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

機械学習を用いたZigBeeネットワーク上の不正通信検知手法の提案
Machine Learning-based Anomaly Detection in ZigBee Networks

大塩 智也 * 岡田 怜士 * 松田 亘 † 満永 拓邦 *
Tomoya Oshio Satoshi Okada Wataru Matsuda Takuho Mitsunaga

キーワード IoT, ZigBee, 異常検知, 機械学習

あらまし

情報技術とネットワークの発展に伴い, IoT デバイスは急速に普及が進んでいる. その中でも ZigBee は近距離無線通信規格の一つで通信速度は低速であるものの低消費電力かつ低コストでの運用が可能なためスマートホームや産業制御システムでの活用が期待されている. しかしながら, 無線通信である ZigBee はパケットの盗聴や偽装パケットの送信を容易に行うことができるため、悪意のある攻撃者にとって攻撃対象となる可能性がある.

2017 年に発表された論文 [1] では, 一般的に広く流通している IoT デバイスの脆弱性を活用した攻撃によって１つのデバイスがワームに感染することで, ネットワーク構成に関わらず連鎖的に感染を広げ、スマートシティに甚大な被害をもたらすことが明らかになった. また, その他にも ZigBee の脆弱性に関するいくつかの実験が行われ、中には ZigBee ネットワークからコンピュータネットワークにまで侵入することに成功した例などもある [2]. 今後, 安全にスマートホームや産業制御システムにおいて ZigBee を利用するためにはサイバー攻撃を迅速に検知するための手法が必要となる.

本研究では, ZigBee の通信の特徴に注目し, ネットワークの異常や ZigBee ネットワーク上のサイバー攻撃を機械学習を用いて検知する手法を提案する.

参考文献

[1] Eyal Ronen, Colin O'Flynn, Adi Shamir, and Acih-Or Weingarten,"IoT Goes Nuclear : Creating a Zigbee Chain Reaction," IEEE Symposium Security and Privacy，p54-p62

[2] Eyal ltkin,"Don't be silly - it's only a lightbulb, Available:https://research.checkpoint.com/2020/dont-be-silly-its-only-a-lightbulb/

* 東洋大学, 〒 115-8650 東京都北区赤羽台 1-7-11 INIAD HUB-1, Toyo university, 1-7-11 Akabanedai, Kita-ku, Tokyo 115-8650
† NTT 社会情報研究所, 〒 180-8585 東京都武蔵野市緑区 3-9-11, NTT Social Informatics Laboratories,3-9-11, Musashinoshi, Midori-ku,180-8585 Tokyo