Service Level Agreements for 5G-Enabled Healthcare Systems: Challenges and Considerations

Haneya Naeem Qureshi, Marvin Manalastas, Ali Imran, and Mohamad Omar Al Kalaa

Abstract

5G and Beyond 5G (B5G) communication networks, with their characteristics of increasing speed, connectivity, reliability, availability and capacity while reducing latency, have the potential to transform the healthcare sector by opening possibilities for novel healthcare use cases and applications. Service level agreements (SLAs) can help enable these new healthcare use cases by documenting the communication requirements, performance standards, and roles and responsibilities of the stakeholders involved in providing safe and effective 5G-enabled healthcare to patients. However, the peculiarities and nuances of 5G implementations give rise to gaps in this area that should be addressed to streamline the implementation of 5G technology in healthcare. This article highlights the key challenges and describes open research questions related to SLAs for 5G-healthcare systems. Addressing the research challenges in this space will help in developing robust SLAs that can ensure that device manufacturers, network service providers, users, and regulatory authorities share a common framework to safely integrate 5G & B5G technology in healthcare.

Introduction

5G technology is revolutionizing the healthcare sector by both augmenting current medical practices with 5G connectivity and enabling new use cases and applications. Emerging use cases of 5G-enabled healthcare include remote robotic-assisted surgery, in-ambulance diagnosis and treatment by remote physician, pervasive wearable and implantable devices or massive IoT, remote diagnosis and teleconsultation, service robotics for assisted living, and facilitating big data management of healthcare data [1]. Different use cases require different quality of service (QoS) guarantees as shown in Fig. 1, which illustrates some 5G-enabled healthcare use cases and qualitatively highlights several communication key performance indicators (KPIs) requirements for each. Inspired by several sources including [2], combined with domain knowledge, we identify commonly used KPIs to highlight the uniqueness of different healthcare use cases in Fig. 1. Among these KPIs, latency is the time required for data to travel between the transmitter and receiver; data rate is the speed at which data is transferred; mobility-related KPIs such as handover failures and radio link failures measure the capability of the network to seamlessly transfer users between network nodes; and reliability is a measure of how well a connection can be maintained between a user and the network after initial establishment. For example, while energy efficiency might be important for wearable and implantable devices, it might not be so significant in other use cases like remote robotic-assisted surgery. Similarly, mobility related KPIs are more important for use cases such as connected ambulance on the move compared to their values to the static use case of telesurgery. Therefore, it is important to properly document the communication requirements of each application and ensure that those requirements are met to successfully enable the different 5G-enabled healthcare applications. Such documentation can be done through service level agreements (SLAs) between a service provider and the consumer. An SLA details the various aspects of services that the service provider will provide to the consumer, which include but are not limited to performance metrics and guarantees, service level failure and indemnification clauses, service level monitoring process, security and privacy management frameworks, and costs, among others. Thus, SLAs can provide assurance of the guaranteed level of services for facilitating 5G-healthcare use cases.

However, the unique technical characteristics and peculiarities of emerging 5G and B5G technologies make the traditional practices and procedures across SLA stages inadequate for 5G and B5G enabled healthcare. In this article, we discuss these challenges and limitations in various stages of the traditional SLA establishment processes and clarify gaps for addressing 5G-enabled healthcare applications. We also highlight future research directions and open questions in this area that should be addressed in evolved 5G-enabled healthcare SLAs to facilitate the implementation of safe and effective 5G-enabled healthcare.

Challenges in SLA Stages for 5G-Enabled Healthcare

The stages of traditional SLA establishment are summarized in Fig. 2. On a high level, the existing approach of SLA development is divided into four major parts. The first is the *development* phase, comprised of stages 1 to 6 in Fig. 2; second is the fulfilment phase which includes stages 7 and 8; followed by the *monitoring* and *assurance*

DISCLAIMER
The mention of commercial products, their sources, or their use in connection with material reported herein is not to be construed as either an actual or implied endorsement of such products by the Department of Health and Human Services.

Haneya Naeem Qureshi (corresponding author) and Mohamad Omar Al Kalaa are with the U.S. Food and Drug Administration; Haneya Naeem Qureshi is also with the University of Oklahoma; Marvin Manalastas and Ali Imran are with the University of Oklahoma.

Digital Object Identifier: 10.1109/MNET.011.2100343

phases reflected as stages 9 and 10, respectively. As shown in phase 1 of Fig. 2, a review and clarification of healthcare service needs and priorities is done first. For example, a hospital establishing a telesurgery system would communicate to the network provider the desired network performance needs such as requirements for latency and reliability. The network provider would

