Expressions of Interests (EoI)

I. **Cyber Security Research Group**,

UTP University of Science and Technology, Faculty of Telecommunications, Computer Science and Electrical Engineering, Al. Prof. Kaliskiego 7, 85-796 Bydgoszcz, Poland

II. **Group's Leader**: Tomasz Andrysiak, received the M. Sc. degree in telecommunication from the Bydgoszcz UTP University in 1992 and Ph. D. degree in computer science (2000) from AGH University of Science and Technology in Cracow. Currently he is with the Department of Digital Technology at the Faculty of Telecommunications, Computer Science and Electrical Engineering. He researches topics cover various aspects of signal processing, machine learning and security of computer networks. He is particularly interested in anomaly detection problems in various date sets.

III. **Group member:** Łukasz Saganowski.

Areas of interest: security of telecommunication/IP networks, anomaly detection in telecommunication/IP networks, anomaly detection in industrial networks, cyber security of WSN networks and embedded systems, cyber security of smart grid networks.

IV. **Leading Research Topic of the Group comprises**:

security of telecommunication/IP networks, anomaly detection in telecommunication/IP networks, anomaly detection in industrial networks, cyber security of WSN networks and embedded systems, cyber security od smart grid networks, critical infrastructure security aspects.

V. **Best Realizations of the Main Research Topic (Brief Characteristics or Description)**:

- Network Anomaly Detection for Railway Critical Infrastructure based on Autoregressive Fractional Integrated Moving Average. Realization concerns detection of anomalies in real world system which protect railroad crossing.

VI. **General Expression of Interests.**

Cyber Security Research group is interested in finding anomalies in telecommunication and IP networks, industrial networks, industrial networks with critical infrastructure, smart grid

networks, sensor networks and PLC networks. Additionally we are focused on protecting network traffic and protecting elements of critical infrastructure for transportation systems.

VII. **Specific Interests and Additional Topics of Extended Interest**:

Signal processing, thermal image usage for security systems, image processing.

VIII. **Other Important Characteristics of the Group.**

In our studies, we use anomaly detection solutions based on mathematical statistics (i.e. ARMA, ARFIMA, GARCH or FIGARH models) or methods of computational intelligence. In this area, our research activities are focused on the use of various techniques of machine learning (including greedy algorithms and methods of signal processing) to identify abnormal behavior in the data sets.

IX. **Main Group's Achievements**:

- Realization of anomaly detection system for modern real world system protecting railroad crossings critical infrastructure,
- Realization of SNORT IDS IP network anomaly detection preprocessor based on Discrete Wavelet Transform.

X. **Max. 5 Best Selected Publications and/or Other Relevant Accomplishments:**

1. T. Andrysiak, Ł. Saganowski, W. Mazurczyk - Network Anomaly Detection for Railway Critical Infrastructure based on Autoregressive Fractional Integrated Moving Average, EURASIP Journal on Wireless Communications and Networking, 2016, 2016(1), pp. 1-14, DOI: 10.1186/s13638-016-0744-8.

2. Saganowski, Ł., Andrysiak, T., Kozik, R., and Choraś, M. (2016) DWT-based anomaly detection method for cyber security of wireless sensor networks. Security Comm. Networks, 9: pp 2911–2922. doi 10.1002/sec.1550.

3. Tomasz Andrysiak, Łukasz Saganowski, Michał Choraś, Rafał Kozik, Proposal and comparison of network anomaly detection based on long-memory statistical models, Logic Journal of the IGPL - 2016, Vol. 24, No. 6, pp. 944-956, DOI: 10.1093/jigpal/jzw051.