NSF Convergence Accelerator's 2022 Cohort Phase 1 Award

Project Title
Lightweight Scalable and Secure 5G and Beyond Networks

Awardee
Novowi

Award/Contract #
49100422C0023

Award Contract Type
R&D

Award Date
July 15, 2022

Principal Investigator
Guevara Noubir
gnoubir@novowi.com

Co-Principal Investigator
Triet Vo-Huu

NSF Funded Directorate
Directorate for Technology, Innovation and Partnerships

NSF Funded Program
NSF's Convergence Accelerator

NSF Program Director
Ibrahim Mohedas
Track G: Securely Operating Through 5G Infrastructure
Convergence Accelerator
Directorate of Technology, Innovation and Partnerships
imohedas@nsf.gov

PROJECT ABSTRACT

5G is assuring an era of massive and ubiquitous connectivity. The 5G standard introduced enhancements towards security and scalability. Yet, the current state is far from meeting the security and robustness needs of the Department of Defense or DoD deployment, and lightweight scalability and extensibility needs of both DoD and civilian applications. From a practical perspective, there is a lack of clean-slate 5G software implementations that are flexible and designed for high security, robustness, and scalability. Many initiatives in DoD and academic research, and for accelerating connectivity, are hindered by the lack of maturity of existing open-source platforms, which have significant amounts of legacy code.

The proposed Lightweight Scalable and Secure 5G and Beyond Networks project intends to iteratively develop a clean-slate forward-looking 5G and beyond dual use base that can be instantiated to meet the security and robustness needs of the DoD while providing the flexibility to support deployments with high societal impacts such as disaster recovery, anti-censorship, and bringing connectivity to under-served areas. This approach leverages recent results by the team on 5G security (e.g., ONR funded ROSETA project RObust and SEcure TActical 5G project). A first step consists of developing a lightweight minimal and extensible base station that can be deployed on low-power/cost platforms (including unmanned aerial vehicles and small-compute platforms) and enabling user equipment and user equipment sidelinks for DoD devices or disaster recovery use case. This base is extensible along multiple dimensions to gradually integrate defense mechanisms, outcomes of the research activities of the team. These techniques aim at spectrum and signaling integrity awareness; avoidance; stealth; and leveraging trusted execution environments towards zero trust.

The proposed activities draw from the team's multidisciplinary expertise spanning applied cryptography, network security protocols design, systems security, wireless communications, and RF machine learning systems.