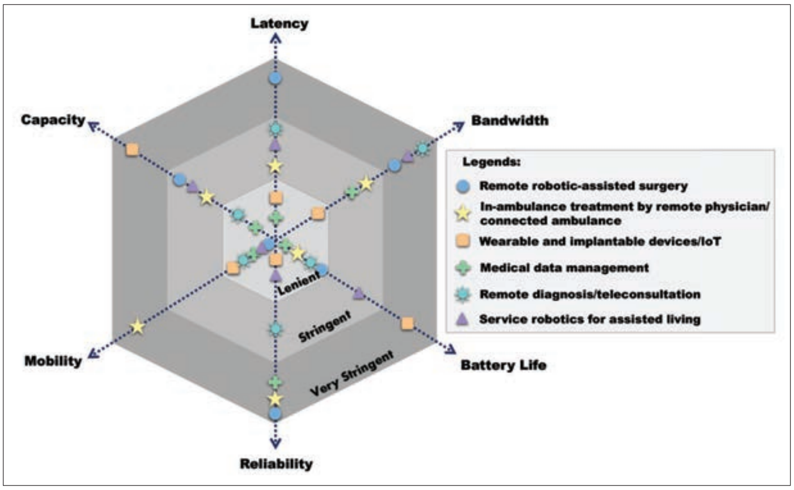

FIGURE 1. Some 5G-enabled healthcare applications and their different degrees of expected requirements. The three tiers of the hexagon indicate the level of expected requirements. The innermost tier corresponds to lenient KPI requirement, the middle tier corresponds to stringent KPI requirement and the outermost tier corresponds to highly stringent KPI requirement. For example, remote robotic-assisted surgery needs *very stringent* latency, data rate and reliability requirements, *stringent* capacity requirement and lenient battery life and mobility requirements.

then identify performance limitations based on its capabilities if applicable (e.g., telesurgery system users might require 5 ms latency, but the network provider is able to provide no less than 10 ms). In phase 2, an agreement on expectations is reached after addressing potential concerns over the expectations and requirements of both healthcare application provider and network provider. The third phase is planning, in which ground rules, communication styles, and preferences are established for working together. The division of responsibilities is discussed and any scheduling issues and constraints (e.g., timelines for the start of service, planned service upgrades) are addressed. Moreover, potential roadblocks are identified (e.g., cases where service quality might not be met). In the fourth stage, the initial SLA content is created, including service performance levels (e.g., quantitative guarantees for promised latency, throughput, capacity), fees/penalties and legal issues (e.g., costs of providing the guaranteed levels of performance and what happens if performance levels are not met, indemnification clauses). Finally, after negotiations, the draft agreement is finalized as illustrated in phase 5. In the sixth stage, all stakeholders (e.g., hospital representatives deploying telesurgery equipment, manufacturers, network providers) review the proposed draft. After joint refinement of the SLA, approval from all stakeholders is gained, concluding the SLA development stage.

In the SLA fulfilment stage (starting from phase 7 in Fig. 2) , pre-implementation tasks such as performance tracking mechanisms (e.g., how to measure the latency and throughput while telesurgery

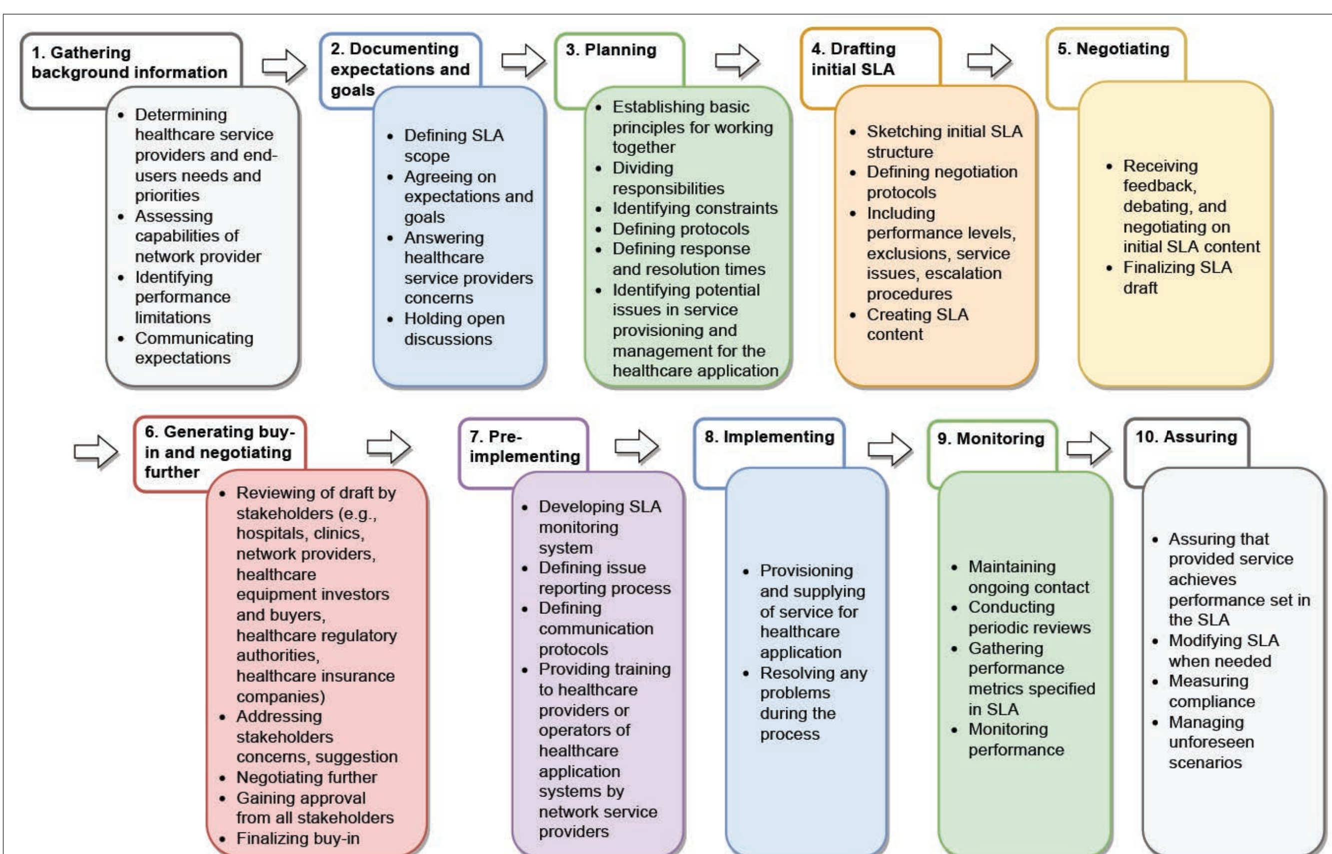

FIGURE 2. Stages of SLA establishment.

is ongoing and who is going to measure it), any training (e.g., the network provider might train the hospital staff on how to switch to a backup system in case of unexpected performance degradation) and communication protocols (e.g., how and where to report a cell outage) are completed. In phase 8., the network provider provisions the agreed service to the hospital (e.g., base stations, access points, cables, configuration).

