness is of critical concern to use cases such as eHealth and lawful interception due to recursive/additive virtualization.

**SLA compliance**: Several security risks, which could be called vertical SLA and regulation compliance management risks, have been identified by the standards authors. One risk is encountered when an API is used to request geolocation information. This API request must be clear to the user and managed correctly so that information reaches its correct network destination as well as satisfying the requirements of the third party making the request. The third party may also be requesting access to a user's infrastructure or assets, and the orchestrator must manage this request in conjunction with the third party. With virtual network functions (VNFs), a clear liability chain must be present to protect the user, the orchestrator, and the third party. Also, VNF life cycles must provide evidence that they will not passively introduce additional security risks to the network via updates and software evolution. Unfortunately, the management of these life cycles are outside the control of the operator.

**Slicing vs. neutrality**: The concepts of network neutrality and slicing are yet to be fully defined by the standards authors in [1]. While some regulations exist within the EU, the regulations do not fully define how to navigate the remaining differences between network neutrality and slicing. Delivering services via a 5G network outside of applicable regulations or in the absence of fully-formed regulations is a clear risk.

**Trust management**: Current trust management protocols do not account for the diversity to be found in the 5G infrastructure. Given the vertical services (as one dimension to the 5G infrastructure) and slicing between security domains and layers (as another dimension to the 5G infrastructure), trust management protocols must be able to span both dimensions simultaneously. Therefore, liability must be considered as the question of which party (a delegated third party or otherwise) is responsible for which part of the chain in a vertical service. Answering this question will be part of the design of the overall security protocols for the 5G standard, and may lead to unwanted or unsupportable system complexity.

**Service provider lock-in**: Each tenant/owner of a network slice must be flexible with their services and infrastructure without negatively affecting security SLAs. A tenant/owner may offer a service in one slice of the network while the supporting infrastructure spans multiple domains. If the 5G security protocol is not designed to account for these needs, then a tenant/owner would be locked in to a single domain and unable to fully exploit the 5G standard; therefore, a common standard must be designed with flexibility for migration as a defining feature.

**Insufficient TRL**: The final version of the security standard will not be fully available during the first phase of deployment (2020). The security requirements of the 5G standard illustrate the insufficient TRLs by exposing new vulnerabilities of the new technologies, which the technologies may not be fully able to mitigate. Designers propose using a "bridge" version of the security standard for the first phase of deployment in 2020 to allow new and non-mature technologies to begin using the 5G standard while adapting and maturing in the time leading up to the final phase of deployment. The "bridge" version may be viewed as a precursor to and primer for the fully deployed security protocol.

Furthermore, security requirements will have to consider which tasks are for which canonical network layer, or which party in the vertical service bears the burden of managing certain functional aspects of the implementation. Additionally, the 5G security protocol must interface with legacy systems. This multi-dimensional problem means new security countermeasures must be designed and standardized.

 ISBN: 978-1-61208-623-1 

The multi-dimensional problem of vertical services and the wide range of these services, including health, transportation, and industrial automation applications means the security protocol should be logical instead of physical. This supports solutions to other problems since many network functions will be virtualized in order to support the vertical services while still working within the framework of physical infrastructure to be implemented. For example, unwanted traffic detection could be based upon an intercept-perceive-decide-execute (IPDE) model. This model is a forward-looking method of detecting (intercepting) problems (unwanted traffic) as they occur, perceiving how the unwanted traffic occurs, deciding how to counteract the unwanted traffic, and executing the chosen countermeasure. These functional components of the virtualized network service would necessarily have to be implemented in multiple canonical network layers spread among multiple physical systems.

Prior European security architectures, including TS 23.101 [6], may be modified slightly in order to account for the new security requirement as well as the context of virtualized network functions (VNFs). Likewise, access control adds a level of complexity to determining which provider in the vertical service is responsible for which aspect and level of security. A privacy-by-design approach is required to accommodate greater awareness of privacy concerns among users.

One possible solution for the three main use cases (cloud, mobile, and IoT) may include forms of attribute-based encryption (ABE). ABE extends and generalizes the concepts of public-key encryption, where users have a private (secret) key as well as a public (accessible) key, and private 1:1 communication with the holder of the private key is possible when messages are encrypted with the public key. In ABE, the encryption keys and encrypted messages may be dependent on sets of user-specific attributes, and may be associated with access policies. As a result, data is encrypted via attributes and/or policies related to groups of target users rather than via each user's public key. Thus, messages can only be decrypted by users whose attributes align with the intended requirements, and/or who satisfy the intended policies.

