

ネットワーク型侵入検知における研究結果の検証に関する一検討

高原尚志^{†1}

概要：インターネット上では、次々と新たなサイバー攻撃の手法が開発されている。これに対応するため、人工知能（Artificial Intelligence: AI）の技術を用いた攻撃検知手法が開発されている。攻撃検知手法には、通信データを基に攻撃を検知するネットワーク型侵入検知システム（Network-based Intrusion Detection System: NIDS）とホスト上のシステム情報から侵入を検知するホスト型侵入検知システム（Host-based Intrusion Detection System: HIDS）がある。この内、本稿では、NIDS に注目し、開発した手法の評価方法について考察する。NIDS 研究では、①手法の理論的な開発、②ソフトウェアによる実装、③データセットによる評価という手順で研究を進めて行くのが一般的である。この際、②のソフトウェアによる実装では、用いるソフトウェアにバグが存在せず問題なく動作することを保証する必要がある。③のデータセットによる評価では、用いるデータセットが実際の攻撃を正しく反映している必要がある。用いるソフトウェアや評価用データセットが上記の要件を満たさなければ、新たな手法を提案しても、その有効性は保証されない。そこで本稿では、NIDS 研究において、ソフトウェアとデータセットを正しく用いるための要件を満たすための課題を示し、その解決策を論じる。当会議において活発な議論が行われ、有効な意見を得られることを期待する。

キーワード：NIDS, 機械学習, KDD Cup 1999 Data

A Discussion on Verification of Research Results in Network Intrusion Detection System

HISASHI TAKAHARA^{†1}

1. はじめに

本稿では、NIDS 研究の手順を明確にし、用いるソフトウェアや評価用データセットの必要要件を示し、それを満たすための課題や提案を行う。これにより、NIDS 研究の信頼性が向上し、急増するサイバー攻撃を防ぐことができる有効な手法の開発が促されることを目指す。

1.1 背景

インターネット上では、日々新たなサイバー攻撃手法が開発されている。サイバー攻撃を検知する手法には、主に次の2つがある[1]。この内、本稿では、NIDS に注目し、研究全体の信頼性を担保するための条件について検討する。

NIDS の研究は、次のステップで行われるのが一般的である。

(STEP1) 手法の理論的开发

(STEP2) 手法のソフトウェアによる実現

(STEP3) データセットを用いた手法の評価

上記において、開発した手法の有効性を正しく評価するためには、(STEP2)で用いるソフトウェアについては誤り（バグ）がないことが保証されている（要件 1）、(STEP3)で用いるデータセットについては実際の攻撃の状況を正しく反映しているものを用いる（要件 2）といった要件を満たす必要がある。しかし、著者らが知る限り、用いるソフトウェアやデータセットが上記の要件を満たすことについて詳細に論じた文献は現在のところ存在しない。

1.2 動機

NIDS の研究において、用いるソフトウェアとデータセットを、1.1 章で指摘した要件を満たしながら活用することは研究全体の信頼性に大きく影響する。これらが担保されないと、手法の評価結果などの研究結果が意味のないものになってしまう。そこで本稿では、(STEP2)で用いられているソフトウェアと(STEP3)で用いられているデータセットについて、現状を分析して、1.1 で指摘した要件を満たすための条件を明らかにする。これにより、今後 NIDS の研究全体の信頼性を担保することへの貢献を目指す。

1.3 既存研究

Atilla らは、2010 年から 2015 年に発行された 65 の科学雑誌の 149 の論文をサーベイして、侵入検知（Intrusion Detection System: IDS）や機械学習研究（Machine Learning Research: MLR）に用いられたアルゴリズム（手法）やソフトウェア、データセットなどを示している[2]。文献[2]によれば、(STEP1)では、機械学習を中心とした手法の開発が広く行われている。