Phase 9 involves SLA monitoring through the methods specified in the SLA (e.g., manual or automated monitoring through a third-party of specific performance metrics). The last stage is the SLA assurance, in which compliance of the specified performance levels in the SLA is measured and unforeseen circumstances (e.g., cell outage due to severe weather) are managed. It also involves conducting periodic service reviews, and implementing modifications to the SLA, if needed.

However, as detailed as it may seem, this conventional SLA establishment method does not consider the nuances of 5G networks. Some of the unique distinctions in 5G radio access network (RAN) include the presence of a heterogeneous operating environment consisting of multiple frequency bands, operators, and vendors, heterogenous data streams from the widespread use of devices with unique traffic profiles spanning wearable devices to imaging devices with high throughput demand (e.g., 3D computed tomography (CT)). Additionally, the inclusion of mmWave spectrum brings in the challenges of cell discovery, cell association, frequent handovers, and beam alignment issues, all of which are exacerbated in high mobility scenarios [3]. One of the novel concepts of 5G is the signal's highly directional nature, especially in mmWave scenarios, which brings new positioning capabilities that can enable novel healthcare innovations. Unlike legacy 4G networks with a fixed symbol duration, 5G can adapt the numerology in use, for example, the symbol duration and bandwidth, with the service. Furthermore, contrary to 4G networks where resource allocation is performed as multiples of one time slot, 5G minislots can be used to allocate resources to users on the symbol level. These slots can also be aggregated and may pre-empt normal transmission.

Similar to the RAN side, the core side of the 5G network also has evolved and unique characteristics vis a vis the 4G core. A prominent feature is network slicing, where network resources can be allocated according to the different requirements of 5G-enabled healthcare applications [4]. However, the inherent dynamicity of this network architecture makes assessing and managing the risks of communication loss, delay, or disruption complicated as compared to the existing service assurances in legacy networks. This highlights the need to develop new scheduling and resource allocation mechanisms, and network admission control policies in per-slice SLAs. In case a slice is dynamically shared between customers or is expected to serve customers based on priority, SLAs should clarify the details of such mechanisms.

The evolution in 5G RAN and core manifests the need for a parallel evolution in SLA development. However, there are challenges in the various stages of the SLA lifecycle for 5G-enabled applications as summarized in Fig. 3. We describe some of these challenges in this section. For a detailed discussion of these challenges, the reader is referred to a recent article [5].

FIGURE 3. Challenges in SLA stages.

SLA Development

Given the complexity of 5G network deployments with multiple technologies operating on a motley of frequency bands through multiple service providers involved in the 5G ecosystem, developing an end-to-end coordination and management framework between different providers and across the various logical architectures, functional splits and quality of service requirements is a challenging task during SLA development.

A study estimates that a typical 5G node is expected to have around 2000 parameters to be configured and optimized, and this number would scale with an increasing number of nodes (i.e., cell densification in 5G) [6]. The complex interdependencies and trade-offs between these parameters further complicate their optimization. Consequently, documenting the service levels based on the effect of the huge number of parameters and their interdependencies during SLA development is challenging. Moreover, in the 5G network slicing environment, SLA management would lead to specifying the service performance metrics on a per-slice basis. Consequently, the mapping of 5G SLA metrics to 5G network parameters, which is needed to capture the impact of varying 5G network configuration on the desired service level, is not trivial. This also makes it hard to develop network optimization strategies, especially in a slice-enabled environment or with shared slices. For example, determining when and which slices to pre-empt along with their service performance is a challenging task. This increased complexity might also render manual negotiations of SLA metrics and service assurances inefficient during the SLA development stage.

The flexible and dynamic nature of 5G environments and 5G-enabled application requirements can lead to circumstances being left uncovered during SLA development. For example, in a telesurgery use case, the network operator might be allocating a portion of the network on-demand to the hospital where the telesurgery is being performed. This portion

The flexible and dynamic nature of 5G environments and 5G-enabled application requirements can lead to circumstances being left uncovered during SLA development.

would have unique characteristics such as low latency and high reliability. However, these performance characteristics may only be needed for the time scheduled for the telesurgery, which can be variable depending on the complexity and type of surgery. This would require the operator to trade off network efficiency (influenced by factors such as pre-emption policies and resource allocation) and cost savings, while maintaining the guaranteed performance levels promised for the desired variable time.

SLA Monitoring

Performance metrics are defined based on detailed infrastructure-based measurements that can generate large volumes of data. The amount of data generated scales with the infrastructure (increased number of base stations per unit area in 5G ultra-dense networks) and the number of KPIs and technical counters [6]. Identifying the most relevant data streams and generating the associated technical reports can reduce the administrative burden of confirming whether the service quality is met according to the SLA terms. However, capturing pertinent data streams from huge amounts of data is a challenge that is further aggravated when multiple network operators are involved in providing the desired service levels, where each operator might use different vendor-specific monitoring tools, define metrics using its own set of counters and naming conventions, and use unique data formats for data collection.

