Copyright ©2022 The Institute of Electronics,
Information and Communication Engineers

SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

SDN-based Detection Method against DoS/DDoS attacks in an IoT environment

Abdul Adhim * Satoshi Okada * Takuho Mitsunaga *

Keywords: IoT, SDN (Software Defined Network), DoS, DDoS, Entropy-based detection

Abstract

The number of IoT devices has been increasing over the years, and it is expected to only keep increasing in the next few years. Keeping these devices secured is always important. One of the ways to keep them more secure is to introduce Software Defined Network (SDN) architecture into the IoT network. SDN enables software-based network management without any physical changes. This technique is well suited for the management and incident response of IoT networks, which continue to grow in size these days. Some of the potential security threats to IoT devices are Denial of Service (DoS), and its other variant Distributed Denial of Service (DDoS). IoT devices' nature to be limited in computation, storage, and network capacity, make them more vulnerable to be compromised. SDN is a promising technology that could help detect and mitigate DoS/DDoS attacks within the IoT network. In this paper, a solution using an entropy-based detection method to detect an incoming DoS/DDoS attack in an SDN-based IoT network is proposed. A statistical approach to distinguish normal traffic from anomalous traffic.

* Toyo University, 1-7-11 Akabanedai, Kita-ku, Tokyo 115-8650