IEEE Sensors Journal

SurveilNet: A lightweight anomaly detection system for cooperative IoT surveillance networks

Martins O. Osifeko is with the Department of Electrical, Electronic and Computer Engineering, University of Pretoria, Pretoria 0002, South Africa (e-mail: u18379428@tuks.co.za).

Gerhard P. Hancke is with the College for Automation and Artificial Intelligence, Nanjing University of Posts and Telecommunications, Nanjing 210049, China, and also with the Department of Electrical, Electronic and Computer Engineering, University of Pretoria, Pretoria 0002, South Africa (e-mail: g.hancke@ieee.org).

Adnan M. Abu-Mahfouz is with the Council for Scientific and Industrial Research, Pretoria 0184, South Africa, and with the Department of Electrical, Electronic and Computer Engineering, University of Pretoria, Pretoria 0002, South Africa (e-mail: a.abumahfouz@ieee.org).

https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9508397

Abstract

The boring and repetitive task of monitoring video feeds makes real-time anomaly detection tasks difficult for humans. Hence, crimes are usually detected hours or days after the occurrence. To mitigate this, the research community proposes the use of a deep learning-based anomaly detection model (ADM) for automating the monitoring process. However, the isolated setup of existing surveillance systems makes ADM inefficient and susceptible to staleness due to the lack of resource sharing and continuous learning (CL). CL is the incremental development of models that adapts continuously to the external world. Thus, for efficient CL in surveillance systems, devices must share resources and cooperate with neighbor sites. Yet, solutions from the literature focus on the isolated environment thereby neglecting the need for resource sharing and CL. To address this gap, this paper proposes a cooperative surveillance system called SurveilNet that allows for resource sharing between surveillance sites under the control of a cooperator node. We further propose a lightweight subscription scheme that allows for a joint specialized model development process that continually adapts to the dynamics of the secured environment. Our proposed scheme offers the ability to learn from the neighboring site's data without compromising data privacy. The performance of our scheme is evaluated using a reclassified UCF-Crime dataset with the result showing the efficiency of our proposed scheme when compared to the state-of-the-art.