JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY

Preface

This special issue contains the selected papers chosen by guest editors from the proceedings of the *7th NATO RCMCIS 2005 Regional Conference on Military Communications and Information Systems*, Zegrze, Poland, 7–8 October 2005. The mission of the conference is to provide forum to disseminate and to discuss important topics for the military. These topics are currently investigated by the NATO research society and related to improvement of the military infrastructure for communications and information systems (CIS). The leading subject of the conference was *Technologies for the Military Transformation*. The majority of about 60 presented papers were related to the above mentioned main topic and they discussed the problems of the latest developments in systems and architectures, communication and information systems technologies, secure communications interoperability protocols, as well as cryptology.

Eight papers presented in this issue represent security and telecommunications technologies areas as discussed during the conference. For the security matters there are four papers. The first, by Christoph Karg and Martin Lies presents *A new approach to header compression in secure communications*. The authors propose a new header compression mechanism for the IPv6 protocol; the main benefit of the mechanism is a reduction of the overhead caused by IPSec in the tunnel mode which enlarges the datagrams in order to provide security services such as authentication and secrecy. The last two papers deal with the problems corresponding to design of the cipher systems. In the paper *Distrubution of the best nonzero differential and linear approximations of s-box functions* Krzysztof Chmiel discusses results of the effective designing of s-boxes for block ciphers; the author considers differential and linear approximations of two classes of s-box functions. Anna Grocholewska-Czuryło (*Random generation of Boolean functions with high degree of correlation immunity*) presents an algorithm that can generate randomly highly nonlinear resilient functions for the use mainly in stream cipher systems.

For the telecommunications technologies area there are five papers. The first paper is *End-to-end service survivability under attacks on networks* by Wojciech Molisz and Jacek Rak. The authors propose a model based on traffic parameters of a demand, like delay or bit rate, that allow establishing survivable attack-proof end-to-end connections. The next paper, *New model of identity checking in telecommunication digital channels* by Piotr Gajewski, Jerzy Łopatka and Zbigniew Piotrowski, describes a watermarking based technology system for correspondent identity verification in military telecommunication digital channels. *Planning the introduction of IPv6 in NATO* by Robert Goode is devoted to the areas which must be covered by the NATO IPv6 transition planning process in order to manage the introduction and migration to IPv6. In the next paper (*Simple admission control procedure for QoS packed switched military networks*) the authors, Damian Duda and Wojciech Burakowski, propose an admission control method based on the online traffic load measurements and take advantage from a possibility of the system over-provisioning. The final paper (*Performance evaluation of the multiple output queueing switch with different buffer arrangements strategy* by Grzegorz Danilewicz, Wojciech Kabaciński, Janusz Kleban, Damian Parniewicz, and Patryk Dąbrowski) deals with the problems of the switching system design.

Finally, we would like to take the opportunity to thank all authors of the presented papers as well as the referees who helped us with the evaluation process.

Wojciech Burakowski and Janusz Stokłosa
Guest Editors