MILITARY COMMUNICATIONS AND NETWORKS


Kevin Chan


Peter H. J. Chong


Frank T. Johnsen

Military applications requiring communications and networking are plentiful, and these operations are conducted in challenging environments. Challenges stem from many places, such as by constraints imposed by the presence of active adversaries, limitations resulting from operations with resource-limited assets, and urgency brought forth from strict mission requirements. In this rich area of communications and networks research and engineering, many solutions have been proposed, leveraging concepts and capabilities including the Internet of Things (IoT), cloud based analytics and blockchain.

IoT remains a hot topic for a wide array of civilian applications, as research targets smart homes, smart cities, and in general approaches to improve the overall quality of life. Military applications of IoT, often called MIoT, leverage the very same IoT concepts, but as the name implies, targets military use cases. In that respect, security is a very important aspect, often neglected in civilian IoT. Another important aspect of MIoT is dependability. The article "Reliability and Fault Tolerance Solutions for MIoT" gives an introduction to MIoT, and emphasizes that a comprehensive approach to reliability and security is required to achieve an appropriate level of dependability for MIoT.

An example of an IoT use case that is both civilian and military is that of leveraging information from smart cities in Humanitarian Assistance and Disaster Recovery Operations. In such operations, it may be beneficial for operating forces to access and integrate the civilian sensor information with their Command and Control (C2) systems, to build a better operational picture and hence improve situational awareness. To achieve such integration, interoperability is needed both for communications protocols and data formats involved. The article "Federation Based on MQTT for Urban Humanitarian Assistance and Disaster Recovery Operations" explores this concept within the confines of a COVID recovery operation, introducing a prototype built on the industry standard MQTT publish/subscribe protocol.

The article "Quality of Information in Gathering Information via Video Analytics for Military Networks" explores optimizing video stream analysis, applying machine-learning techniques in distributed information collection. The collecting end-systems are mobile, with the consequence that they have limited computing power and energy. The authors propose that neither local processing nor off-loading are the best use of the overall system for information collection, but that an optimal combination of mobile and Cloud systems provides the best solution. This work is relevant not only to military operations, but to emergencies where police, firefighters, and paramedics need to coordinate their activities.

Security measures remain a major concern in military communications, applying to the radios, protocols, data exchanges and overall C2 and other software systems that comprise the totality of military communications. The article "Security Accreditation and Software Approval with Smart Contracts" explores how smart contracts can be used as part of a software security accreditation process. The article discusses the concept from a NATO perspective, and presents an implementation based on Hyperledger Fabric as a proof-of-concept.

In summary, these four articles introduce a wide range of recent technologies to cover military applications. We hope that these articles will be informative and inspiring to encourage our readers to research these exciting areas. We would like to thank all the authors who submitted papers to this Series and the reviewers who spent their time to help review and comment on the papers. We express our gratitude to the Editor-in-Chief and publication staff of *IEEE Communication Magazine* for their continuous support.

BIOGRAPHIES

KEVIN CHAN is a research scientist with the Computational and Information Sciences Directorate at the U.S. Combat Capabilities Development Command Army Research Laboratory (DEVCOM ARL), Adelphi, MD. Prior to joining ARL, he received a Ph.D. in electrical and computer engineering (ECE) and an M.S.E.C.E. from Georgia Institute of Technology. He also received the B.S. in ECE/EPP from Carnegie Mellon University. His research is in the area of network science and cybersecurity for tactical networks.

PETER H. J. CHONG is a professor and an Associate Head of School (Research) in the School of Engineering, Computer and Mathematical Sciences at Auckland University of Technology, New Zealand. He received the Ph.D. degree from the University of British Columbia, Canada, in 2000. He was previously an associate professor (tenured) at Nanyang Technological University, Singapore. His research interests include MANETs/VANETs, V2X, Internet of Things/Vehicles, artificial intelligence for wireless networks, and 5G networks.

FRANK T. JOHNSEN is a principal scientist at the Norwegian Defence Research Establishment (FFI), Kjeller, Norway. He is currently working in the area of information and integration services, with a special focus on applying Service-Oriented Architecture (SOA) in the tactical domain. He received his Cand.scient. and Ph.D. degrees from the University of Oslo, Norway. His research interests include military applications of IoT and cloud in tactical networks and at the tactical edge.