また、文献[2]によれば、(STEP2)で用いられるソフトウェアは、Weka[3](20.4%)、Matlab[4](15.9%)、Libsvm[5](5.5%)といった既存のソフトウェアが広く用いられており、プログラミング言語を用いた独自のプログラムを用いたもの（Java[6]=4.3%、C++=3.0%、C#=1.8%）を抑える結果となった。特に、日本の論文で多く用いられている Python(1.2%)[7]や R(0.6%)[8]を明示的に示している論文は少ない。しかし、最も多いのは、用いられているソフトウェアを明らかにしていない論文(47.6%)であり、ここでどの

^{†1} 新潟県立大学
University of NIIGATA PREFECTURE

ようなソフトウェアやプログラミング言語が用いられているかは不明である。(表 1.)

(注) () 内は、当該ソフトウェアを用いている論文の割合である。

表 1. 論文中で用いられているソフトウェア
(文献[2] Table 8.より完全引用)

Table1. Software used in Reviewed Articles of [2]

Software Tool/Package	Article Count
No Information(Software used is unclear)	78
Weka	34
Matlab	26
Java	7
C++	5
CSharp	3
Pascal; Hadoop; Python; MOA	2 for each

更に文献[2]によれば、(STEP3)で用いられるデータセットの内 64.9%は KDD Cup 1999 Data[9][10][11](以降、KDD99 と称す)である。また、University of New Brunswick(UNB)の Canadian Institute for Cybersecurity において KDD99 の欠点を改良した NSL-KDD[10][12][13]とそのもととなったデータセットである DARPA 1998 Dataset[14]を合わせると 80.5%の論文が使用していることになる。日本の論文で広く用いられている CCC などのデータセットは、世界的には少数という結果となっている(文献[2]の統計の中には表れない)。ただし、京都大学が提供しているデータセットである Kyoto(Kyoto2006+)[15][16][17][18]は、1.5%で世界的に用いられているという結果となった。(表 2.)

表 2. 多く用いられているデータセット

*印は IDS 用データセットを表す。用いている論文数が 3 より少ないものは省略。(文献[2] Table.9 より完全引用)

Table2. Most used Datasets

Dataset Name	Article Count
KDD99*	133
NSL-KDD*	23
DARPA*	9
Iris	8
Glass	5
Breast Cancer	5
Synthetic Data	5
Porker Hand	5
Image Segmentation	3

ISCX*	3
Wine	3
Kyoto*	3

Sharafaldin らは、IDS 用データセットに対する課題を指摘し、データセットのラベル付けなど課題をクリアするための 11 個の基準を提案し、現在用いられている IDS 用データセットを基準に照らし合わせた一覧表を示した[19][20]。更に、Sharafaldin らは文献[20]の中で、上記の 11 個の基準をクリアしたデータセット[21]を提案し、上記 11 個の基準に照らし合わせて、他のデータセットとの比較を一覧表で示した。(表 3.)

表 3. IDS 評価用データセットを基準に照らし合わせた一覧
(文献[20]の Table5.より引用 (一部抜粋))

Table3. Comparison between generated dataset and public datasets based on last IDS dataset evaluation framework

	Network	Traffic	Label	...	Features	Meta
DARPA	YES	NO	YES	...	NO	YES
KDD'99	YES	NO	YES	...	YES	YES
DEFCON	NO	NO	NO	...	NO	NO
...	...	...	...	...	...	...
KYOTO	YES	NO	YES	...	YES	YES
...	...	...	...	...	...	...
CICIDS2017	YES	YES	YES	...	YES	YES

1.4 解決すべき課題

IDS の研究を行うに当たっては、用いるソフトウェアとデータセットの有効性を十分に示す必要がある。しかし、日本の関連論文の現状では、次の点が課題となっている。

①用いるソフトウェアについての課題

ソフトウェアについては自前のものを用いている場合が多いが、プログラム自体を公開していないものが多く、その結果、読者による結果の検証が困難である。

②用いているデータセットについての課題

用いているデータセットについては、日本国内の論文では、CCC[22]をはじめとしたラベルがないデータセットを用いているものが多く、KDD99 などのデータセットを用いている論文は、近年では著者らが知る限りほとんどない。日本国内の論文では、ラベルを付与したデータセットとして Kyoto2016[23]を用いたものが存在するが、日本国内の論文では、CCC などラベルのないデータと自組織のネットワークから得たデータを組み合わせたデータセットを用いた

