Invitation to Submit

Advanced Communication and Networking Techniques for Artificial Intelligence of Things (AIoT)
Guest Editors: Prof. Dr. Shibo He, Dr. Fangyuan Xing, Prof. Dr. Victor C. M. Leung, Dr. Lei Yang and Prof. Dr. Huan Zhou
Deadline: 15 October 2023

Editorial Board Members' Collection Series: Smart Cities/From 5G to 6G/Digital Twins
Guest Editors: Dr. Pal Varga and Prof. Dr. Jemal Abawajy
Deadline: 15 January 2024

Distributed Machine Learning and Federated Learning for Network Optimization towards 6G
Guest Editors: Dr. Adamantia Stamou, Dr. Vasos Vassiliou and Dr. Jose Costa-Requena
Deadline: 15 January 2024

Advances and Challenges in Future Networks
Guest Editors: Prof. Dr. Jain-Shing Liu and Dr. Chunhung Richard Lin
Deadline: 15 January 2024

Special Issue Books

Recent Developments on Mobile Ad-Hoc Networks and Vehicular Ad-Hoc Networks
Guest Editors: Dr. Dimitris Kanellopoulos and Prof. Dr. Francesca Cuomo

Innovative Technologies and Services for Smart Cities
Guest Editors: Prof. Dr. Subhas Mukhopadhyay and Prof. Dr. Tarikul Islam

MDPI is a member of

Affiliated Society

Follow

facebook.com/MDPIOpenAccessPublishing
twitter.com/MDPIOpenAccess
linkedin.com/company/mdpi
instagram.com/mdpiopenaccess
weibo.com/mdpicn
Wechat: MDPI-China

Subscribe

blog.mdpi.com

mdpi.com **mdpi.com/journal/electronics**

Visit mdpi.com for a full list of offices and contact information.
MDPI is a company registered in Basel, Switzerland, No. CH-270.3.014.334-3, whose registered office is at St. Alban-Anlage 66, CH-4052 Basel, Switzerland.

electronics

an Open Access Journal by MDPI

IMPACT FACTOR 2.9

CITESCORE 4.7

Section Networks

electronics

an Open Access Journal by MDPI

IMPACT FACTOR 2.9

CITESCORE 4.7

Section **Networks**

Section Editor-in-Chief

Prof. Dr. Juan-Carlos Cano
Department of Computer Engineering, Universitat Politècnica de València, 46022 Valencia, Spain

jucano@disca.upv.es

Section Information

The Network Section provides full coverage of all topics of interest involved in the networking area. The purpose of this Section is to bring together researchers, engineers, and students from academia and industry to present novel ideas and solid research about the theoretical and practical aspects in the application domains of computer communications and networks.

Author Benefits

- **Open Access** Unlimited and free access for readers
- **No Copyright Constraints** Retain copyright of your work and free use of your article
- **Thorough Peer-Review**
- **2021 Impact Factor: 2.690 (*Journal Citation Reports* - Clarivate, 2022)**
- **No Space Constraints, No Extra Space or Color Charges** No restriction on the length of the papers, number of figures or colors
- **Coverage by Leading Indexing Services** Scopus, SCIE (Web of Science), CAPlus / SciFinder, Inspec, and other databases
- **Rapid Publication** First decision provided to authors approximately 16.6 days after submission; acceptance to publication is undertaken in 2.7 days (median values for papers published in this journal in the first half of 2022)

Selected Papers

DOI:10.3390/electronics12040888

An Automotive Reference Testbed with Trusted Security Services

Authors: Teri Lenard, Béla Genge, Piroska Haller, Anastasija Collen and Niels Alexander Nijdam

Abstract: While research in the field of automotive systems inclined in the past years towards technologies such as Vehicle-to-Everything (V2X) or Connected and Automated Vehicle (CAV), the underlying system security still plays a crucial role in assuring trust and system safety. The work at hand tackles the issue of automotive system security by designing a multi-service security system specially tailored for in-vehicle networks. The proposed trusted security services leverage Trusted Platform Module (TPM) to store secrets and manage and exchange cryptographic keys. To showcase how security services can be implemented in a in-vehicle network, a Reference TestBed (RTB) was developed. In the RTB, encryption and authentication keys are periodically exchanged, data is sent authenticated, the network is monitored by a Stateful Firewall and Intrusion Detection System (SF/IDS), and security events are logged and reported. A formal individual and multi-protocol analysis was conducted to demonstrated the feasibility of the proposed services from a theoretical point of view. Two distinct scenarios were considered to present the workflow and interaction between the proposed services. Lastly, performance measurements on the reference hardware are provided.

