SPECIAL ISSUE on Adaptive Intrusion Detection System using Machine Learning in Wireless Sensor Networks

GUEST EDITORS

Tarek Moulahi, Qassim University, Saudi Arabia.

Rateb Jabbar, Qatar University, Qatar.

Musab Al-Ghadi, La Rochelle University, France.

ADVISORY EDITOR

Christos Anagnostopoulos, University of Glasgow, United Kingdom

DESCRIPTION

This special issue in Open Computer Science (IF 2022: 1.5) focuses on A vast variety of detection nodes make up a Wireless Sensor Networks (WSN), which collects and sends data to a central point. However, distribution tactics, communications channels, and limited supply nodes provide a number of safety concerns for WSN. Therefore, in order to enhance the security aspects of wireless sensor networks, it is imperative to identify unauthorized access. These functions are given to the network-by-network intrusion detection systems, and they are necessary for all interactions on the network. Intrusion Detection Systems (IDS) frequently include Machine Learning (ML) approaches; yet, ML techniques' effectiveness is subpar when managing unbalanced assaults. According to their inadequate rechargeable energy supply, small bandwidth assistance, data travel over multiple hop nodes, reliance on intermediaries or other nodes, dispersed nature, and organization, WSN nodes are vulnerable to a variety of security-related attacks.

The widespread use of WSN presents issues for maintaining their secrecy, credibility, and reliability. Intrusion detection serves as a strong first line of defense for the WSNs and is a crucial active defense mechanism. The disparity between dependable information distribution and restricted sensing power, as well as the dispute over the impact of detection and the scarcity of network resources, must be balanced given the special characteristics of WSN. WSN may overcome the drawbacks of conventional monitoring techniques, which considerably lower the expense of detection while also streamlining the laborious procedure. WSN assaults are visible at every model tier. Because of this, wireless sensor nodes face a variety of problems. Some are connected to technical concerns, while others arise as a result of assaults. To identify and stop threats, defensive and network monitoring systems must be built. The ability to create an affordable ML model for quick intrusion detection and prevention in border regions using WSN is made possible by the notable rise in appeal of accessible ML algorithms and the sharp rise in the utilization of artificial data. However, extra protection precautions need to be taken since WSNs differ from typical networks in terms of design and technology. To guarantee WSN security, an IDS is modelled in this work. A hybrid architecture that combines the use of authorization, overuse, and anomaly-based detection techniques with intrusion detection systems is suggested because these techniques alone are unable to offer reliability. A compact intelligent intrusion detection model for WSN is proposed in this special issue. With the use of anomalous network data, our model can detect attack behaviors in WSNs with speed

and accuracy. Therefore, the supervised neural network satisfies the criterion of convenient data analysis in contrast with different machine learning methods

Potential topics include, but are not limited to:
• Machine learning approaches for Intrusion detection in wireless sensor networks.
• A hierarchical neural network-based intrusion detection solution for wireless sensor networks.
• A cooperative intrusion detection technology optimized for wireless sensor networks.
• An extensively artificial network-based self-adaptive technique for wireless intrusion detection.
• A thin-layer proactive intrusion detection structure for wireless sensor networks.
• Regarding the viability of machine learning for intrusion detection in sensor networks.
• Efficient supporting vector machine-based intrusion detection method for wireless sensor networks.
• Machine learning-based intrusion detection system with optimization support in wireless sensor networks.
• Designing Intrusion Detection Systems in Wireless Sensor Networks via Machine Learning Technologies.
• A wireless Internet of things intrusion detection solution powered by machine learning.
• Developing autonomous machine learning network intrusion detection solutions for abuse.

HOW TO SUBMIT

Before submission authors should carefully read the Instruction for Authors.
Manuscripts can be written in TeX, LaTeX (strongly recommended) - the journal's LATEX template. Please note that we do not accept papers in Plain TEX format. Text files can be also submitted as standard DOCUMENT (.DOC) which is acceptable if the submission in LATEX is not possible. **For an initial submission, the authors are strongly advised to upload their entire manuscript, including tables and figures, as a single PDF file.**

All submissions to the Special Issue must be made electronically via online submission system Editorial Manager:

All manuscripts will undergo the standard peer-review process (single blind, at least two independent reviewers). **When entering your submission via online submission system please choose the option *"SI: Adaptive Intrusion Detection System using ML in WSN".***

Submission of a manuscript implies that the work described has not been published before and it is not under consideration for publication anywhere else.

The deadline for submissions is June 15, 2024, but individual papers will be reviewed and published online on an ongoing basis.

Contributors to the Special Issue will benefit from:

- critical peer-review
- no space constraints
- quick online publication upon completing the publishing process (**continuous publication model**)
- better visibility due to **Open Access** – free, unrestricted and permanent access to all the content

- liberal policies on copyrights (authors retain copyrights) and on self-archiving (no embargo periods)
- promotion of published papers to readers and citers
- long-term preservation – content archiving with Portico

We are looking forward to your submission!

In case of any questions please contact AssistantManagingEditor@degruyter.com