ものが大半を占めている。しかし、この場合、”どの通信を攻撃通信と見なすかが画一的でない”や”自組織から得られた通信データが非公開であるため読者による結果の検証が困難である”などの課題が存在する。

1.5 本研究の貢献

本論文の学術的貢献は以下の通りである。

- ・IDS 研究の手順を整理する
- ・ソフトウェアやデータセットを正当に用いるための要件を示し、その要件を満たすための条件について、現状を分析し、課題や解決策を示す

これにより、信頼性が担保された検証可能な論文の作成を促す。

2. NIDS 研究の現状と課題

2.1 手法のソフトウェアによる実現

(STEP1)で開発した手法を実現する方法 (STEP2)には、以下のようなものがある。

(S1) 既存のソフトウェアで実現する方法

(S2) プログラミング言語を用いて独自にソフトウェアを開発する方法

(S1)の方法では、プログラムにランダムな要素が含まれる場合は別として、パラメータの値など必要な情報を合わせて公開することにより、読者による検証可能性を大きく前進させることになると考えられる。しかし、一方で、既存のソフトウェアでは、既存の手法の組み合わせやパラメータチューニングによる手法の開発はできるが、まったく新しい手法などソフトウェアのライブラリにない手法を理論的に開発しても、評価することはできないという課題もある。

(S2)の方法では、バグがないことを保証する必要があるが、用いられたソフトウェアが公開されることはほとんどなく、それをどのように担保するかが課題となると考えられる。解決策として、開発したソフトウェアの公開が考えられるが、一方で攻撃者を利してしまう可能性もある。

上記のように、サイバーセキュリティの分野では、現実の攻撃を扱っているため、開発したソフトウェアを公開すると攻撃者に情報を与えてしまい、結果として研究の成果が攻撃者を利するものとなる危険性があり、公開にはなじまないという意見がある。つまり、サイバーセキュリティの分野においては、学術研究に必須の他者による検証可能性を保証することと、実際に攻撃者を利してしまうことで公開、非公開はトレードオフの関係にあり、十分に議論されなければならない項目である[24]と考える。

なお、現在の状況として、日本の論文では独自のソフトウェアを用いる傾向が強く、海外の論文では既存のソフトウェアを用いる傾向がある。

2.2 データセットを用いた手法の評価

(STEP3)のデータセットを用いた手法の評価で用いられ

るデータセットには、以下のようなものがある。

(DA1) 評価用データセットにどの通信が攻撃でどの通信が正常かといったラベルがついているもの

(DA2) ラベルがついていないもの

具体的には、ラベルが付されているデータセットには KDD99 や Kyoto2016 などがあり、ラベルが付されていないデータセットには CCC や BOS[22][25]などがある。ラベル付けされていない理由として、CCC や BOS は加工されていない通信データであり、この場合、各々の通信データに対するラベル付けが難しいということがあげられる。

また、日本の論文では、評価用データセットの新しさの観点からラベルが付されていないデータセットを評価用として用いる傾向があり、海外の論文ではラベルが付されているものを用いる傾向がある。

データセットにラベルが付されていない場合、どの通信が正常でどの通信が攻撃かを判断することは困難である。そこで、供給されているデータセットがハニーポットによるものである場合が多いことを踏まえて、提供されたデータセットのすべての通信を攻撃とみなし、自前のネットワークから収集したデータを正常通信として、提供されたデータセットと混ぜて評価を行うという方法が広く用いられている。しかし、この方法には以下のような課題がある。

