JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY

Preface

Modern military operations are conducted in a dynamic environment usually with unanticipated partners and irregular adversaries. In order to act successfully, they need technical support that gives modularity, flexibility and security in connecting heterogeneous systems of cooperating allies. The efficiency of such operations strongly relies on communications and information systems' (CIS) ability to facilitate decision superiority, the state in which better-informed decisions are made and implemented faster than an adversary can react. A key challenge is to improve the situational awareness and reactivity, i.e., the capability to quickly benefit from new information that changes the operational situation. Usually, this depends on a complete reaction process, involving environmental data, data services, and decision makers, all of them interconnected. However, the broad use of information technology in modern command and control system makes its infrastructure the most valuable asset and the most vulnerable point of attack. Finding effective ways to protect and defend communications and information systems by ensuring their availability, integrity and confidentiality challenges even the most advanced technology.

Many research efforts aimed at elaboration and implementation of innovative communications and information technologies in military systems, and especially at delivering new information assurance and cyber defence capabilities have been undertaken world-wide. Selected results of such activities are presented in this issue of the *Journal of Telecommunications and Information Technology*. It contains 11 carefully selected papers that reflect the current state of the art in selected areas of communications and information technology development with application to the military domain. The papers cover a wide spectrum of questions relevant to information assurance (IA) and cyber defence (CD) provision, service oriented architecture (SOA) implementation in tactical domain as well as an effective use of wireless networks resources.

The first group of contributions consists of 6 papers related to information assurance and cyber defence. A discussion of digital signature scheme implementation in environments with space and bandwidth constraints is a subject of the paper *A New Short Signature Scheme with Random Oracle from Bilinear Pairings* by S. Akleylek *et al*. They propose a new

and efficient short signature scheme constructed by bilinear inverse-square Diffie-Hellman problem that does not require any special hash function. The exact security proofs are also explained in the paper. The authors compare the results of the proposed solution with the BLS and ZSS signature schemes. The next paper, *Network Management in Non-classified Data Hiding System Using Master Resident over Hidden Layer* by K. Sawicki and Z. Piotrowski, depicts a practical implementation of a system that takes advantage of hidden data transmission during voice communication leading to information superiority over the adversary. The authors describe a mechanism of master resident, the transmission controller that allows the system's operator to use commands transmitted over hidden layer for remote control of protocol interpreter. The third paper, *Authentication in VoIP Telephony with Use of the Echo Hiding Method* by J. Rachoń, Z. Piotrowski and P. Gajewski, describes an implementation of echo hiding technique for VoIP subscriber identification. The authors present the results of experiments performed in testbedding environment that confirm the efficiency of the proposed solution. A. Flizikowski *et al*. in the paper *The INTERSECTION Framework: Applied Security for Heterogeneous Networks* present an example of security framework. The authors describe various ISO standards addressing telecommunication security management and intrusion detection architecture. They discuss the impact of known network threats on connected networks and propose anomaly detection techniques. The next paper, *Anomaly Detection Framework Based on Matching Pursuit for Network Security Enhancement* by R. Renk and W. Hołubowicz, present a novel framework for recognizing the anomalies in a network traffic based on correlation approach and propose new signal-based procedure for intrusion detection using matching pursuit algorithm. They combine and correlate parameters from different layers that allow detection of 0-day attacks and reduction of false positives. The effectiveness of the proposed approach has been proved in attack and anomaly detection scenarios. The final paper in this group, *Tunneling Activities Detection Using Machine Learning Techniques* by F. Allard *et al*., describes a statistical analysis of ciphered flows that allows detection of the carried inner protocol. Regarding the deployed security policy, this technology could be added in security tools to detect forbidden protocols usages. In the defence domain, this technology could help preventing information leaks through side channels. The authors present a high-level tunnel detection tool architecture and discuss the results of experiments with a public database containing real data flows.

The next group composed of 3 papers is focused on vital aspects of service oriented architecture implementation in military domain. The first paper in this group, *Success Factors for SOA Implementation in Network Centric Environment* by J. Śliwa and M. Amanowicz, identifies 9 fundamental challenges for the SOA approach that make the benefit for the network enabled capability (NEC) programme and increase the effectiveness of military missions. The authors propose the quick wins solutions that can speed up the process of achieving network-enabled capability in heterogeneous multinational NEC environment. B. Jasiul *et al*. in the paper entitled *Authentication and Authorization of Users and Services in Dynamic Military SOA Environments* discuss the security requirements for a cross-domain information exchange in a federated environment. The authors propose an effective method of secure access to information resources based on web services. A special attention is paid to the authentication and authorization of users and services. The solution presented in the paper was examined in multinational experimentations and military exercises. The last paper in this group, *Web Services Efficiency in Disadvantaged Environment* contributed by J. Śliwa, T. Podlasek and M. Amanowicz presents the experimental results of web services (WS) provision techniques carried out in a test-bedding environment that emulates tactical disruptive network. The authors discuss the advantage of different WS adaptation techniques that allow minimizing the XML message size and JPEG image attachments. The presented results show the efficiency of considered methods that adapt the WS provision scheme to the network's constraints.

The last group of papers deals with the questions of effective use of resources in military wireless networks. T. Ginzler and M. Amanowicz in the paper entitled *Adaptation of the Kademila Routing for Tactical Networks* propose a modification of the widely used Kademlia peer-to-peer system to tactical environment. They show that optimizations in the routing may lead to faster lookups and extend the battery lifetime of mobile nodes, as well as

increase the robustness of the network. The final paper in this issue, *Review of Distributed Beamforming* contributed by J. Uher, T. A. Wysocki and B. J. Wysocki, discusses the question of improving the range of communications and saving the precious battery power in wireless sensor networks by cooperative distributed beamforming. The authors present a review of current solutions focused on distributed beamformers implementations. The paper covers the calculation of ideal beamforming weights, practical considerations, such as carrier alignment or smart antennas based on distributed beamformers, and concludes with open research problems.

I would like to take this opportunity to express my thanks to the authors and reviewers for their efforts in the preparation of this issue of the *Journal of Telecommunications and Information Technology*. I trust that the Readers will find the papers dealing with the most recent research results in the area of military information and communications technology both useful and interesting.

Marek Amanowicz
Guest Editor