## III. V2X: VEHICULAR CONNECTIVITY

Considering the transport vertical services [3], short and long range communications standards will be necessary [3], and they will be required to dovetail with the 5G standard. Transportation services typically are referred to as "Vehicle-to-anything" (V2X) which encompasses the four component services listed in Table 2. Primary use cases in V2X scenarios include activities such as automated driver assistance systems (ADAS), situational awareness, mobility services, and auxiliary services/comfort. Two highly desirable auxiliary service use cases include dynamic route guidance and having municipalities connect to vehicles denoting the locations of available parking, which would provide a mechanism for conserving fuel. Key risks are summarized in [7]-[9]. In the US, Europe, and China multiple projects and testing sites have been leveraged to understand the different foci of the V2X spectrum in different locations.

TABLE 2: 5G VEHICULAR SERVICES

| Service | Description |
|---|---|
| V2V | Vehicle-to-Vehicle |
| V2I | Vehicle-to-Infrastructure |
| V2N | Vehicle-to-Network |
| V2P | Vehicle-to-Pedestrian |

Contemporary communications technologies, such as 4G/LTE and dedicated short-range communications (DSRC), have shown promise in V2X applications. DSRC is a two-way, short-range wireless technology that provides high throughput for active safety applications [10] and is based on a conventional implementation of frequency-division multiplexing (FDM). In some respects, 4G/LTE V2X communications may provide operational advantages over DSRC. As new V2X use case appear, become possible, or become desirable, the Society of Automotive Engineers (SAE) J2735 [11] dictionary already has the necessary flexibility to adopt these new use cases. J2735 has a dictionary of at least 16 messages with more than 230 elements, which means LTE adaptation and adoption of LTE V2X is likely because most use cases are already included. Additionally, the connectivity/platform for road operators, certificate and certificate revocation list distribution, range extension, and roadside unit (RSU) backhaul can be done on the LTE network, which provides business value for mobile providers. However, in comparison testing, 4G/LTE has been shown to lack important characteristics for many real-time V2X scenarios. For example, the cellular handoff mechanisms required by 4G/LTE implementations resulted in long lag-times for collision avoidance, and although 4G/LTE has extended range, it is not effective when high throughput and/or point-to-multipoint connections are required [12]. As a result, and even though it may be cost-prohibitive in certain scenarios, DSRC may continue to dominate V2X communications technologies and intelligent transportation systems for near-term applications, as many manufacturers are already implementing DSRC systems in some or all of their vehicles.

While incumbent technologies such as 4G/LTE and DSRC may prove useful in V2X applications, the exploitation of the 5G standard and IEEE 802.11p [13] could solve current and future problems altogether. Unfortunately, IEEE 802.11p has not been updated to account for multiple transmit and receive antennas and other optimizations such as Multiple Input/Multiple Output [MIMO] and beamforming), or advanced modulation and channel access techniques (orthogonal frequency-division multiple-access, or OFDMA), which may become important aspects of V2X technologies in the future. And, again, security issues arise. The Security Credential Management System (SCMS) will have to be designed to account for multiple authorities across several network functions in the virtualized 5G network. The design,

 ISBN: 978-1-61208-623-1 

for the sake of privacy, will have to be such that no one authority has enough information to track a vehicle for a long period of time. Instead, a lawful intercept (LI) will bring together enough pieces of the total picture of a vehicle's data to track them, and an entity with a LI will never have all of the pieces of the picture. The disparate security requirements of the different services to be provided causes the design of the security protocol to have increased complexity. Furthermore, the security protocol design must account for how strong (or weak) the slicing must be between the different providers in this vertical service.

## IV. The Internet of Things (IoT)

IoT is a widespread aspect of the 5G standard. IoT has two main use cases: critical and massive [4]. These use cases have key differences between them. Critical IoT must have low latency and high reliability because it provides connectivity cases such as public safety. Massive IoT requires that devices be inexpensive with multi-year battery lives; low latency and high reliability are desirable if they can be designed into the device, otherwise these features need not be present.