(DP1) ハニーポットのデータがすべて攻撃ということは担保されない

(DP2) 自前のネットワークと評価用データセットとの環境が異なるため、ネットワーク環境の違いによって識別される可能性もあり、混ぜるのは適当ではない

(DP3) 自前のネットワークから収集したデータは公開されていることがなく、読者が結果を検証することができない

(DP3)の場合、自前のネットワークから収集したデータは、セキュリティポリシー[26]などにより、原則公開が認められない場合が多い[23]。確かに個人情報保護などの観点からは公開になじまないデータであるが、一方で学術論文という立場からは、他者による検証は必須である。このような状況を踏まえ、手法の検証には、正常通信のデータとして自前のネットワークから収集したデータを用いるのを極力避け、公開データセットの中で正常通信と攻撃通信が混ざったデータセットを用いるのが適当ではないかと考える。

また、評価用データセットを次のようにに分けることもできる。

(DB1) CCC や BOS などのように得られた通信データ (PCAP データ) をそのまま提供しているもの

(DB2) KDD99 や Kyoto2016 のようにセッションデータとして加工して提供しているもの

(DB1)の場合、PCAP データをそのまま使用しているため、汎用性が高いものとなる一方で、攻撃と正常のラベルを付するのが難しいという課題があり、(DB2)の場合、ある一定期間観察したセッションデータを用いるため、比較的ラ

ベル付けをし易いが、加工後の特徴量をどのように設定するかということが課題となる。

3. まとめ

本稿では、NIDS の研究にあたり、現状を分析し、その課題を、用いるソフトウェアと用いるデータセットの観点から指摘した。科学技術論文の原則である読者による検証が可能であることは、その結果を保証する意味からも重要であると考えられ、NIDS の研究にあたり、読者によって検証を可能とすることをどのように担保するかは今後の課題と考えられる。本稿では、その解決策として、用いるソフトウェアの観点からは、既存のソフトウェアの活用やプログラムを独自に開発した場合には、その公開を提案した。また、用いるデータセットの観点からは、独自ネットワークの通信データを用いた場合にはその公開を提案した。また、研究者ごとに攻撃通信と正常通信の判定が異なることを避けるため、ラベル付きデータを用いることを提案した。