Monitoring SLA parameters can be done manually. However, given the continuous growth in cell density, importance of developing time saving solutions, and increasing pressure to reduce operational costs, this approach is becoming impracticable [7]. Another way can be the use of a common monitoring tool managed by a third-party. However, this leads to additional challenges of mapping the SLA requirements to the technical configurations of different vendor-specific network equipment used by different operators. An alternative approach for SLA monitoring that accounts for the huge data volume resulting from data collection is the identification of the most relevant data streams and metrics by SLA stakeholders, and then gathering only those data streams to assess service consistency with the SLA terms. However, customers might be interested in acquiring detailed data collection for transparency and traceability or for compliance with external reporting agreements. Therefore, there is a need for developing automated, scalable, and transparent data collection mechanisms for 5G-enabled healthcare SLAs. In addition, the SLA monitoring processes should consider the interoperability of cross-domain modules involving multiple vendors, operators, outsourcing companies, administrative entities, and systems so that end-to-end service provisioning can be assessed in a common platform. This can include different network performance monitors, service and application monitors, virtualization managers, and storage managers to monitor the SLA services using different vendor-defined metrics, counters and naming conventions.

SLA Fulfillment

The evolving capabilities of 5G and B5G can be considered as a challenge since, on one hand, customers can be interested in improving their applications to remain competitive by maintaining up-to-date technology, while on the other hand, this interest might not translate into a financial incentive that encourages the service providers to offer technical capabilities beyond what is needed to meet the established SLA terms. Accordingly, documenting the investment in upgrading the service quality by the service provider and consequently determining the changes in its cost structures constitute challenges for SLA fulfilment with evolving technology. Additionally, the challenge of correlating the quality of services to business value creation and maintaining an acceptable customer cost-benefit ratio, becomes more pronounced with growing enterprise complexity where a large number of internal customer entities have their own requirements and expectations. Another consideration that links business costs to successes and risk sharing models is the determination by SLA stakeholders if and how to consider risk-sharing during SLA fulfilment. Risk management of 5G-enabled medical devices is further elaborated below.

A large number of frequency carriers are used in 5G and B5G networks. Accordingly, a challenge for service providers is to ensure that the users are camped on the optimal carrier according to the service type. An example is determining whether to camp a user on low, medium or high frequency bands according to a specific 5G-healthcare use case. This is an important consideration for minimizing inter-frequency handovers, radio link failures, and voice muting scenarios. In 5G voice services, the predominant problem is call muting, rather than call drops or subpar call quality. Voice muting is a gap in voice packets, which can last for a few seconds and is perceived by the human ears as silence. Call drop means that a call ends unexpectedly. Packet loss has a more noticeable impact on time-critical ultra-reliable low-latency communication (URLLC) applications, such as emergency management scenarios like in-ambulance treatment of a critically ill patient by a remote physician while the patient is en route to the hospital. In such cases, the ambulance might expect to be camped on a low spectrum band since lower frequencies intrinsically have wider coverage than higher frequencies. However, low bands have less bandwidth than high bands, not to mention the spectrum congestion due to the interoperation of legacy technologies such as 2G, 3G, 4G and other services. Accordingly, dynamically deciding which band is best suited for such time-critical applications is challenging during SLA fulfillment.

Another challenge while fulfilling the SLA terms in healthcare scenarios using 5G and B5G is the management of resource allocation dictated by provisions like spectrum sharing, infrastructure sharing, bandwidth adaption, slot aggregation, and mini-slot pre-emption. Typically, user resource requirements vary with time, location and the needed service, where high quality of service is not needed at all times. In such scenarios, trade-offs involving the complexity of managing the network resource reservation, balancing the overall service performance of all customers, maximizing resource utilization, while at the same time minimizing the negative impact to other users caused by mini-slots pre-empting normal transmissions should be evaluated. These trade-offs are application-specific and lack known best practices. Moreover, in addition to the interoperability between various network equipment vendors, interoperability between the various components of the 5G-enabled medical device application should also be considered for smooth SLA service delivery.

SLA Assurance

Unpredictable changes in customer requirements are challenging to address during SLA assurance. With the dynamic nature of 5G and B5G networks, time varying user requirements and business needs can be addressed by dynamic SLAs to help the SLA stakeholders maximize their flexibility during the SLA period. Forecasting can leverage automation tools, such as artificial intelligence (AI) based models to help improve the assurance of SLA services along with improving communication performance, problem resolution, root cause analysis, and identifying risky or suspicious behavior that might lead to cybersecurity attacks. For example, AI-based cell outage detection and compensation to prevent service disruption in connected medical devices. Similarly, if spatio-temporal prediction of medical IoT traffic density can be accurately made, service provisioning can be efficiently done to assure that the required service performance is achieved at all times and locations. Similarly, network coverage can be improved by dynamic network parameter optimization based on forecasting the temporal behavior of medical IoT user traffic and their trajectories. Developing and automating these prediction functions can be challenging because of the dynamic nature of cellular networks, uncertain user behavior, and diverse healthcare applications demand for communication. For example, coverage prediction can be hindered by environmental factors such as changing vegetation patterns with seasons and severe weather. Similarly, users' mobility and varying traffic patterns might render a certain optimization function outdated.

