MILITARY COMMUNICATIONS AND NETWORKS


Kevin S. Chan


Frank T. Johnsen

Communications and networking in military settings and environments present unique challenges distinguishing them from commercial or civilian settings, which necessitates the development of capabilities and technologies to address these challenges. In a variety of settings, such as the Internet of Things (IoT) and cloud computing, existing civilian technologies can be adapted to the military setting through consideration of these specific constraints or needs.

Civilian trends in IoT are increasingly being investigated in the context of military applications. Typically, many use cases support both civilian and military use, e.g., logistics. Also, the driving force behind civilian IoT, that of using cheap, abundant sensors for various applications, is also intriguing from a military viewpoint. IoT in the context of battlefield networks is often referred to as the Internet of Battlefield Things (IoBT). For IoBT, one can consider that civilian IoT approaches may provide an additional sensing capability to already existing, military-specific ones. Currently, there is an initiative in NATO to research IoT in conjunction with military C2 systems. There are also many independent, national efforts around addressing this same problem space.

Another civilian trend is that of cloud computing, which can be seen as a modern and efficient approach to deploying, governing, using, and maintaining IT resources. NATO has also become aware of cloud computing benefits. Given that the benefits of cloud can also be applied to military applications, this could potentially enable more efficient operations in the future. For NATO, the prospect of more stable, more efficient IT systems for coalition forces could be an enabler for more agile operations in the future.

The battlefield poses a harsh communications environment, with frequent disconnections, limited throughput, and mobility. Also, deployed units in different locations may need to collaborate, giving rise to a need for beyond line of sight (BLOS) communications in addition to local area tactical communications approaches. Because of this, leveraging civilian technology approaches like IoT and cloud computing cannot necessarily be done using off-the-shelf solutions in a military tactical network without further research, testing, and possibly some adaptations.

In this Series issue we provide four papers that all shed light on different parts of these aspects.

In the article "Security, Privacy and Dependability Evaluation in Verification and Validation Lifecycles for Military IoT Systems," the authors provide a construct for Security, Privacy and Dependability Evaluation of IoT systems that could be used for verification and validation processes. The work is discussed from a NATO perspective, and particularly targets IoT in conjunction with unmanned ground vehicles.

For civilian applications, Kubernetes, an open-source system for automating deployment, scaling, and management of containerized applications, is often used in conjunction with a cloud provider to build resilient applications. In NATO, there is ongoing research to investigate Kubernetes from a coalition force perspective, with an emphasis on interoperability and interconnecting different nations' Kubernetes clusters at the tactical edge. This ongoing work is discussed in the article "Federated Control of Distributed Multi-Partner Cloud Resources for Adaptive C2 in Disadvantaged Networks."

To highlight the opportunities and challenges related to military tactical communications, the article "Exploring Performance Trade-offs in Tactical Edge Networks" explores trade-offs between information availability, risk, and resource utilization when facing wireless links that have limited capacity and are prone to disconnections. Finally, the article "Airborne Beyond Line of Sight Communication Networks" presents ongoing NATO research investigating non-satellite and non-high-frequency methodologies for BLoS communications.

The Series Editors are pleased to provide readers with articles that demonstrate how academia, industry, and government are advancing the state of the art with regard to military communications and networks. We commend the community for their resilience despite inconveniences caused by the global pandemic situation, and encourage continued support of this Series and research area amid these extraordinary times. We are confident that the ingenuity and persistence of this community will continue to innovate in this rich area of research, perhaps even how this community has worked in response to the pandemic.

BIOGRAPHIES

KEVIN CHAN [SM'18] (kevin.s.chan.civ@mail.mil) is the Network Science Team Lead with the Computational and Information Sciences Directorate at the U.S. Combat Capabilities Development Command Army Research Laboratory (CCDC ARL), Adelphi, Maryland. Prior to his position at ARL, he received a Ph.D. in electrical and computer engineering and M.S.E.C.E. from Georgia Institute of Technology. He also received his B.S. in ECE/EPP from Carnegie Mellon University. His research is in the area of distributed analytics, network science and cybersecurity for tactical networks.

FRANK T. JOHNSEN (frank-trethan.johnsen@ffi.no) is a principal scientist at the Norwegian Defence Research Establishment (FFI). He is currently working within the area of information and integration services, with a special focus on applying service-oriented architecture (SOA) in the tactical domain. He also holds a part-time position as an associate professor at the University of Oslo, which involves supervising students and teaching SOA. He received his Cand.scient. and Ph.D. degrees from the University of Oslo.