

Editorial

Mobile Sensor Networks Applications and Confidentiality

Ansar-Ul-Haque Yasar,¹ Haroon Malik,² and Zahoor Khan³

¹*Transportation Research Institute, Hasselt University, Hasselt, Belgium*

²*School of Computer Science, University of Waterloo, Waterloo, Canada*

³*Computer Information Sciences, Higher Colleges of Technology, Fujairah Campus, UAE*

Correspondence should be addressed to Ansar-Ul-Haque Yasar; ansar.yasar@uhasselt.be

Received 7 September 2015; Accepted 7 September 2015

Copyright © 2015 Ansar-Ul-Haque Yasar et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This special issue is mostly based on the best papers from the 5th International Conference on Future Networks and Communications (FNC-2014), which was held in Niagara Falls, Ontario, Canada, on August 17–20, 2014. A large number of scientific papers from all around the world were presented in the conference. Many interested techniques were provided in order to enhance the growing demand of Future Networks and Communications technologies, including mobile broadband and all optical networks. All selected papers for this special issue underwent three rounds of rigorous peer-review process. Based on the reviewers' feedback, as well as the evaluations of the Guest Editors, the accepted papers cover remarkable works on new developments in future networked systems such as Wireless Sensor Networks (WSNs), Body Area Networks (BANs), and sensor network confidentiality.

The paper by E.-S. M. El-Alfy and F. Al-Obeidat is entitled "Detecting Cyber-Attacks on Wireless Mobile Networks Using Multicriterion Fuzzy Classifier with Genetic Attribute Selection." This paper investigates a novel methodology based on multicriterion decision making and fuzzy classification that can provide a viable second line of defence for mitigating cyber-attacks. The suggested approach has the advantage of dealing with various types and sizes of attributes related to network traffic such as basic packet headers, content, and time. Using three datasets covering a variety of network attacks, the performance enhancements due to the proposed approach are manifested in terms of detection errors and model construction times.

The paper by Z. Khan et al. is entitled "QPRD: QoS-Aware Peering Routing Protocol for Delay-Sensitive Data in Hospital Body Area Network." The paper proposes a routing

protocol by considering the QoS requirements of the Body Area Network (BAN) data packets. A mechanism for handling delay-sensitive packets is provided by this protocol. The scalability of the protocol is demonstrated by simulating a 24-bed real hospital environment with 49 nodes. The experimental results illustrate that QPRD outperforms comparable protocols in terms of higher throughputs, lower overall network traffic, no packets dropped due to MAC buffer overflow, and fewer number of packet timeouts in both mobile and static patient scenarios. Moreover, linear programming based modelling along with graphical analysis is also done.

The paper by A. Dahane et al. is entitled "Energy Efficient and Safe Weighted Clustering Algorithm for Mobile Wireless Sensor Networks." The authors presented a new energy efficient and safe weighted clustering algorithm (ES-WCA) for mobile WSNs using a combination of five metrics. Among these metrics lies the behavioural level metric which promotes a safe choice of a cluster head in the sense where this last one will never be a malicious node. Extensive simulations are done for the performance evaluation of the proposed algorithm.

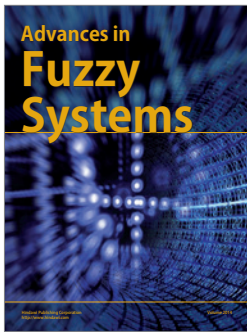
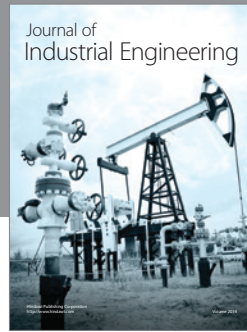
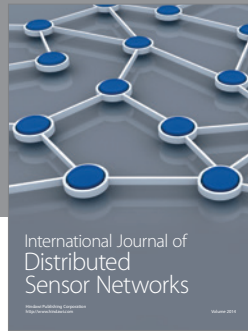
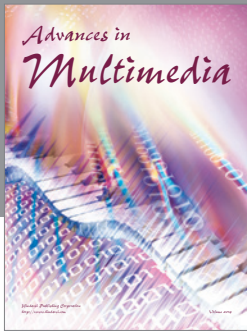
The paper by B. Al-Madani et al. is entitled "AVL and Monitoring for Massive Traffic Control System over DDS." The authors have proposed a real-time Automatic Vehicle Location (AVL) and monitoring system for traffic control of pilgrims coming towards the city of Makkah in Saudi Arabia based on Data Distribution Service (DDS) specified by the Object Management Group (OMG). The suggested DDS based middleware employs Real-Time Publish/Subscribe (RTPS) protocol that implements many-to-many communication paradigm suitable in massive traffic control

applications. This middleware approach helps to locate and track huge number of mobile vehicles and identify all passengers in real time who are coming to perform annual Hajj. Various performance matrices are examined over WLAN using DDS for validation of the proposed framework. Results show that DDS based middleware can meet real-time requirements in large-scale AVL environment.

The paper by N. Jabeur et al. is entitled “Enabling Cyber Physical Systems with Wireless Sensor Networking Technologies, Multiagent Paradigm, and Natural Ecosystems.” This paper proposes an agent-based architecture that migrates the complex processing loads outside the physical sensor network while incorporating missing characteristics such as autonomy, intelligence, and context awareness to the WSN. In addition, authors explore the ecosystem metaphor for WSNs with the aim of taking advantage of the efficient adaptation behaviour and strong communication mechanisms used by living organisms. Based on mapping these organisms onto sensors and ecosystems onto WSNs, authors highlight the shortcomings that would prevent WSNs from matching the capabilities of ecosystems at several levels, including structure, topology, goals, communications, and functions. In contrast to existing works, authors use software agents to bridge the gap between WSNs and natural ecosystems, achieve an optimal mapping between both systems, and enhance the capabilities of WSNs to take advantage of bioinspired algorithms.

It is our pleasure to thank all authors for their valuable contributions and their efforts of preparing high quality manuscripts. We would like to thank reviewers for providing their thoughtful and useful comments to authors.

*Ansar-Ul-Haque Yasar
Haroon Malik
Zahoor Khan*



Hindawi

Submit your manuscripts at
<http://www.hindawi.com>