Enterprise applications comprise a third use-case, which will address needs serving vertical services. Typical needs may include personal digital assistants or insurance telematics. The primary market drivers include applications such as connected wearables, cars, homes, cities, and industrial IoT. Vertical requirements will depend upon the operator's perspective, and the operator will have requirements to a greater or lesser degree depending up on the services they provide. Typical functional requirements include traffic patterns, identity/security, simple installation, mobility, SLAs, reliability, sector regulations, analytics, and charging efficiency. To address these requirements, 3GPP Rel.14 [14] was enhanced to improve positioning capabilities, greater multicast downlink transmission, mobility awareness, higher data rates, and packetized voice via voice-over-LTE (VoLTE). These enhancements provide for third party and group-based communications with better support in the radio aspect.

Of special note is the use case regarding private and other networks that intend to use unlicensed or shared spectrum. In most instances, basic capabilities exist in wireless ("WiFi" or IEEE 802.11x) [13] and wired Ethernet [15] to create network partitions. For example, wireless partitions can be created in unlicensed spectrum using the Service Set Identifier (SSID or "network name"), and wired partitions can be created using Virtual LANs (VLANs). Both of these approaches create isolated traffic via a shared infrastructure, which is a foundational capability for 5G networks. However, the overlapping or simultaneous use of licensed and unlicensed wireless spectra can be more complicated.

One promising approach in this regard is the concept of Licensed-Assisted Access (LAA), which is standardized in 3GPP Rel.13 [16] and enhanced (eLAA) in 3GPP Rel.14 [14]. LAA and eLAA provide systems based on 4G/LTE the ability to operate using unlicensed spectrum. Via a combination of techniques, including dynamic channel avoidance and "listen before talk," these hybrid systems can coexist efficiently. MuLTEfire is the tradename for Qualcomm's implementation of LAA/eLAA [17]. MuLTEfire exploits parts of LAA for downlink and eLAA for uplink transmissions. In trials, MuLTEfire has been shown to coexist fairly with WiFi in a fashion which can roughly double overall system throughput. Future releases of MuLTEfire will include IoT-specific enhancements. Private networks using MuLTEfire will have to meet the new security requirements for the disparate services to be provided so that they complete the private tasks necessary to them while operating seamlessly within the new standard, within the unlicensed spectrum, and without degrading the security requirements across disparate domains of providers.

## V. Use Cases & Performance Evaluation Models

Although highly preliminary, a starting point is necessary for understanding whether or not an aspect of the 5G standard will work. In [5], the authors provide a background setting of how testing was to be conducted, and whether it could be applied to almost all aspects of the 5G standard. The beginning of the roadmap denotes use cases meant to encompass the entire standard, namely: device density, mobility, infrastructure, traffic type, user date rate, latency, reliability, availability, and 5G service type (e.g. machine type communication, or MTC). Key performance indicators (KPIs) are sorted based upon their evaluation method, and those methods are inspection, analysis, or simulation. Furthermore, vertical services will have security requirements and localized needs/requirements. Vertical services have a set of use cases to which these KPIs apply. The use cases are dense urban, broadband everywhere, connected vehicles, future smart offices, low bandwidth IoT, and tactile internet/automation. These use cases are mapped to vertical services use cases, including automotive, eHealth, energy, media and entertainment, and factories of the future. The KPIs and the use cases cover most, if not all, of the needs presented by the 5G standard.

Analysis methods have been developed and have been applied to measure such details as control plane latency ([5], Table 3), user plan latency ([5], Table 4), massive MTC (mMTC) device energy consumption improvement ([5], Table 5), inter-system handover, interruption time, mobility interruption time, and peak data rate. Although these measurements and calculations are simple to complete, they provide benchmarks regarding device performance with respect to the new network.

These benchmarks need to be measured in the different contexts of the use cases even though not all use cases occur in all contexts. A context is a specific configuration for a BS, and contexts being considered for the 5G standard include indoor hotspot, urban macro, outdoor small cells, and rural macro/long distance configurations.

## VI. Conclusion

This paper set out to explore several aspects of the 5G cellular standard with respect to security issues as the focus. The paper explores the general security protocol design as

 ISBN: 978-1-61208-623-1 

written by 5GPPP; the V2X communications standard results from research completed by the 3GPP; the IoT results from research completed by the 5GPPP; and the general design of 5G cellular standard with respect to the use cases and how to measure, via KPIs, when the use cases were being met. Security is a common thread among the use cases as well as the vertical services to be used by the 5G cellular standard. Security concerns are noted in each of the aspects. The general security protocol design written by the 5GPPP provides an introduction to the issue itself. The V2X and IoT aspects highlight how the general security protocol could or does impact implementation in these specific vertical services. Both V2X and IoT aspects will result in enormous numbers of additional network nodes, each of which presents numerous threat vectors. Additionally, Network as a Service (NaaS) or slicing is one approach to reconciling competing priorities. However, slicing produces a host of additional issues related to virtualization, automation, and guarantees of isolation. Whether the discussion is about network and infrastructure or vertical services, security is a concern affecting both the vertical services and use case dimensions at all levels, and security is a concern that arises even when security is not the specific focus.