Moreover, reputation management algorithm based on review evaluation can be challenging to implement during SLA assurance in 5G networks. An example is the potential of leveraging a large number of dummy reviews by either the service providers, the customers, or any third party, which can in turn falsely impact the reputation of the service providers.

SLA Considerations for 5G-Enabled Medical Devices

Internet of Medical Things (IoMT) is a connected infrastructure of medical devices, software applications, and healthcare systems and services [8]. Incorporation of 5G and B5G technologies into medical devices, such as wearable and implantable devices, fall in this domain.

While 5G promises to ensure that the medical devices connected to 5G networks can meet their target latency, data rate, security, and energy consumption, this comes with the responsibility to consider the hazards and risks associated with using 5G technology to enable medical functions in order to assure safe and reliable performance throughout the lifecycle of the device. Medical device risk management plays an integral role in supporting device safety, while helping device manufacturers optimize efficiency and costs. A risk management process is specified in the ISO 14971 standard for application of risk management to medical devices [9]. The U.S. Food and Drug Administration (FDA) guidance document on the use of radio frequency wireless technology in medical devices [10] also recommends several considerations for the design, testing, and use of wireless technology in medical devices, including the selection of wireless technology, wireless coexistence [11], and others. The risk management process of 5G-enabled medical device can include the SLA implemented for that medical device as it clarifies how the 5G service is used to facilitate a medical function, delineates the roles and responsibilities of stakeholders, and quantitatively specifies the impact of network performance metrics on medical device functions along with applicable mitigation strategies to ensure device safety.

While 5G promises to ensure that the medical devices connected to 5G networks can meet their target latency, data rate, security, and energy consumption, this comes with the responsibility to consider the hazards and risks associated with using 5G technology to enable medical functions in order to assure safe and reliable performance throughout the lifecycle of the device.

Another component of SLAs for 5G-enabled medical devices is the consideration of cybersecurity. The FDA draft guidance for management of cybersecurity in medical devices includes aspects of medical device cybersecurity management, such as risk assessment, designing a trustworthy device, and device labeling recommendations, among other topics [12]. In this section, we focus on the cybersecurity aspects of 5G technology that enable connected medical devices. As compared to short-range and currently common wireless technologies, for example, Bluetooth or WiFi, 5G technology introduces unique cybersecurity challenges that stem from the technical advancements enabling 5G capabilities. For example, Ericsson forecasts around 5 billion Internet of Things (IoT) connections to 5G by 2025 [13]. When such a large volume of heterogenous equipment is connected to the 5G network, intrusion detection can be challenging. Similarly, with 5G high connection throughput and data rates, attackers can download sensitive data in a compromised network very quickly. Moreover, direct patient harm resulting in serious injury or death can be the result of hacking a medical device like an insulin pump that is compromised to apply an overdose of insulin, or an implantable cardiac defibrillator that is made to administer a shock, inducing a fatal heart rhythm [14]. Therefore, considering and addressing cybersecurity risks in the SLA can help enhance the security of 5G-enabled medical devices. Figure 4 shows several types of cybersecurity threats in a 5G network, their point of attack,[1] and the affected healthcare application in case the attacks are successfully carried out. Notably, medical IoT devices are susceptible to the attacks on the user and RAN side of the 5G network, while remote medical procedures, using low latency capabilities and edge computing, are

[1] Interested readers can refer to [15] for a detailed discussion of the 5G network architecture.

