Replies to the NTIA Challenge RFC

Tommaso Melodia, Stefano Basagni, Salvatore D'Oro, Michele Polese
Institute for the Wireless Internet of Things
Northeastern University, Boston, MA
melodia@northeastern.edu

1. How could a Challenge be structured such that it would take advantage of DoD's role as an early U.S. Government adopter of 5G technology to mature the open 5G stack ecosystem faster, encourage more participation in open 5G stack development including encouraging new participants, and identify any roadblocks to broader participation?

   - **Incentives and Infrastructure.** Small teams - not traditional telecom equipment manufacturers - need to be incentivized to participate in the challenge and bring to the table non-traditional solutions that will advance the US wireless ecosystem. To that end, they will need (i) access to development resources/funding; (ii) access to testing platforms with carrier-grade scale and equipment. Moreover, the challenge needs to be structured to provide incentives to develop high-quality, carrier-grade, reliable software, that is ready - or almost ready - for production. Therefore, the DoD could address this and foster participation to the challenge by allowing the U.S. wireless ecosystem to expand to non-traditional actors and thrive by (i) allowing small entities to tap into a common, large-scale testing infrastructure with open interfaces for the software development of this challenge; (ii) promoting testing-driven development for high-quality, reliable software, and (iii) granting development funding to the participants of the challenge.
   - **A Common Playground.** Infrastructure (i.e., testbeds and open software) will play a key role in the Challenge development, by serving as a common playground for the participants. Therefore, the DoD should support access to an end-to-end, programmable, and virtualized platform, based on open - preferably open source - components. The Challenge platform will need to include the different components of an end-to-end, open 5G network [1], including RAN and core networks, orchestrators, and edge platforms. Participants should be asked to start from a common canvas and develop improved and complementary intelligent solutions on the shared platform to enrich its functionalities toward an open, interoperable, reliable, and secure 5G ecosystem. Finally, once the solutions have been developed and tested in controlled environments, the DoD should facilitate transition to commercial networks.

2. How could a Challenge be structured to focus on the greatest impediments to the maturation of end-to-end open 5G stack development?

   - **Interoperability.** The Challenge should promote multi-vendor/multi-participant interoperability through standardized open interfaces.
   - **Funding.** The Challenge should provide a modest amount of funding to incentivize early participation by a variety of groups; higher levels of funding for groups that distinguish themselves in the early stages of the competition.
   - **Softwarization.** The Challenge should be based (or include as a key component) on softwarization, and be based on white-box hardware re-programmable via software APIs. The success of 5G rests on the ability to rapidly react in real-time to varying traffic demands,

user mobility patterns, channel conditions and user requirements. White box hardware and control APIs are crucial to meet all of the above requirements and realize the 5G vision.

- **Testbeds.** The Challenge should be based on one or more shared infrastructure/testbeds where different teams can focus on adding different functionalities, while being able to test their solutions in an end-to-end, programmable environment. Nationally available testbed include Colosseum and the suite of testbeds developed within the NSF Platforms for Advanced Wireless Research Program.
- **Robustness.** The Challenge should support the development of reliable and robust software, especially for the RAN components, and provide incentives (e.g., through the scoring system) for robustness and reliability of the proposed solution.
- **Technology Transition.** The Challenge should promote transition of mature solutions on commercial networks.

3. What should be the goals of a Challenge focusing on maturation of the open 5G stack ecosystem? How could such a Challenge be structured to allow for the greatest levels of innovation? What metrics should be used in the assessment of proposals to ensure the best proposals are selected?

   - The challenge should target a demonstration of proposed solutions using open source software and white box hardware. The software developed for the challenge should meet specific code quality and reliability levels set by NTIA, DoD, and its partners.
   - The goal should be to achieve intent-based control of network functionality *for different thrusts* of the Challenge. Network controllers and intelligent RAN algorithms should be able to define high-level directives (e.g., minimize latency) and requirements (e.g., Service Level Agreements (SLAs)). The system must be able to satisfy constraints and attain objectives.
   - Scalability and reactivity should be considered as key metrics for the Challenge. Winning solutions should be those that are able to track quickly changes in traffic, channel dynamics, mobility, and operational requirements.
   - The DoD might provide a set of control directives and requirements. Solutions should be designed to achieve these goals while satisfying all requirements. Solutions that have best performance, are most reliable, and are interoperable with solutions from other teams should score higher. The challenge should have a testing phase where one of the objectives is to test the adaptability of the solution to control directives and requirements never seen before and not included in the original set provided by DoD. Solutions that demonstrate their generality should score high.