## ACKNOWLEDGMENT

The lead author would like to acknowledge the contribution of Dr. George Koutitas, Texas State University.

## REFERENCES

[1] 5GPPP (2017 June). “5G PPP Security Landscape.” [Online] https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf [accessed Sept. 2017]

[2] 5G Americas (2017 Oct.). “V2X Cellular Solutions.” [Online] http://www.5gamericas.org/files/2914/7769/1296/5GA_V2X_Report_FINAL_for_upload.pdf [accessed Sept. 2017]

[3] 5G Americas (2017 Dec.). “LTE Progress leading to the 5G Massive Internet of Things.” [Online] http://www.5gamericas.org/files/8415/1250/0673/LTE_Progress_Leading_to_the_5G_Massive_Internet_of_Things_Final_12.5.pdf [accessed Sept. 2017]

[4] Global Mobile Suppliers Assoc. “5G Network Slicing for Vertical Industries.” [Online]. https://gsacom.com/paper/5g-network-slicing-vertical-industries/ [accessed Sept. 2017]

[5] 5GPPP (2016 April). “5G PPP Use Cases and Performance Evaluation Models.” [Online] https://5g-ppp.edu/wp-contents/uploads/2014/02/5G-PPP-use-cases-and-performance-evaluation-modeling_v1.0.pdf [accesed Sept. 2017]

[6] 3GPP TS 23.101, “General Universal Mobile Telecommunications System (UMTS) architecture” [Online] http://www.3gpp.org/dynareport/23-series.htm [accessed Feb. 2018]

[7] National Transportation Library (2016 Sept.). “Connected Vehicle Pilot Deployment Program Phase 1 – Deployment Readiness Summary – New York City.” [Online] https://rosap.ntl.bts.gov/view/dot/31731 [accessed Sept. 2017]

[8] National Transportation Library (2016 Sept.). “Connected Vehicle Pilot Deployment Program Phase 1 – Deployment Readiness Summary – Tampa (THEA).” [Online] https://rosap.ntl.bts.gov/view/dot/31721 [accessed Sept. 2017]

[9] National Transportation Library (2016 Sept.). “Connected Vehicle Pilot Deployment Program Phase 1 – Deployment Readiness Summary – ICF/Wyoming.” [Online] https://rosap.ntl.bts.gov/view/dot/37124 [accessed Sept. 2017]

[10] S. Sill. “DSRC: The future of safe driving.” Intelligent Transportation Systems Joint Program Office. [Online] https://www.its.dot.gov/factsheets/dsrc_factsheet.htm [accessed Feb. 2018]

[11] SAE J2735. DSRC Message Set Dictionary. [Online] https://www.sae.org/standards/content/j2735_200911/ [accessed Feb. 2018]

[12] Z. Xu et.al. “DSRC versus 4G-LTE for Connected Vehicle Applications: A Study on Field Experiments of Vehicular Communication Performance,” Journal of Advanced Transportation, Volume 2017 (2017), Article ID 2750452, Aug. 2017. [Online] https://doi.org/10.1155/2017/2750452 [accessed Feb. 2018]

[13] IEEE 802.1, Wireless Local Area Networks, The Working Group for WLAN Standards [Online]. http://www.ieee802.org/11/ [accessed Feb. 2018]

[14] 3GPP Release 14. [Online]. http://www.3gpp.org/release-14 [accessed Feb. 2018]

[15] IEEE 802.3, Ethernet Working Group [Online]. http://www.ieee802.org/3/ [accessed Feb. 2018]

[16] 3GPP Release 13. [Online]. http://www.3gpp.org/release-13 [accessed Feb. 2018]

[17] D. Malladi, “Best Use of Unlicensed Spectrum,” Qualcomm, Feb. 3, 2016. [accessed Feb. 2018]

 ISBN: 978-1-61208-623-1 