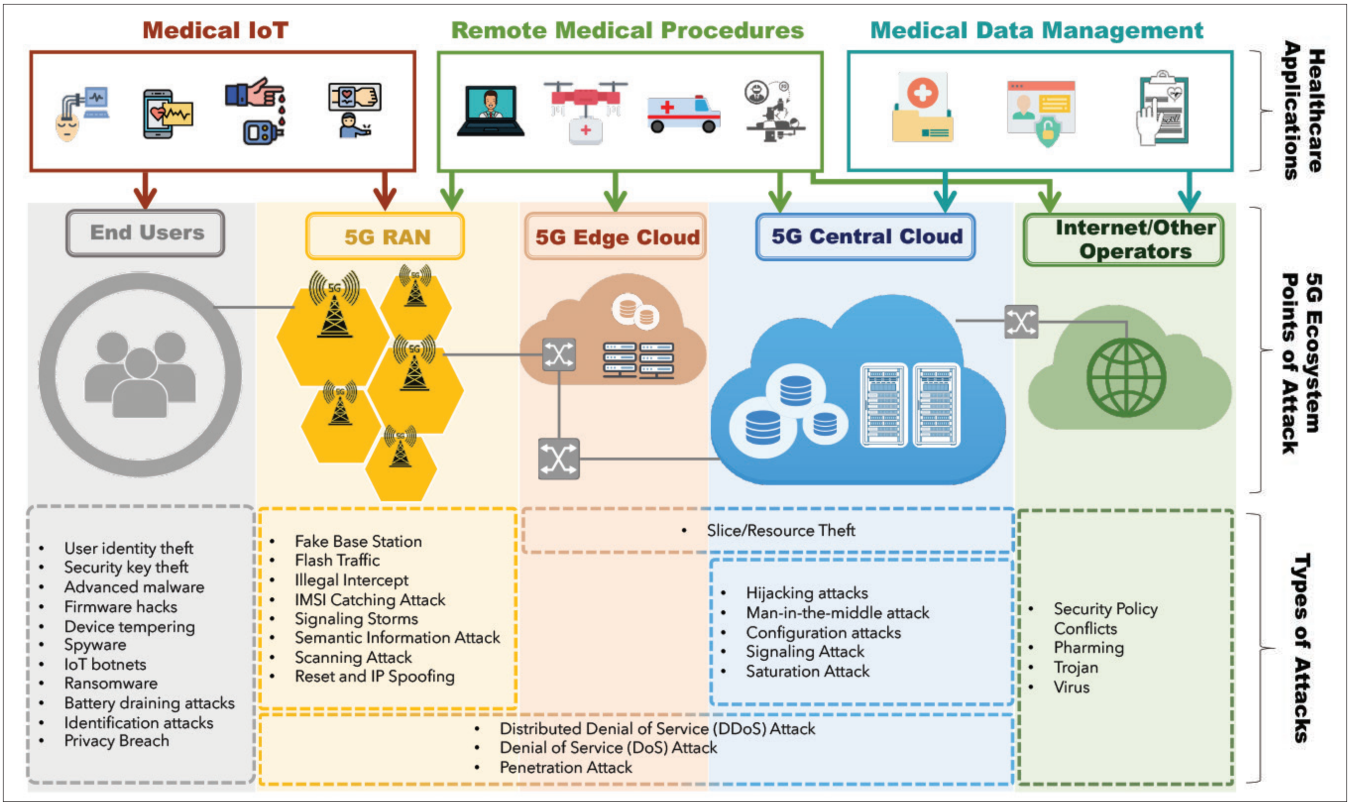

FIGURE 4. Cybersecurity threats to the 5G ecosystem mapped to the affected healthcare application.

susceptible to attacks on the 5G cloud edge. Confidential data attacks can happen on the source/end-users (i.e., devices) of the data and where it is stored (i.e., cloud). Medical IoT devices are susceptible to attacks on the user side of 5G network because of the attack vectors that could be executed when IoT nodes are exchanging data with the network through the RAN. Examples of attacks on the end-user side include medical identity theft by leveraging poor or missing encryption, compromised, weak, or stolen credentials, out of date operating systems, ransomware resulting in users' inability to access their data until a ransom is paid, and spyware which enables unauthorized access to data. Attacks on 5G clouds can also impact confidential data such as patient electronic health records. In 5G-healthcare applications, medical related data may travel across the globe between patients, healthcare professional, and facilities. Additionally, the use of machine learning and AI further contributes to the data being in motion for distributed edge processing.

Given the variety of potential threats and attack modalities, care should also be taken while specifying metrics related to cybersecurity in the SLA. Examples of metrics relevant for consideration in SLAs of 5G-enabled medical devices include authenticity, confidentiality, integrity, availability, vulnerability, agility, resilience, mean time to detect, mitigation/recovery time, and proactiveness [5]. The extensive range of possible applications motivates cybersecurity engagement between all SLA stakeholders, including the end-users (e.g., patients, hospitals), network service providers, and third parties responsible for assisting with network security assurance. Additionality, innovative strategies to mitigate security threats can be considered in SLAs where applicable, for instance, encryption key management (e.g., electrocardiography-based key generation) and using artificial intelligence for anomaly detection to mitigate service disruptions, eavesdropping, and signal jamming.

Future Directions

We illustrate open research questions in Fig. 5 based on the SLA challenges described earllier when considering 5G-enabled healthcare use cases. These include trade-offs and practical implementation considerations in 5G network resource allocation. Other considerations include optimizing device performance when using bandwidth adaptation, network slice sharing modes, and dynamic network resource optimization. With the mmWave spectrum enabling 5G performance, research is also needed to understand the integration of user mis-association probability to mmWave cells in medical device risk evaluation and strategies to address it in the SLA. This is relevant in scenarios like connected ambulance where mobility is important to deliver the intended functionality. With 5G and B5G networks becoming increasingly complex in terms of the number of configuration and optimization parameters and counters, adaptive algorithms to reduce the large set of observable network counters and metrics are needed for helping in efficient network monitoring, especially during the SLA service monitoring and assurance phases. Moreover, algorithms are also needed to flexibly map and optimize the network configuration parameters to meet a desired healthcare application requirement while maintaining business objectives for all stakeholders. This can extend to the development

