Special Issue Proposal

IEEE Transactions on Intelligent Transportation Systems (T-ITS)

1. Topic and Scope of the proposed Issue

Security, Reliability and Safety in IoT-Enabled Maritime Transportation Systems

Although modern Maritime Transportation Systems (MTS) has extensively benefitted from Internet of Thing (IoT) technology, risks and challenges in safety and reliability has also increased substantially. With numerous connected devices getting direct access to sensitive information, ensuring security and privacy of transmitted data is very vital. GPS jamming, cargo system manipulation, ransomware attacks are few of the recent cyber security threats faced by the industry. The maritime transportation industry was hit by major cyber-attacks in 2017, 18 and 19 affecting operators, ports, shipbuilders and leading to the loss of revenue and it is crucial to come up with sustainable cyber risk management policies and techniques to prevent such attacks in future.

This special issue will focus on discussions and insights into possible threats, risks and challenges to security, safety and reliability in IoT-Enabled Maritime Transportation Systems, its deployed applications and realizable solutions to resolve them.

The authors strongly believe that this issue on "Security, Reliability and Safety in IoT-Enabled Maritime Transportation Systems" is presented for the first time IEEE Transactions on Intelligent Transportation Systems and will be timely to bring quality research work to the forefront and enhance understanding on security and safety issues in IoT-Enabled Maritime Transportation Systems. This special issue will provide the research and industrial communities the opportunity to disseminate new scenarios, results, and development efforts related to IoT-Enabled Maritime Transportation.

2. Topics and Scope of the proposed Issue

This special issue will feature possible threats, risks and challenges to security, safety and reliability in *IoT-Enabled Maritime Transportation Systems*, its deployed applications and realizable solutions to resolve them. Topics of interest for this special issue include, but are not limited to

- Security, privacy, and trust issues in IoT-enabled MTS
- Architectures and protocols for scalable, secure, robust and privacy enhancing IoT-enabled MTS
- System and data integrity in IoT-enabled MTS
- Intrusion and malware detection in IoT-enabled MTS
- Reliable protocols for data transmission in IoT-enabled MTS
- Cyber and cyber-physical attacks detection, prevention
- Novel methods, protocols, and algorithms enabling security
- Security challenges and mitigation approaches

- Intelligent techniques for security in IoT-enabled MTS
- Hardware and software focused vulnerabilities and their mitigations
- Threat and vulnerability modeling for IoT-enabled MTS
- Secure Communication Protocols for IoT-enabled MTS
- Novel policies for ensuring safety in IoT-enabled MTS
- Future perspectives of security, reliability and safety for IoT-enabled MTS

3. A plan for obtaining high quality papers

To attract high-quality papers for our proposed special session, apart from the publicly distributed Call for Papers (CFP), we will implement the following steps:

- We will disseminate the CFP aggressively through the professional circles of the GEs. The diversity of GEs affiliations spanning multiple countries put us in a good position to disseminate the CFP to a wider audience and collect quality works. We will announce Special Session within our organizations, organizations we are affiliated to (adjunct positions), GE's personal websites, and on their individual LinkedIn profiles to promote the visibility and attract the attention of the research community and organizations.

- We will also share CFP with the highly ranked authors within the scope of the topic and larger networking community. The GEs will contact researchers who have been supportive of this special issue.

4. The Guest Editors

Lead Guest Editor

Dr. Ali Kashif Bashir
Department of Computing and Mathematics, Manchester Metropolitan University, UK
Editor in Chief, *IEEE Future Directions Newsletter*
Email: dr.alikashif.b@ieee.org
Home: https://www.mmu.ac.uk/cfacs/staff/profile/index.php?id=4373

Guest Editors:

Dr. Danda B. Rawat
IET Fellow, Senior Member, IEEE
Department of Electrical Engineering & Computer Science
Howard University, USA
Email: db.rawat@ieee.org
Home: https://www.rawatonline.com/

Professor Jun Wu
Professor/Vice Dean of Institute of Cyber Science and Technology
Shanghai Jiao Tong University, China
Email: junwuhn@sjtu.edu.cn
Home: https://scholar.google.com/citations?user=O205KPAAAAAJ&hl=en

Professor Muhammad Ali Imran
Fellow of IET, Senior Member, IEEE, Senior Fellow, Higher Education Academy (SFHEA), UK
Professor of Communication Systems / Dean University of Glasgow UESTC
University of Glasgow, UK
Email: Muhammad.Imran@glasgow.ac.uk
Home: https://www.gla.ac.uk/schools/engineering/staff/muhammadimran/

