5ZA-02

ニューラルネットワークを用いた侵入検知システム改良手法の検討

近松　康次郎†　　平川 豊‡
†芝浦工業大学大学院理工学研究科　‡芝浦工業大学工学部

1. 研究背景

ネットワーク型侵入検知システム(NIDS)は、コンピュータネットワーク内の不正なアクセスを検知し、ネットワーク管理者に通知するシステムである。NIDS には検知方法の一つに、あらかじめ正常なパターンや通信を定義し、その定義から外れたものを異常として検知するアノマリ型検知がある。近年、アノマリ型 NIDS では、しばしば機械学習アルゴリズムが用いられており、機械学習を用いた NIDS の検知精度を向上させるための研究が行われている。

NIDS の研究に広く用いられているデータセットとして、KDDCUP1999 データセット(KDD'99)[1]がある。KDD'99 は、訓練用データとして約 500 万レコード、テスト用データとして約 200 万レコードが用意されており、各レコードは、41 個の特徴量と 1 個のラベルで構成されている。ラベルは、正常を表す Normal と 4 種類の攻撃 Probe, DoS, U2R, R2L の全 5 種類のうちのいずれかが付与されている。また、評価基準としては、全体の精度や各ラベル別の検知率に加えて、しばしばコスト[2]が用いられる。コストは、システムの分類結果と表 1 のコストマトリクスを掛け合わせることで算出される。各誤検知やテストデータの各ラベルの割合によっては、全体の精度が向上していたとしても、コストが増加している場合がある。そのため、システムを適切に評価するためには、全体の精度と各ラベル別の検知率に加えて、コストを評価基準に用いる必要がある。

表 1: コストマトリクス

Actual / Prediction	Normal	Probe	DoS	U2R	R2L
Normal	0	1	2	3	4
Probe	1	0	1	2	2
DoS	2	2	0	2	2
U2R	2	2	2	0	2
R2L	2	2	2	2	0

2. 既存研究

文献[3]では、KDD'99 にいくつかの問題があるとし、それらの問題を解決した NSL-KDD データセットを提案している。NSL-KDD のレコードの基本的な構成は KDD'99 と同じである。また、この研究では、様々な機械学習アルゴリズムを KDD'99 と NSL-KDD を用いて評価している。文献[4]では、様々な機械学習アルゴリズムを用いて評価した結果から、各ラベル別に検知率の高いアルゴリズムを組み合わせたシステムを提案している。また、各ラベル別の検知率に加えて、コストを評価基準に用いている。

この他にも、KDD'99 や NSL-KDD を用いた研究は多数あるが、コスト評価を行っているものは少ない。また、KDD'99 を用いたいくつかの研究では、各ラベル別の検知率を見たとき、U2R と R2L の検知率が極端に低く、全体の精度を向上させるには、これらの検知率を向上させる必要があると指摘されている。しかし、NSL-KDD を用いた比較的新しい研究では、各ラベル別の検知率ですら評価されていないものが多い。また、[4]をはじめ、複数の機械学習アルゴリズムを用いた手法が多く提案されているが、複数の機械学習アルゴリズムを用いることは、必要となる知識や技術が多くなり、ネットワーク管理者や技術者に対して多くの負荷を伴うことが考えられる。

3. 提案手法

そこで本研究では、機械学習アルゴリズムとして、ニューラルネットワークの一つである多層パーセプトロンのみを用いた NIDS の改良手法を検討する。

具体的な手順は、まず、既存手法において最も検知率の低いラベルを持つレコードとその他のラベルを持つレコードでサブモデル用の訓練データを作成し、元の訓練データを用いて学習させたメインモデルと新たに作成したデータを用いて学習させたサブモデルの 2 つの分類器を構築する。テスト時には、テストデータを各モデルに分類させ、各分類結果を統合した結果を最終的な分類結果とする。分類結果は表 2 に基づいて統合される。検知率の低い攻撃に対する専用の分類器を構築することにより、その攻撃の検知率向上が期待できる。提案手法のフローチャートを図 1 に示す。

表 2: 分類結果の統合

メインモデル分類	サブモデル分類	最終的な分類
Normal	Normal	Normal
Normal	特定攻撃検知	特定攻撃検知
攻撃検知	Normal	攻撃検知
攻撃検知	特定攻撃検知	攻撃検知