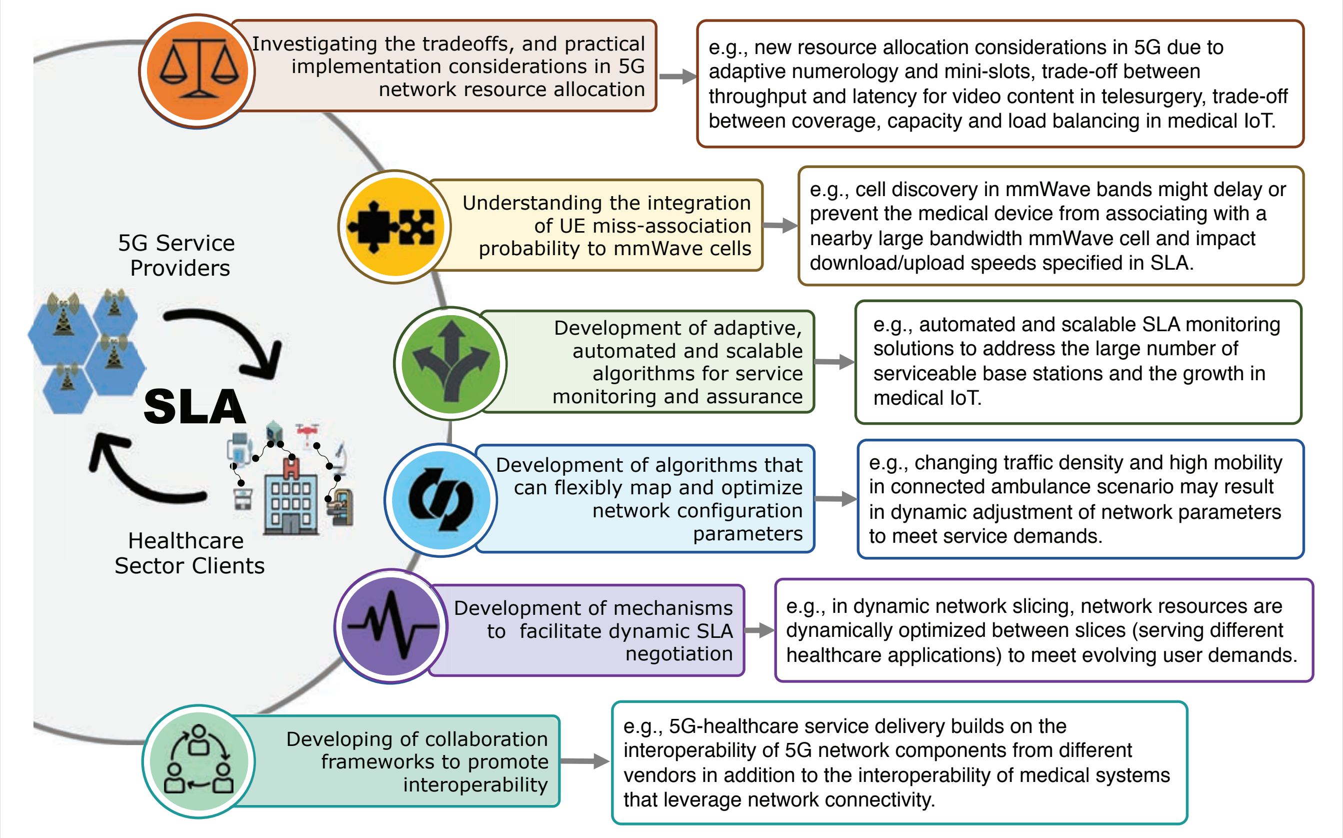

FIGURE 5. Future research directions to facilitate the safe use of 5G communication in healthcare through SLAs.

of continuous forecasting and optimization techniques, where AI can play a key role. Given the evolving nature of 5G and B5G networks, and the diverse communication requirements for different healthcare use cases, mechanisms for dynamic SLA negotiation are also needed. Additionally, the heterogenous and multi-domain nature of 5G and B5G networks indicates that collaboration frameworks are needed between the SLA stakeholders to promote interoperability and service delivery.

Conclusion

5G and B5G networks open possibilities for augmenting existing medical device connectivity and advancing novel healthcare use cases and applications. However, the integration of 5G technology in medical devices should be done safely, securely, and reliably. SLAs are a framework that can facilitate this goal by documenting the communication requirements for diverse 5G-healthcare use cases and specifying the roles of all stakeholders to ensure that the delivered 5G service meets the set performance requirements. The unique features of 5G networks bring new challenges to SLA establishment for healthcare. In this article, we highlight how the nuances of 5G networks give rise to new challenges in different stages of 5G-enabled healthcare SLAs, which lead to the need for evolving SLAs. We also discuss open questions and future research directions that can promote the establishment of robust SLAs for 5G-healthcare applications. This will help ensure that device manufacturers, network service providers, and regulators share a common framework for healthcare service delivery.

Acknowledgment

This project was supported in part by an appointment to the Research Participation Program at the U.S. Food and Drug Administration administered by the Oak Ridge Institute for Science and Education through an interagency agreement between the U.S. Department of Energy and the U.S. Food and Drug Administration.

References

[1] D. Li, "5G and Intelligence Medicine: How the Next Generation of Wireless Technology Will Reconstruct Healthcare?" *Precis. Clin. Med.*, vol. 2, no. 4, 2019, pp. 205–08.
[2] ITU-R Recommendation M.2083-0. IMT Vision D Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond, Sept. 2015.
[3] X. Wang *et al.*, "Millimeter Wave Communication: A Comprehensive Survey," *IEEE Commun. Surveys & Tutorials*, vol. 20, no. 3, 2018, pp. 1616–53.
[4] A. Vergutz, G. Noubir, and M. Nogueira, "Reliability for Smart Healthcare: A Network Slicing Perspective," *IEEE Network*, vol. 34, no. 4, 2020, pp. 91–97.
[5] H. N. Qureshi *et al.*, "Service Level Agreements for 5G and Beyond: Overview, Challenges and Enablers of 5G-Healthcare Systems," *IEEE Access*, vol. 9, 2021, pp. 1044–61.
[6] A. Asghar, H. Farooq, and A. Imran, "Self-Healing in Emerging Cellular Networks: Review, Challenges, and Research Directions," *IEEE Commun. Surveys & Tutorials*, vol. 20, no. 3, 2018, pp. 1682–1709.
[7] H. N. Qureshi, A. Imran, and A. Abu-Dayya, "Enhanced MDT-Based Performance Estimation for AI Driven Optimization in Future Cellular Networks," *IEEE Access*, vol. 8, 2020, pp. 161406–26.
[8] H. Magsi *et al.*, "Evolution of 5G in Internet of Medical Things," *Proc. IEEE Int'l. Conf. Computing, Mathematics and Engineering Technologies (iCoMET) 2018*, Mar. 3, pp. 1–7.
[9] M. N.Teferra, ISO14971-Medical Device Risk Management Standard," *Int'l. J. Latest Res. Eng. Technol. (IJLRET)*, vol. 3, no. 3, 2017, pp. 83–87.
[10] FDA, Radio Frequency Wireless Technology in Medical Devices, Guidance for Industry and Food and Drug Admin-