4. How will the open 5G stack market benefit from such a Challenge? How could a Challenge be structured to provide dual benefit to both the Government and the open 5G stack market?

   - Limitations of the open 5G stack ecosystem include ([1], Sec. IX): (i) Open implementations often do not keep pace with standard specifications; (ii) latency and scalability issues of software-based solutions; (iii) limited availability of open and/or open source projects focusing on the RAN; (iv) the lack of robust, reliable, well-documented software, ready to be deployed without additional development or integration efforts, and (v) the need for security-driven development in open 5G stack projects.
   - The success of the open 5G stack market, and this challenge, will pave the way toward 6G and beyond. Promoting an open 5G is key for the ability of the U.S. ecosystem to accelerate the level of innovation to maintain competitiveness. Openness will bring new players into the market and cross-pollinate different fields. If those benefits are demonstrated via this Challenge, U.S.-based manufacturers of different components of the disaggregated and open stack will have an opportunity to become market leaders.

5. What are the incentives in open 5G stack ecosystem development that would maximize cooperation and collaboration, promote interoperability amongst varied open 5G stack components developed by different participants, and mature desired featured sets faster with greater stability?

   - The success of this challenge rests on the availability of a shared, basic, end-to-end infrastructure, which would provide a common playground for the participants to develop and benchmark their solutions to the different thrusts of the Challenge. The DoD should promote interoperability and openness as part of the challenge, including *incentives* for participants to contribute the developed solutions back to the shared platform and/or the wireless open source community.
   - The scoring system should evaluate the level of interoperability, with blind and randomized testing of the integration of different components of the end-to-end network, and higher scores for efforts that work well with components developed by other teams.
   - The "openification" of hardware components in the data-center and the Internet world through Software-defined Networking (SDN) has clearly shown that open and multi-vendor hardware not only represents a more efficient solution than monolithic and black-box-based ones, but that it also diversifies and revives the hardware market, creating business opportunities that were not available before.

6. Could a Challenge be designed that addresses the issues raised in previous questions and also includes test and evaluation of the security of the components?

   - The Challenge should cover security aspects that might rise from adopting open implementations. Software should be free from backdoors and loopholes. The Challenge might include a final audit on software/hardware security to ensure that all software components are transparent and secure.
   - Heightened attention to software development following best practices for robustness and security is sorely required, to guarantee privacy, integrity, and security to the end users of softwarized networks [1, 2]. Openness already facilitates useful scrutiny of the code. Audits and reviews from the open source community can help prevent bugs and/or security holes, and can be embedded in the scoring system of the challenge. The Challenge should also strive to promote a security-by-design approach, for example, through a dedicated thrust. The exposure of Application Programming Interfaces (APIs) to third party vendors (e.g., for the O-RAN xApps) could introduce new vulnerabilities in the network if the APIs are not properly securely designed and contain weaknesses that can be exploited by attackers. It is clear that the security of the open source software deployed in 5G and beyond systems must be a key concern for the developers and telecom ecosystem. Participants to the Challenge should follow best practices developed over the years by other open source communities (e.g., the Linux kernel), that make it possible to tighten the security of open source products.

7. Could a Challenge be designed that would require participants to leverage software bill of materials design principles in the development of components for an open 5G stack?

   - A thrust of the Challenge could focus on development of automated control, tracking, and accounting software for the management of end-to-end open 5G networks. This software should be able to monitor which software and hardware components are instantiated and are running in the network (e.g., through an authentication process), so that it can create and maintain a virtual BOM for enhanced security and accountability.

8. Many open 5G stack organizations have developed partial implementations for different aspects of an open 5G stack. What portions of the open 5G stack has your organization successfully developed with working code? What portions of the open 5G stack does your organization believe

can be developed quickly (6 months or less)? What development support would best enable test and evaluation of the different elements of an open 5G stack?