今後、自らの提案手法も含め、既存の様々な手法について、公開ソフトウェア及び公開データセットを用いて検証を行って行く予定である。

謝辞

本研究は JSPS 科研費 JP17K00187 の助成を受けたものです。この場を借りて、感謝の意を表します。

参考文献

- [1] Y. Bai, H. Kobayashi, "Intrusion Detection Systems: technology and development," Proceeding of 17th International conference on Advanced Information Networking and Applications(AINA 2003), (2003).
- [2] Atilla Ozgur, Hamit Erdem, "A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015 (online)," available from <https://peerj.com/preprints/1954/> (accessed 2018-04-26).
- [3] "Weka 3 - Data Mining with Open Source Machine Learning Software in Java (online)," available from <https://www.cs.waikato.ac.nz/ml/weka/> (accessed 2018-04-26).
- [4] "MATLAB - 技術計算言語 - MATLAB & Simulink," available from <https://jp.mathworks.com/products/matlab.html>, (accessed 2018-04-26).
- [5] "LIBSVM -- A Library for Support Vector Machines," available from <LIBSVM -- A Library for Support Vector Machines> (accessed 2018-04-26).
- [6] "java.com あなたと Java (online)," available from <https://java.com/ja/> (accessed 2018-04-26).
- [7] "Welcome to Python.org (online)," available from <https://www.python.org/> (accessed 2018-04-26).
- [8] "R The R Project for Statistical Computing (online)," available from <https://www.r-project.org/> (accessed 2018-04-26).
- [9] "KDD Cup 1999 Data," available from <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html> (accessed 2018-04-26).
- [10] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," *Proc. the 2009 IEEE Symposium on Computational Intelligence in Security and Defense Applications* (CISA 2009), pp.53-58 (2009).
- [11] Saffa O. Al-mamory, Firas S. Jassim: Evaluation of Different Data Mining Algorithms with KDD CUP 99 Data Set, *Journal of Babylon University, Pure and Applied Sciences*, vol.21, no.8, p.2663-2681 (2013).
- [12] "NSL-KDD Datasets Research Canadian Institute for Cybersecurity UNB (online)," available from <http://www.unb.ca/cic/datasets/nsl.html> (accessed 2018-04-26).
- [13] S. Revathi, A. Malathi, "A Detailed Analysis on NSL-KDD Dataset Using Various Machine Learning Techniques for Intrusion Detection," *International Journal of Engineering Research & Technology (IJERT)*, vol.2, Issue 12, p.1848-1853 (2013).
- [14] "MIT Lincoln Laboratory DARPA Intrusion Detection Evaluation (online)," available from <https://www.ll.mit.edu/ideval/data/1998data.html> (accessed 2018-04-26).
- [15] "Traffic Data from Kyoto University's Honeypots (online)," available from <http://www.takakura.com/Kyoto_data/> (accessed 2018-04-30).
- [16] Jungsuk SONG, Hiroki Takakura, and Yasuo Okabe, "Description of Kyoto University Benchmark Data (online)," available from <http://www.takakura.com/Kyoto_data/BenchmarkData-Description-v5.pdf> (accessed 2018-04-26).
- [17] Jungsuk Song, Hiroki Takakura, Yasuo Okabe, Masashi Eto, Daisuke Inoue, Koji Nkao, "Statistical Analysis of Honeypot Data and Building of Kyoto 2006+ Dataset for NIDS Evaluation," In Proceedings of The 1st International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS'11), pp.29-36, (2011).
- [18] Jungsuk SONG, Hiroki TAKAKURA, Yasuo OKABE, "Cooperation of Intelligent Honeypots to Detect Unknown Malicious Code," in Proceedings of Workshop on Information Security Threats Data Collection and Sharing (WOMABT), pp.31-39, (2008).
- [19] Iman Sharafaldin, Arash Habibi Lashkari and Ali A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," In Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2018), pp.108-116, (2018).
- [20] Iman Sharafaldin, Amirhossein Gharib, Arash Habibi Lashkari and Ali A. Ghorbani, "Towards a Reliable Intrusion Detection Benchmark Dataset," *Journal of Software Networking*, Vol.2017, Issue 1, pp.177-200, (2018).
- [21] "IDS 2017 Datasets Research Canadian Institute for Cybersecurity UNB (online)," available from <http://www.unb.ca/cic/datasets/ids-2017.html> (accessed 2018-04-26).
- [22] "マルウェア対策研究人材育成ワークショップ 2017 (MWS2017)(online)," available from <https://www.iwsec.org/mws/2017/about.html> (accessed 2018-04-26).
- [23] 多田竜之介, 小林良太郎, 嶋田創, 高倉弘喜, "NIDS 評価用データセット: Kyoto 2016 Dataset の作成," *情報処理学会論文誌*, Volume 58, No.9, pp1450-1463, (2017).
- [24] "第 15 回科学技術・学術審議会 総合政策特別委員会 資料 3 H28.11.24(online)," available from <http://www.mext.go.jp/b_menu/shingi/gijyutu/gijyutu22/siryo/_ic_sFiles/afidfield/2016/12/08/1380241_04.pdf> (accessed 2018-05-06).
- [25] 高田雄太, 寺田真敏, 村上純一, 笠間貴弘, 吉岡克哉, 畑田充弘, "マルウェア対策のための研究用データセット ～MWS Datasets 2016～ (online)," available from <http://www.iwsec.org-mws-2016-20160714-takata-dataset.pdf> (accessed 2018-04-26).
- [26] "高等教育機関における情報セキュリティポリシー策定について - 事業 - 国立情報学研究所(online)," available from <https://www.nii.ac.jp/service/sp/> (accessed 2018-05-06).