A Horizontal Federated Learning Approach to IoT Malware Traffic Detection: An Empirical Evaluation with N-BaIoT Dataset

Phuc Hao Do[*, ***], Tran Duc Le[**], Vladimir Vishnevsky[****], Aleksandr Berezkin[*] and Ruslan Kirichek[*, ****]

[*]The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Saint-Petersburg, Russia

[**]University of Science and Technology – The University of Danang, Da Nang, Viet Nam

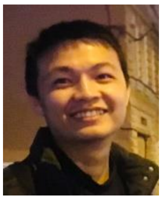
[***]Danang Architecture University, Da Nang, Viet Nam

[****]V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia

haodp@dau.edu.vn, *letranduc@dut.udn.vn*, *vishn@inbox.ru*, *pcdreams@mail.ru*, kirichek@sut.ru

Abstract— **The increasing prevalence of botnet attacks in IoT networks has led to the development of deep learning techniques for their detection. However, conventional centralized deep learning models pose challenges in simultaneously ensuring user data privacy and detecting botnet attacks. To address this issue, this study evaluates the efficacy of Federated Learning (FL) in detecting IoT malware traffic while preserving user privacy. The study employs N-BaIoT, a dataset of real-world IoT network traffic infected by malware, and compares the effectiveness of FL models using Convolutional Neural Network, Long Short-Term Memory, and Gated Recurrent Unit models with a centralized approach. The results indicate that FL can achieve high performance in detecting abnormal traffic in IoT networks, with the CNN model yielding the best results among the three models evaluated. The study recommends the use of FL for IoT malware traffic detection due to its ability to preserve data privacy.**

Keywords— **IoT, abnormal traffics, malware detection, federated learning, AI model**



Phuc Hao Do received his MS degree in Computer science from the University of Danang - University of Science and Technology in 2017. He is currently a Ph.D. student in the Department of Communication Networks and Data Transmission at the Bonch-Bruevich Saint- Petersburg State University of Telecommunications, Russia. His research interests include AI, ML, D and its application in different fields like network, blockchain.

Dr. Duc Tran Le acquired his degree of Ph.D. at Admiral Makarov State University of Maritime and Inland Shipping, Russia in 2018. He works in Information Technology Faculty, The University of Danang - University of Science and Technology, Danang, Vietnam from 2019. His research areas include Internet of Things, wireless network, network security, QoS, WLAN, Software-defined networking.

Dr. Sc. Vladimir M. Vishnevsky received the Engineering degree in applied mathematics from the Moscow Institute of Electronics and Mathematics, Russia, in 1971, the Ph.D. degree in queuing theory and telecommunication networks and the D.Sc. degree in telecommunication networks from the V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences (ICS RAS), in 1974 and 1988, respectively. He became a Full Professor with ICS RAS in 1989 and the Moscow Institute of Physics and Technology in 1990. He was an Assistant Head of the Institute of Information Transmission Problems of RAS from 1990 to 2010 and an Assistant Head of laboratory with ICS RAS from 1971 to 1990. He is currently the Head of Telecommunication Networks Laboratory, ICS RAS. He is a member of Expert Councils of Russian High Certifying Commission and Russian Foundation for Basic Research, member of IEEE Communication Society, International Telecommunications Academy and New York Academy of Science. He has authored over 300 papers in queuing theory and telecommunications. He is a Co-Chair of IEEE conferences - ICUMT, RTUWO, and the General Chair of DCCN conference. His research interests lie in the areas of computer systems and networks, queuing systems, telecommunications, discrete mathematics (extremal graph theory, mathematical programming) and wireless information transmission networks.

Dr Aleksandr Berezkin, is working at the Bonch Bruevich Saint Petersburg State University of Telecommunications as the Associate Professor of Department of Programming Engineering and Computer Science. Science interest are Computer Vision and Machine Learning. In 2009, he defended his thesis with the topic "Model and method of decoding error correction based on neural network". Now he is doctoral student at the Department of Programming Engineering and Computer Science.

Dr. Sc. Ruslan Kirichek is working at the Bonch Bruevich Saint Petersburg State University of Telecommunications as the head of Department of Programming Engineering and Computer Science. He was born in 1982 in Tartu (Estonia). He graduated Military-Space Academy A.F. Mozhaiskogo and the Bonch-Bruevich St. Petersburg State University of Telecommunications in 2004 and 2007, respectively. He received Ph.D. at the Bonch-Bruevich St. Petersburg State University of Telecommunications in 2012 and Dr.Sc. at the Povolzhskiy State University of Telecommunications and Informatics in 2018. From 2008 to 2013 he worked as a senior researcher at the Federal State Unitary Enterprise "Center-Inform". Since 2012 he has been working as the Head of the Internet of Things Laboratory at the Bonch-Bruevich Saint Petersburg State University of Telecommunications. Since 2017 he has been working as ITU-T Q12/11 Rapporteur in “Testing of Internet of things, its applications and identification systems”. Since 2023 he has been working as the Rector of the Bonch-Bruevich Saint Petersburg State University . He is a General Chair of the International Conference “Internet of Things and Its Enablers” (inthiten.org).