一般社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report

# On Attack Pattern Classification in IoT Networks for Network Intrusion Detection Systems

Atuhurra Jesse[†], Takanori Hara[†], Yuanyu Zhang[‡], and Shoji Kasahara[†]

† Division of Information Science, Nara Institute of Science and Technology
8916-5, Takayama-cho, Ikoma, Nara 630-0192 Japan
‡ School of Computer Science and Technology, Xidian University

E-mail: † {atuhurra.jesse.ag2, hara.takanori, kasahara}@is.naist.jp, ‡ yyuzhang@xidian.edu.cn

**Abstract** With the proliferation of IoT devices, IoT security problems arise. To protect heterogeneous connected devices in IoT networks against cyber-attacks and various attack patterns by intruders, many researchers have introduced network intrusion detection systems (NIDSs) which are based on machine learning techniques. An NIDS in IoT networks must maintain the appropriate security level despite the limited computational resources. To address the limitation, we propose a classification method for detecting the attacks by intruders to realize the NIDS designed for IoT networks. Through numerical experiments using a realistic botnet dataset in IoT networks with imbalanced class distribution, we demonstrate that the proposed classification yields high area under the receiver operating characteristics curve (AUC) score as well as balances the high accuracy with low false-positive rate, with the help of the synthetic minority over-sampling technique (SMOTE).

**Keywords** Network Intrusion Detection System, Synthetic minority over-sampling technique (SMOTE), Machine learning, IoT security problem