A Neural Network Approach for Network Intrusion Detection System
†Kojiro Chikamatsu, ‡Yutaka Hirakawa
†Electrical Engineering and Computer Science, Shibaura Institute of Technology, Tokyo, Japan
‡Computer Science and Engineering, Shibaura Institute of Technology, Tokyo, Japan

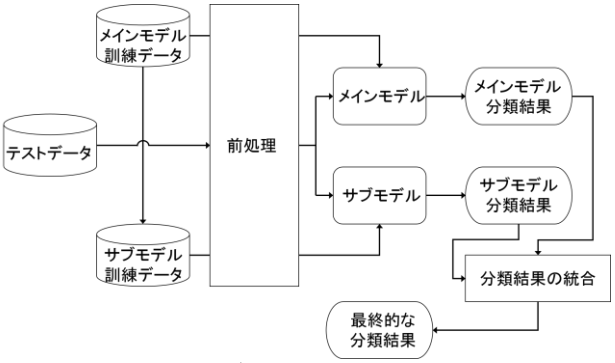

図 1: 提案手法フローチャート

4. 評価

評価では、訓練データとして KDD’99 と NSL-KDD を用いて既存手法及び提案手法を評価した。本研究における既存手法とは、提案手法におけるメインモデルのみを使った手法を指す。テスト用データとしては、同条件における評価のため、NSL-KDD のみを用いている。評価基準としては、全体の精度と各ラベル別の検知率に加えて、コストをテストデータ数で割った 1 レコードあたりのコストを用いる。表 3 に訓練データとして KDD’99 を用いたときの評価結果を示す。

表 3: 評価結果(KDD’99 使用)

	既存手法	提案手法
Normal DR* (%)	94.23	85.38
Probe DR* (%)	28.78	29.95
DoS DR* (%)	74.6	74.57
U2R DR* (%)	0.0	0.0
R2L DR* (%)	0.0	44.99
Accuracy (%)	68.36	70.16
CPE**	0.822	0.675

*DR: Detection Rate
**CPE: Cost per Example

既存手法の結果から、最も検知率が低かったのは、U2R と R2L であった。表 1 のコストマトリクスからわかるように、R2L を誤検知した際のコストは U2R を誤検知した際のコストより高いため、提案手法では R2L について分割する。既存手法と比べて提案手法では、分類器を分けた R2L についての検知率が大幅に向上している。また、Normal の検知率が若干下がっているが、R2L の検知率の向上が大きいため、全体の精度としては向上しており、コストも低減させることができた。次に、訓練データに NSL-KDD を用いたときの評価結果を表 4 に示す。

表 4: 評価結果(NSL-KDD 使用)

	既存手法	提案手法
Normal DR* (%)	97.51	93.82
Probe DR* (%)	68.74	69.31
DoS DR* (%)	73.39	73.55
U2R DR* (%)	0.0	0.0
R2L DR* (%)	0.0	38.6
Accuracy (%)	73.66	76.9
CPE**	0.734	0.574

*DR: Detection Rate
**CPE: Cost per Example

KDD’99 を用いたときの提案手法と比べて、R2L の検知率は下がっているが、Normal や Probe の検知率が向上しているため、最も高い精度と最も低いコストを実現することができた。

5. まとめと今後の課題

本研究では、ニューラルネットワークを用いた NIDS の改良手法として、検知率の低い攻撃について分類器を分割する手法を提案した。評価結果から、提案手法は既存手法と比べて、全体の精度を向上させるだけでなく、システムのコストも低減させることができた。

今後の課題としては、R2L 以外の攻撃について分割した場合の評価や多層パーセプトロン以外の機械学習アルゴリズムを用いた場合の提案手法の評価などがある。

参考文献

[1] KDD Cup 1999, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, Dec 2018.
[2] Charles Elkan, “Results of KDD’99 Classifier Learning”, ACM SIGKDD Explorations Newsletter, Vol.1, No.2, pp.63-64, 2000.
[3] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani, “A Detailed Analysis of the KDD CUP 99 Data Set”, Proceedings of the 2009 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2009), pp.53-58, 2009.
[4] Maheshkumar Sabhnani, Gursel Serpen, “Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context”, Proceedings of the International Conference on Machine Learning, Models, Technologies and Applications (MLMTA 2003), pp.209-215, 2003.