istration Staff, accessed: Oct. 29, 2020; available: https://www.fda.gov/media/71975/download.
[11] M. O. Al Kalaa and S. J. Seidman, "5-GHz band LTE-LAA Signal Selection for Use as the Unintended Signal in ANSI C63.27 Wireless Coexistence Testing," *IEEE Trans. Electromagn. Compat.*, vol. 62, no. 4, Aug. 2020, pp. 1468–76.
[12] FDA, Content of Premarket Submissions for Management of Cyber-Security in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff, accessed: Sep. 25, 2020; available: https://www.fda.gov/media/119933/download.
[13] Ericsson, Cellular IoT in the 5G Era: Realizing Cellular IoT for Industrial Transformation, white paper, accessed: April 20, 2021; available: https://www.ericsson.com/en/reports-and-papers/white-papers/cellular-iot-in-the-5g-era.
[14] Z. Ankarali *et al.*, "A Comparative Review on the Wireless Implantable Medical Devices Privacy and Security," *Proc. 2014 4th Int'l. Conf. Wireless Mobile Communication and Healthcare-Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH)*, IEEE, 2014, pp. 246–49.
[15] P. Rost, "Mobile Network Architecture Evolution Toward 5G," *IEEE Commun. Mag.*, vol. 54, no. 5, May 2016, pp. 84–91.

Biographies

Haneya Naeem Qureshi received her B.S. degree in electrical engineering from Lahore University of Management Sciences (LUMS), Pakistan, in 2016, and the M.S. degree in electrical and computer engineering from the University of Oklahoma, USA in 2017. She is currently a Ph.D. candidate in electrical and computer engineering with the University of Oklahoma, USA, working in the Artificial Intelligence (AI) for Networks Research Center, where she is contributing to several NSF-funded projects. She is also an ORISE Fellow working with the Center for Devices and Radiological Health, U.S. Food and Drug Administration (FDA), Maryland, where she is evaluating the use of the 5th generation of mobile communication networks (5G) in medical devices. Her other current research interests include network automation and a combination of machine learning and analytics for future cellular systems. She has also been engaged in system design of unmanned aerial vehicles deployment, channel estimation and pilot contamination problem in Massive MIMO TDD systems.

Marvin Manalastas received his B.S. degree in electronics and communication engineering from the Polytechnic University of the Philippines in 2011, and M.S. degree in electrical and computer engineering from the University of Oklahoma–Tulsa in 2020. He has more than seven years of industry experience in the field of Telecommunications. He worked as a microwave transmission engineer with Huawei Technologies Philippines from 2011 to 2015. He then moved to Tokyo, Japan from 2015 to 2018 to work as a radio network performance engineer focused on LTE network optimization. In 2019, he did an internship as an RF engineer at Mobilecomm Professionals in Dallas, Texas. He is currently a Ph.D. student in electrical engineering at the University of Oklahoma–Tulsa, working with the Artificial Intelligence (AI) for Networks (AI4Networks) Research Center. His research interest is in machine learning applied in 5G and beyond networks.

Ali Imran is a presidential associate professor in ECE and the founding director of the Artificial Intelligence (AI) for Networks (AI4Networks) Research Center and TurboRAN Testbed for 5G and Beyond at the University of Oklahoma. His research interests include AI and its applications in wireless networks and healthcare. His work on these topics has resulted in several patents and over 100 peer-reviewed articles, including some of the most influential papers in the domain of wireless network automation. On these topics he has led numerous multinational projects, given invited talks/keynotes and tutorials at international forums, and advised major public and private stakeholders and co-founded multiple start-ups. He received a B.Sc. degree in electrical engineering from the University of Engineering and Technology Lahore, Pakistan, in 2005, and the M.Sc. degree (Hons.) in mobile and satellite communications and the Ph.D. degree from the University of Surrey, Guildford, U.K., in 2007 and 2011, respectively. He is an Associate Fellow of the Higher Education Academy, U.K. He is also a member of the Advisory Board to the Special Technical Community on Big Data of the IEEE Computer Society.

Mohamad Omar Al Kalaa received the Bachelor's degree in electronics and telecommunication from Damascus University, Damascus, Syria, in 2008, the M.E. degree in advanced telecommunication from the Ecole Nationale Superieure des Telecommunications de Bretagne, Brest, France, in 2012, and the M.Sc. and Ph.D. degrees in electrical and computer engineering from the University of Oklahoma, Norman, OK, USA, in 2014 and 2016, respectively. He is a Staff Fellow Electrical Engineer with the Center for Devices and Radiological Health (CDRH), U.S. Food and Drug Administration (FDA). His research interests include healthcare applications enabled by wireless technology, wireless coexistence of technologies in unlicensed bands, coexistence testing methodologies, cognitive radio, PHY and MAC design, and the application of machine learning in wireless communication. He currently serves as the co-chair of the medical device innovation consortium (MDIC) 5G-enabled medical device working group and the secretary of the ANSI C63.27 standard for evaluation of wireless coexistence working group.