GIIDS: Generalized Intelligent Intrusion Detection System for Heterogeneous UAVs in UAM

Fahmina Kabir*, Nishat I Mowla**, Inshil Doh***

** Division of Artificial Intelligence and Software, Ewha Womans University, Korea*

*** Department of Industrial Systems, RISE Research Institutes of Sweden. Sweden*

**** Department of Cyber security, Ewha Womans University, Korea*

kabirfahmina@ewhain.net, nishat.mowla@ri.se, isdoh1@ewha.ac.kr

***Abstract*— Unmanned Aerial Vehicles (UAVs) are increasingly integral in various sectors, simultaneously encountering rising security threats as UAV and Urban Air Mobility (UAM) networks continue to expand. This paper addresses the challenge of securing UAM networks while also emphasizing generalizability of the security solution to protect heterogeneous UAVs against threats that compromise their stability, reliability and can cause catastrophic failures such as a crash landing. The deployment of traditional machine learning (ML) based intrusion detection systems (IDSs) is often hampered in real-world applications due to a lack of generalizability of the security solution. As a result, the system fails to provide adequate security across the varying models and platforms of UAVs, each with its unique statistical properties and data distributions. To address these challenges, we focus on employing a comprehensive set of UAV sensor parameters, tailored feature engineering and selection to develop multi-stage cross-validated ensemble learning systems to facilitate generalized detection of attack and non-attack cases. For additional analysis, we cross-validate the models using two different cross-validation techniques. The proposed deep stacking ensemble system provides the overall best performance, with AUC within the range of 92% to 99.9% across different cross validations.**

***Keyword*— Urban air mobility, machine learning, generalizability, intrusion detection system, unmanned aerial vehicle**

Fahmina Kabir received the B.S. degree in Computer Science and Engineering from Ahsanullah University of Science and Technology, Dhaka, Bangladesh. She is currently pursuing an M.S. degree in the Division of Artificial Intelligence and Software, majoring in Cyber Security at Ewha Womans University, Seoul, South Korea. Her research interests include artificial intelligence, machine learning, network security, anomaly detection, and intrusion detection systems (IDS).

Nishat I Mowla (Member, IEEE) received the B.S. degree in Computer Science from Asian University for Women, Chittagong, Bangladesh, in 2013, and the M.S. and Ph.D. degrees in Computer Science and Engineering from Ewha Womans University, Seoul, South Korea, in 2016 and 2020, respectively. She was awarded the Best Paper Award at the Qualcomm Paper Awards, Seoul, in 2017. She is currently a Senior Researcher at the Department of Industrial Systems, RISE, Sweden. Her research interests include network security, machine intelligence, and cyber physical systems.

Prof. Inshil Doh received the B.S., M.S., and Ph.D. degrees in Computer Science and Engineering from Ewha Womans University, Seoul, South Korea, in 1993, 1995, and 2007, respectively. From 1995 to 1998, she has worked at Samsung SDS, South Korea. She was a Research Professor at Ewha Womans University, in 2009 and 2010, and Sungkyunkwan University, in 2011. She is currently an Associate Professor of the Department of Cyber Security, Ewha Womans University. Her research interests include wired and wireless network security, sensor network security, IoT network and UAM security.