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

教師なし学習を用いた低レート DoS 攻撃検知手法の設計と実装
A Design and Implementation of Low-Rate DoS Attack Detection Method Using Unsupervised Learning

樫場 叶耀 * ギリエ ルイス † 和泉 諭 ‡ 阿部 亨 * § 菅沼 拓夫 * §
Kayaba Kiyoaki Guillen Luis Izumi Satoru Abe Toru Suganuma Takuo

キーワード 教師なし学習，低レート DoS 攻撃

あらまし

近年，DoS 攻撃による被害は年々増加しており，少ないパケット数で長時間にわたり通信を続け，セッションを占有する低レート DoS 攻撃が観測されている．低レート DoS 攻撃は，一般的な大規模 DoS 攻撃への対策である IDS や IPS での検知が困難であるため，別の対策が必要となる．

低レート DoS 攻撃の対策として，教師あり学習を用いた検知手法が提案されている [1]．教師あり学習は高い検知性能と複雑な設定を必要としない検知システムの構築を達成している一方で，学習に使用するデータセットには攻撃データが必要となり，実環境における攻撃データの収集が課題となっている．

本研究では，攻撃データを必要としない教師なし学習アルゴリズムに着目し，教師なし学習を用いた新たな低レート DoS 攻撃検知手法の設計と実装を行った．既存のネットワークから収集した正規のユーザによるトラフィックデータを用いて学習用データセットを作成し，教師なし学習によって検知システムを構築する．構築した検知システムにトラフィックデータを定期的に入力することで，低レート DoS 攻撃の有無を判定する．提案手法の概要を図 1 に示す．

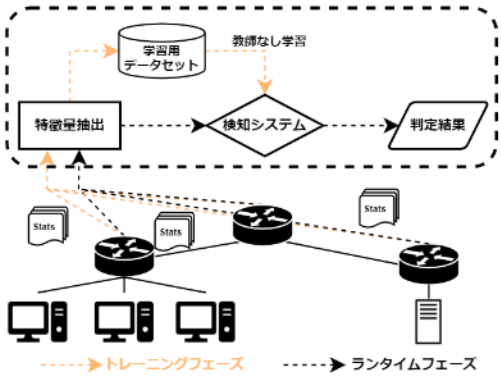

図 1: 提案手法の概要

CICIDS2017[2] データセットを使用した評価実験では，教師なし学習アルゴリズムである AutoEncoder が F1 0.855 ± 0.064 を達成し，低レート DoS 攻撃検知に対して教師なし学習が有効であることが示された．

参考文献

[1] T. V. Phanet al.: “Q-MIND: Defeating Stealthy DoS Attacks in SDN with a Machine-Learning Based Defense Framework,” 2019 IEEE Global Communications Conference (GLOBECOM), pp. 1-6, 2019.

[2] I. Sharafaldin al.: “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” 4th International Conference on Information Systems Security and Privacy (ICISSP), pp. 1-8, 2018.

* 東北大学大学院情報科学研究科 〒 980-8579 宮城県仙台市青葉区荒巻字青葉 6-3-09. Graduate School of Information Sciences, Tohoku University, 6-3-09 Aoba, Aramaki-aza Aoba-ku, Sendai, Miyagi, 980-8579, Japan.
† 東北大学電気通信研究所 〒 980-8577 宮城県仙台市青葉区片平 2-1-1. Research Institute of Electrical Communication, Tohoku University, 2-1-1 Katahira, Aoba-ku, Sendai, Miyagi, 980-8577, Japan.
‡ 仙台高等専門学校 〒 989-3128 宮城県仙台市青葉区愛子中央 4-16-1. National Institute of Technology, Sendai College, 4-16-1 Ayashichuo, Aoba-ku, Sendai, Miyagi, 989-3128, Japan.
§ 東北大学サイバーサイエンスセンター 〒 989-8578 宮城県仙台市葉区荒巻字葉 6-3. Cyberscience Center, Tohoku University, 6-3 Aramaki-Aza-Aoba, Aoba-ku, Sendai, Miyagi, 980-8578, Japan.