DOI:10.3390/electronics12030771

DOA Estimation Based on Convolutional Autoencoder in the Presence of Array Imperfections

Authors: Dah-Chung Chang and Yan-Ting Liu

Abstract: Array imperfections may exist in an antenna system subject to non-ideal design and practical limitations. It is difficult to accurately model array imperfections, and thus complicated algorithms are usually inevitable for model-based methods to estimate the direction of arrival (DOA) with imperfect arrays. Deep neural network (DNN)-based methods do not need to rely on pre-modeled antenna array geometries, and have been explored to handle flawed array models because of their better flexibility than model-based methods. The DNN autoencoder (DAE) method has been proposed for the array imperfection problem, which decomposes the input into multiple components in different spatial subregions. These components have more concentrated distributions than the original input, which avoid a large number of connections and nodes used in the layers to realize DOA estimation classifiers. In this paper, we study the convolutional AE (CAE) method that substantially focuses on the learning of local features in a different manner from the previous DAE method. The advantage of the convolutional operation using a kernel in CAE is to capture features in a more efficient manner than the DAE, and thus be able to reduce the number of parameters that are required to be trained in the neural networks. From the numerical evaluation of DOA estimation accuracy, the proposed CAE method is also more resistant to the noise effect than the DAE method such that the CAE method has better accuracy at a lower signal-to-noise ratio.

DOI:10.3390/electronics12030652

Machine Learning Techniques for Non-Terrestrial Networks

Authors: Romeo Giuliano and Eros Innocenti

Abstract: Traditionally, non-terrestrial networks (NTNs) are used for a limited set of applications, such as TV broadcasting and communication support during disaster relief. Nevertheless, due to their technological improvements and integration in the 5G 3GPP standards, NTNs have been gaining importance in the last years and will provide further applications and services. 3GPP standardization is integrating low-Earth orbit (LEO) satellites, high-altitude platform stations (HAPSs) and unmanned aerial systems (UASs) as non-terrestrial elements (NTEs) in the NTNs within the terrestrial 5G standard. Considering the NTE characteristics (e.g., traffic congestion, processing capacity, oscillation, altitude, pitch), it is difficult to dynamically set the optimal connection based also on the required service to properly steer the antenna beam or to schedule the UE. To this aim, machine learning (ML) can be helpful. In this paper, we present novel services supported by the NTNs and their architectures for the integration in the terrestrial 5G 3GPP standards. Then, ML techniques are proposed for managing NTN connectivity as well as to improve service performance.

DOI:10.3390/electronics12030518

Random Routing Algorithm for Enhancing the Cybersecurity of LEO Satellite Networks

Authors: Ruben Fratty, Yuval Saar, Rajnish Kumar and Shlomi Arnon

Abstract: The recent expansion of networks of low-earth orbit (LEO) satellites such as Starlink, OneWeb, and Telesat and the evolution of communication systems toward B5G and 6G with densely interconnected devices could generate opportunities for various cyber attacks. As the satellite network offers many crucial services to the public and governmental organizations, cyberattacks pose severe risks to the communication infrastructure. In this study, we propose a random routing algorithm to prevent distributed denial-of-service (DDoS) attacks on an LEO satellite constellation network. The routing algorithm utilizes the classical algorithms, i.e., k-DG, k-DS, k-SP, and k-LO, by introducing randomness and selecting one with weighted probability distribution to increase the uncertainty in the algorithm. The study shows that the proposed random routing algorithm improves the average and median cost of the attacker against DDoS attacks while maintaining the functionality of the network. The algorithm is optimized by formulating a Bayesian optimization problem. In addition to providing an additional level of uncertainty in the routing, there is an improvement of 1.71% in the average cost and 2.05% in the median cost in a typical scenario. The algorithm causes the network to be robust to cyber attacks against LEO Satellite Networks (LSNs), however, similar to any other defensive measures, it reduces the network's goodput.

DOI:10.3390/electronics12030503

3D Hybrid Localization Algorithm for Mitigating NLOS Effects in Flying Ad Hoc Networks

Author: Jung Min Pak

Abstract: Positions of unmanned aerial vehicles (UAVs) are typically obtained using the global positioning system (GPS). However, in GPS-denied or GPS-degraded environments, ad hoc networks with flying sensor nodes are used for UAV localization. In this study, we propose a novel three-dimensional (3D) localization algorithm for UAVs in flying ad hoc sensor networks. Interacting multiple model probability data association and finite impulse response filters are integrated in our hybrid localization algorithm. The non-line-of-sight condition can be overcome using the proposed algorithm, which is demonstrated through 3D localization simulations based on flying ad hoc networks.