5. The proposed review process and list of potential reviewers

The peer-review process is essential to ensure the selection of high standard, novel, and quality research articles submitted by the academia and industrial research community. Additionally, the review process must also guarantee the unbiased and speedy critical review process, which is necessary to quickly publish the new ideas. In order to achieve the above-said objectives, each submission will go through the rigorous review process by at least 3-4 reviewers that are specialized in that respective research under review. Also, we will make sure that each handling guest editor must also include his critical comments based on the careful review of the manuscript. All the guest editors have collectively compiled the list of reviewers based on their expertise, experience in the research area, and trust to meet the quality standards of the IEEE Transactions on Intelligent Transportation Systems (T-ITS). In case we find that any submission requires additional expert reviewers, we may seek help from the T-ITS's general pool of the reviewers. In short, all the guest editorial team members are committed to meet the high standards of the T-ITS by utilizing all the available expertise and resources throughout the special issue duration and beyond.

6. Proposed call-for-papers

Security, Reliability and Safety in IoT-Enabled Maritime Transportation Systems

CALL FOR PAPERS

Internet of Things (IoT), the intelligently connected devices technology for data gathering and processing via sensors, actuators and other devices is unleashing a new dimension of services that is rapidly improving people's quality of life. IoT is delivering solutions with improved efficiency, security and providing better productivity in manufacturing, retail and other sectors. Maritime Transportation Systems (MTS) is currently adopting this promising technology to move towards a digitalized, data-driven world with increased efficiency, lower costs, and creating new revenue opportunities. Integration of IoT also enables real-time tracking of shipments, improved efficiency in cargo handling, pre-emptive maintenance, and route optimization, reduced fuel consumption and improved safety in maritime transportation systems. With IoT

technology expanding and evolving rapidly, more applications are predicted to assist and improve all aspects of maritime transportation systems, making it hassle free and safe.

Although modern MTS has extensively benefitted from IoT technology, risks and challenges in safety and reliability has also increased substantially. With numerous connected devices getting direct access to sensitive information, ensuring security and privacy of transmitted data is very vital. GPS jamming, cargo system manipulation, ransomware attacks are few of the recent cyber security threats faced by the industry. The maritime transportation industry was hit by major cyber-attacks in 2017, 18 and 19 affecting operators, ports, shipbuilders and leading to the loss of revenue and it is crucial to come up with sustainable cyber risk management policies and techniques to prevent such attacks in future.

This special issue will feature possible threats, risks and challenges to security, safety and reliability in *IoT-Enabled Maritime Transportation Systems*, its deployed applications and realizable solutions to resolve them. Topics of interest for this special issue include, but are not limited to

- Security, privacy, and trust issues in IoT-enabled MTS
- Architectures and protocols for scalable, secure, robust and privacy enhancing IoT-enabled MTS
- System and data integrity in IoT-enabled MTS
- Intrusion and malware detection in IoT-enabled MTS
- Reliable protocols for data transmission in IoT-enabled MTS
- Cyber and cyber-physical attacks detection, prevention
- Novel methods, protocols, and algorithms enabling security
- Security challenges and mitigation approaches
- Intelligent techniques for security in IoT-enabled MTS
- Hardware and software focused vulnerabilities and their mitigations
- Threat and vulnerability modeling for IoT-enabled MTS
- Secure Communication Protocols for IoT-enabled MTS
- Novel policies for ensuring safety in IoT-enabled MTS
- Future perspectives of security, reliability and safety for IoT-enabled MTS

Submission Guidelines

Authors must follow the T-ITS's guidelines regarding the manuscript and its format. For details and templates, please refer to the T-ITS's **Author Information** webpage. All papers should be submitted according to the following schedule:

Timeline:

First submission deadline: October 2021
Notification of first decision: January 2022
First revision submission deadline: March 2022
Notification of final decision: July 2022
Final manuscript (camera ready) submission deadline: August 2022
Issue of Publication: October 2022

Guest Editors

- **Ali Kashif Bashir,** Manchester Metropolitan University, UK
- **Danda B. Rawat,** Howard University, USA
- **Jun Wu**, Shanghai Jiao Tong University, China
- **Muhammad Ali Imran**, University of Glasgow, UK

7. A brief resume of the proposed Guest Editors should be included.

Following are the personal webpages that describe respective guest editorial team's academic contributions.

- **Ali Kashif Bashir**
  Home: https://sites.google.com/site/sayyoorj/

- **Danda B. Rawat**
  Home: http://www.rawatonline.com/

- **Jun Wu**
  Home: https://scholar.google.com/citations?user=O205KPAAAAAJ&hl=en

- **Muhammad Ali Imran**
  Homehttps://www.gla.ac.uk/schools/engineering/staff/muhammadimran/