- The Institute for the Wireless Internet of Things (WIoT) at Northeastern University has proven expertise on data-driven control of open source softwarized wireless networks. Solutions for zero-touch network control have been defined and implemented [3], as well as closed-loop data-driven network automation [4], solutions for network optimization [5], RAN and edge slicing [6], and software-defined networking [7]. Additionally, the WIoT develops and has access to several end-to-end, softwarized testing facilities with software-defined radios, datacenters for storage, computing, and machine learning applications, including Arena [8], Colosseum (the world's largest hardware-in-the-loop network emulator) [9], and the PAWR platforms [10, 11, 12]. WIoT researchers use these testbeds to instantiate softwarized, standard-compliant cellular networks and evaluate their solutions at scale in a variety of configurations. These testbeds allow testing in scenarios as close as possible to those of commercial deployments, while avoiding the risk of disrupting production networks.
- Researchers from the WIoT have recently demonstrated the first O-RAN data-driven control loop on a *large scale experimental testbed using open source, programmable* RAN and O-RAN components [4]. We deployed O-RAN on Colosseum [9] and used it to control different network slices instantiated on four base stations serving 40 mobile devices.
- To enable Challenge participants to develop solutions in a short timeframe (6 months or less), the challenge should provide a common, end-to-end, open testing platform, which the participants can improve by developing and testing intelligent algorithms, or by new RAN and/or edge/control functionalities.

9. What 5G enabling features should be highlighted in the Challenge, such as software defined networking, network slicing, network function virtualization, radio access network intelligent controller, radio access network virtualization?

    - The Challenge should focus on creating and developing an end-to-end open 5G stack, with an holistic approach that include efforts in all the areas mentioned above through different Challenge thrusts. In each of these thrusts, particular attention should be given to data- and intent-driven control.

10. What software and hardware infrastructure will be needed to successfully execute this Challenge?

    - The challenge should rely on end-to-end platforms with white box hardware, that are representative of a wide variety of deployment scenarios. Participants should aim at developing solutions that work on multiple platforms, starting from testing in a controlled, emulated scenario, and then moving to over-the-air, large scale platforms, and, eventually, commercial deployments.
    - The Challenge could provide access to an end-to-end experimental platform such as Colosseum and the PAWR testbeds. **Colosseum** [9] is a massive RF and computational facility that can emulate different wireless scenarios (e.g., open field, downtown area, shopping mall, or a desert), generating more than 52 terabytes of data per second with 256 software-defined radios that emulate up to 65536 80 MHz-wide RF channels. Colosseum has been created by DARPA for the Spectrum Collaboration Challenge, and is now operated by the WIoT at Northeastern University. While in the SC2 challenge Colosseum was primarily used to demonstrate new bluesky approaches to spectrum sharing, Colosseum can instantiate large-scale emulated cellular systems. For example, in [4], we have used Colosseum to demonstrate for the first time O-RAN compliant slicing and resource allocation controlled through deep reinforcement learning algorithms over a large scale system (4 base stations and 40 clients). **Arena** is a first-of-its-kind experimental platform that consists of a medium-sized ceiling 8x8

antenna grid testbed, covering an indoor area of 2240 square ft, connected to 24 USRPs controlled by 12 host servers [8]. The Arena wireless environment is an indoor multi-disciplinary open-space research laboratory, with high multi-path and dynamic reflections effects. The NSF-funded **PAWR** program enables experimental investigation of new wireless devices, communication techniques, networks, systems, and services in real wireless environments through several heterogeneous city-scale testbeds [13]. **POWDER-RENEW** is an outdoor testbed that at capacity will have more than 400 radios in a large coverage area in Salt Lake City. This area includes a variety of terrain types, building sizes, and densities, as well as two kinds of MIMO technologies—conventional MIMO and 256-antenna Massive MIMO installed on rooftops and fiber-connected street poles. **COSMOS** [11] is being deployed in the densely-populated neighborhood of West Harlem, New York City, NY, and focuses on providing ultra-high-bandwidth and low-latency wireless communications, and it will have edge-computing capabilities. Among others, COSMOS will allow researchers to experiment with mmWave and optical switching technologies. **AERPAW** [12], developed in the North Carolina Research Triangle, will be the first-ever wireless platform to allow large-scale uas experimentation for 5G technologies and beyond.

- Thanks to containerized environments, it is possible to instantiate an experiment in Colosseum and then replicate it in one of the other testbeds by moving the experiment container. This capability can be leveraged to create multi-platform challenges, where competitors are evaluated on their ability to compete with a solution that can operated over multiple platforms.
- In terms of software, the challenge should provide a softwarized, end-to-end platform, including RAN, edge, core, and orchestration components [1]. In this way, participants would have a common playing field in which they could quickly develop and test open 5G stack solutions.

11. What is a reasonable timeframe to structure such a Challenge? Should there be different phases for such a Challenge? If so, what are appropriate timelines for each suggested phase?

