Special Session on Military Applications of IoT
(in conjunction with IEEE WF-IoT 2018)

Call for papers

Modern military operations are conducted in a complex, multidimensional, highly dynamic and disruptive environment - sometimes with unanticipated partners and irregular adversaries. Military commanders operate under strong time pressures and high operational tempos. Commanders have increasingly shorter timeframes to obtain an accurate assessment of the situation, to assess potential courses of action, and to make decisions. Furthermore, they need to draw from all possible sources to ensure that the most complete and relevant picture can be created of the situation, in near real-time, and understand the implications of their decisions and courses of action.

One response to these challenges is to introduce the concept of Internet of Things (IoT) into the military domain. The Internet of Things is extensively developed world-wide with a focus on civilian applications. IoT is a paradigm that considers the pervasive presence of a variety of smart things/objects in the environment. By means of wireless and wired connections, they are able to interact and cooperate with each other to create new applications/services in order to reach common goals. Objects/things make themselves recognizable and can behave intelligently by making context related decisions thanks to information aggregation and sharing with other objects. Furthermore, they can be components of complex services. However, the integration of heterogeneous sensors and systems diverse in technology, environmental constraints, and levels of fidelity is a challenging issue not only for military organizations.

Modern military equipment is expected to be increasingly equipped with processing and communication capabilities, which can be employed to inspect or modify the status of the equipment. To some extent, the equipment could be regarded as sensors or actuators and integrated into the rest of the military information infrastructure. Physical and virtual military things have identities, physical attributes, virtual personalities, use intelligent interfaces, and should be seamlessly integrated into the military information network. In order to accomplish full integration, the relevant security mechanisms, protocol adaptions, and scalability properties must be provided. The possible outcome of this integration is a wider set of sensors and information for use in situation awareness applications, medical information applications, transport and logistics applications, etc.

The technical topics of interest include, but are not limited to:

- Scenarios for use of IoT in military environment such as smart bases that incorporate commercial IoT technologies in buildings, facilities, etc., force protection at bases as well as maritime and littoral environments, health and personnel monitoring, monitoring and just-in-time equipment maintenance.
- Smart city monitoring and leveraging services in smart city environments for disaster response and other activities.
- Applications of IoT technologies to support tactical reconnaissance.

- Architectural aspects of military IoT infrastructure, including security, information, and communication architectures, work flow / business processes, interoperability and Integration of disparate technologies.
- Examples of physical instantiations of military IoT systems built from commercially available elements and architectures.
- Information management challenges for military application of IoT – trustworthiness, pedigree, provenance, and enabling military commanders and missions to benefit from IoT generated information.
- Security challenges related to co-existence and interconnection of military and civilian IoT networks.
- Challenges related to reliability and dependability, especially when IoT becomes mission critical.
- Zero-configuration or other approaches to simplify the deployment and configuration of IoT, especially in coalition settings where disparate IoT resources need to coexist and interoperate.
- Knowledge discovery, including semantic and syntax discovery of information provided by IoT.
- Challenges related to actuation of IoT devices, especially with real-time requirements
- Power challenges for tactically deployed IoT devices.

Organizing Committee

Dr **Niranjan Suri** (U.S. Army Research Laboratory, Adelphi, MD, USA)

Dr.-Ing. **Konrad Wrona** (NATO Communications and Information Agency, The Hague, The Netherlands)

Prof. **Zbigniew Zielinski** (Military University of Technology, Warsaw, Poland)

Technical Program Committee

Marek Amanowicz (Military University of Technology, Poland)

Giacomo Benincasa (Florida Institute for Human & Machine Cognition, USA)

Jan Chudzikiewicz (Military University of Technology, Poland)

Aaron Cohen (U.S. Naval Research Laboratory, USA)

Dejan Drajic (DunavNET, Serbia)

Christoph Fuchs (Fraunhofer FKIE, Germany)

Janusz Furtak (Military University of Technology, Poland)

Krzysztof Gierłowski (Gdansk University of Technology, Poland)

Tomasz Gierszewski (Gdansk University of Technology, Poland)

Nenad Gligoric (DunavNET, Serbia)

Alex Gluhak (Digital Catapult, UK)

Mika Helsingius, (Finnish Defence Research Agency, Finland)

Frank Johnsen (Norwegian Defence Research Establishment (FFI), Norway)

Srdjan Krco (DunavNET, Serbia)

Michał Marks (Research and Academic Computer Network (NASK), Poland)

James Michaelis (US Army Research Laboratory, USA)

Ewa Niewiadomska-Szynkiewicz (Institute of Control and Computation Engineering, Warsaw University of Technology, Poland)

Phil Nobles (Defence Academy, UK)

Ian Owens (Defence Academy, UK)

Boris Pokric (DunavNET, Serbia)

Antonio Skarmeta (ODIN Solutions / University of Murcia, Spain)

Michael Street (NCI Agency, The Netherlands)

Mauro Tortonesi (University of Ferrara, Italy)

Witold Zorski (Military University of Technology, Poland)

Paper Submission Guidelines

All submissions should be in English with a maximum paper length of six (6) pages. See conference web site for detailed formatting instructions.

Important Dates

Paper submission deadline: September 30, 2017
Acceptance Notification: November 15, 2017
Camera-Ready: December 15, 2017