    - The Challenge should be structured in multiple, parallel thrusts, dedicated to the development of different open 5G stack functionalities, such as, for example, ultra-low latency open stacks, resource allocation at scale, applications and algorithms for 5G FR2 networks, security in open RAN, also considering adversarial data attacks, and secure ML for open RAN.
    - To quickly promote the development of the open 5G stack ecosystem, the Challenge should provide a common end-to-end infrastructure to the participants. This would reduce the start-up time for the development of new solutions, thus reducing the overall duration of the challenge phases.
    - Phase zero would involve the setup of the testing platform(s) in both its hardware and software components (6 months).
    - A first phase would involve enrollment of participants and (3 months), with tutorials, webinars, and town halls for discussion among participants. Participants would select the thrust(s) of the challenge in which they want to compete. Shared datasets would be provided to the challenge participants.
    - In the second phase (6 months), participants would develop solutions to the challenge and test them in the shared platform.
    - In the third phase, top scorers in each thrust will further refine the proposed solutions and compete in commercial-grade, O-RAN based networks (6 months).

References

[1] L. Bonati, M. Polese, S. D'Oro, S. Basagni, and T. Melodia, "Open, Programmable, and Virtualized 5G Networks: State-of-the-Art and the Road Ahead," *Computer Networks*, vol. 182, pp. 1–18, December 2020.

[2] T. Melodia, "Talk at NSF Workshop on Next-G Security, Panel on Security issues in the virtualization of Next-G networks." [Online]. Available: https://www.dropbox.com/s/efykd8q1qdwsqjh/Tommaso-5gsecurityWorkshop.pptx?dl=0

[3] L. Bonati, S. D'Oro, L. Bertizzolo, E. Demirors, Z. Guan, S. Basagni, and T. Melodia, "CellOS: Zero-touch Softwarized Open Cellular Networks," *Computer Networks*, vol. 180, pp. 1–13, October 2020.

[4] L. Bonati, S. D'Oro, M. Polese, S. Basagni, and T. Melodia, "Intelligence and Learning in O-RAN for Data-driven NextG Cellular Networks," *arXiv:2012.01263 [cs.NI]*, December 2020.

[5] S. D'Oro, L. Bonati, F. Restuccia, and T. Melodia, "Coordinated 5G network slicing: How constructive interference can boost network throughput," *submitted to IEEE/ACM Transactions on Networking (TNET)*, 2020.

[6] S. D'Oro, L. Bonati, F. Restuccia, M. Polese, M. Zorzi, and T. Melodia, "Sl-EDGE: Network Slicing at the Edge," in *Proceedings of ACM Mobihoc*, Virtual Conference, October 2020.

[7] Z. Guan, L. Bertizzolo, E. Demirors, and T. Melodia, "WNOS: An optimization-based wireless network operating system," in *Proc. of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, Los Angeles, CA, USA, June 2018.

[8] L. Bertizzolo, L. Bonati, E. Demirors, A. Al-Shawabka, S. D'Oro, F. Restuccia, and T. Melodia, "Arena: A 64-antenna SDR-based Ceiling Grid Testing Platform for Sub-6 GHz 5G-and-Beyond Radio Spectrum Research," *Computer Networks*, November 2020.

[9] Colosseum. https://www.colosseum.net. Accessed February 2021.

[10] J. Breen, A. Buffmire, J. Duerig, K. Dutt, E. Eide, M. Hibler, D. Johnson, S. Kumar Kasera, E. Lewis, D. Maas, A. Orange, N. Patwari, D. Reading, R. Ricci, D. Schurig, L. B. Stoller, K. Van der Merwe, K. Webb, and G. Wong, "POWDER: Platform for Open Wireless Data-driven Experimental Research," in *Proceedings of ACM WiNTECH*, September 2020.

[11] D. Raychaudhuri, I. Seskar, G. Zussman, T. Korakis, D. Kilper, T. Chen, J. Kolodziejski, M. Sherman, Z. Kostic, X. Gu, H. Krishnaswamy, S. Maheshwari, P. Skrimponis, and C. Gutterman, "Challenge: COSMOS: A City-Scale Programmable Testbed for Experimentation with Advanced Wireless," in *Proceedings of ACM MobiCom*, London, United Kingdom, September 2020.

[12] V. Marojevic, I. Guvenc, M. Sichitiu, and R. Dutta, "An Experimental Research Platform Architecture for UAS Communications and Networking," in *Proc. of IEEE Vehicular Technology Conference (VTC2019-Fall)*, Honolulu, HI, USA, September 2019.

[13] Platforms for Advanced Wireless Research (PAWR). https://www.advancedwireless.org. Accessed February 2021.