ダークネットトラフィックの可視化とオンライン更新によるモニタリング

畑中 拓哉[1]　北園 淳[1]　小澤 誠一[1]　班 涛[2]　中里 純二[2]　島村 隼平[3]

概要：未使用の IP アドレス空間であるダークネットには，DDoS 攻撃への返信やスキャンなど，不正な通信に伴うパケットが大量に届く．それらを観測・分析することで，インターネット上で発生している悪性な活動の動向を把握することが可能になると期待されている．本論文では，ダークネットの通信パターンの分布を可視化しモニタリングする手法を提案する．提案法では，通信パターンを特徴ベクトルとして表現し，次元圧縮することで 2 次元の散布図として可視化する．また，新たな観測データが得られる毎に散布図を逐次更新することで，リアルタイムに変化を捉える．これにより，攻撃の傾向の変化や新たな攻撃の発生の検知を行うことが期待される．

キーワード：ダークネット，スキャン，可視化，モニタリング

1. はじめに

近年，コンピュータやネットワークの普及により，様々なサービスをネットワークを通して受けるようになった．しかしその一方でサーバのサービス停止や個人情報の漏洩などを目的とした不正なプログラムであるマルウェアに侵される危険も含んでおり，その対策が必要とされている．

攻撃対象を探すために宛先をランダム，もしくは総当たりにして接続を試みることでサーバのセキュリティに脆弱性がないかを調べることをスキャンという．このようにスキャンは攻撃の始まりといえるので，悪意のあるスキャンを受けた場合に，それを検知し，早急にセキュリティの向上など対策を行うことで，その後の攻撃を未然に防ぐことが可能であると考えられる．

しかしパケットが正常なものか不正なものかを判断することは容易ではない．そこで，ダークネット [1] で観測されたパケットを使用する方法がある．ダークネットとは，到達可能かつ特定のホストコンピュータに割り当てられていない IP アドレス空間のことである．ダークネットのアドレスは使用されていないにもかかわらず，実際には相当数のパケットがダークネット上で観測される．この原因となっているのが，ランダムに IP アドレスを生成し行うスキャン行為や，送信元を詐称した DDoS 攻撃の跳ね返りパケットであるバックスキャッタなどが挙げられる．実際に，スキャンがダークネットで観測される例として，あるアドレス空間に対して総当たりでパケットを送ると，宛先の IP アドレスの中には，ホストが割り当てられていないものも存在する，そういった IP アドレスに送信されたパケットはダークネットで観測される．つまりダークネットに到達するパケットは何らかの不正な活動に起因していると考えられる．

攻撃のパターンは，様々であり日々変化していき新しいものが現れてくる．そこで本稿では，ダークネットで観測されたスキャンパケットから特徴ベクトルを作成し，特徴ベクトルを 2 次元に次元削減を行い平面に可視化する．可視化することで，時間変化による攻撃や活動パターンの多様化が容易に確認することができる．さらに新たなデータが観測されると逐次追加し，散布図を更新していくことで，ダークネットトラフィックのモニタリングを行い，新しい攻撃の早期検知を目指す．

可視化のための次元削減には，t 分布型確率的近傍埋め込み法 t-SNE(t-distributed stochastic neighbor embedding)[2] を用いる．t-SNE を用いる理由として，今回扱うデータが非線形で高次元のクラスタ構造を持つことが挙げられる．他の次元削減手法としては，例えば，線形な手法である主成分分析と（古典的）多次元尺度構成法がある．これらの手法では，元のデータ点間の距離関係を保存するように次元を削減するが，非線形構造・クラスタ構造の抽出には必ずしも適していない．非線形な次元削減手法の代

1　神戸大学大学院工学研究科
2　国立研究開発法人 情報通信研究機構
3　株式会社クルウィット

表例としては，Isomap [3]，Locally linear embedding [4]，Laplacian eigenmaps [5]，Diffusion maps [6] などが挙げられる．これらの手法は，データが低次元の多様体上に分布していると仮定できる場合には有効であり，人工データでその有用性が確認されている．しかしながら，多くの実データではその仮定は成立せず，必ずしも良い結果が得られないことが知られている．一方で t-SNE は，非線形・高次元の構造の抽出に適しているとされ，実データに対する実験でその有効性が確認されている．

t-SNE の損失関数 C は，回転や平行移動について不変であり，最適化の初期値に依存して，向きが変わる．このため，新しく観測されたデータを追加し，そのまま t-SNE で次元削減をし直し可視化を行った場合，前回の可視化結果とは，大きく異なる図になる可能性があり，新しい攻撃などが現れていたとしても視覚的に捕らえることが容易ではない．そこで，新しいデータを追加し，t-SNE で次元削減を行う際に，前回の結果を次の計算の初期値として与えることで，前回結果の図からそれぞれのデータの位置関係が大きく変わることなく更新できることを示す．さらに視覚的な比較をしやすくするために，スケーリングを行い可視化結果を更新した際の図の変化を少なくする．

2. 提案手法

2.1 特徴ベクトル作成

特徴ベクトルの作成 [7][8] には，ホストごとに最初のパケットが観測されてから 30 秒間のパケットを使用する．このとき観測されたパケット数が 20 未満であった場合は，特徴ベクトルは作成せず，時間をずらし 20 パケット取得するまで，観測を続ける．この理由として，少ないパケット数で特徴ベクトルを生成した場合に十分な情報が得られないと考えられるためである．また，1 時間パケットが観測されなかったとき，そのホストより新たな攻撃が行われている可能性が考えられるので，1 時間後以降に新しくパケットを抽出し，再度特徴ベクトルを作成する．

次に，特徴ベクトル作成に用いた 17 個の特徴を以下に示す．また，パケット数に関する特徴は，特徴ベクトル間で大きな差が見られるため，自然対数をとる．

- パケット総数
- 送信元ポートごとの送信されたパケット数の平均・分散
- 送信先 IP アドレスごとの送信されたパケット数の平均・分散
- 送信先ポートごとの送信されたパケット数の平均・分散
- パケット間の時間間隔の平均・分散
- プロトコルの種類の総数
- 送信元ポートの総数
- 送信先 IP アドレスの総数
- パケット間の送信先 IP アドレスの差分の平均・分散
- 送信先ポートの総数
- ペイロードのサイズの平均・分散

これらの特徴がスキャンなどの判別に有効である理由として，たとえば，DDoS 攻撃では，送信元ポートを自由に設定でき，その返信パケットの送信先ポート番号はランダムになり，その数は大きくなる傾向にある．それに対して IP スキャンは，ある特定のポート番号に向けてパケットを送りアプリケーションの脆弱性を調べるものなので，送信先のポート番号の数は限られてくる．これらの差より，どういった攻撃であるかの判別が可能である．

特徴ベクトルの作成に使用した特徴量の中で，パケット数やペイロードサイズ等の特徴は非常に大きな値をとる場合がある．この場合，これらの値の大きい特徴の影響が大きく出てしまい，他の小さい値の特徴が無視されてしまう可能性があるので，これを避けるために，各特徴の最大値が 1，最小値が 0 となるように値の正規化を行う．これによりすべての特徴を偏りなく用いて判定を行えるようになる．

2.2 次元削減

可視化を目的とした次元削減では，一般に，N 個の高次元ベクトルからなるデータ $\boldsymbol{X}=(\boldsymbol{x}_1,...,\boldsymbol{x}_N)$ が与えられたとき，このベクトル同士の位置関係を保ちながら，低次元（通常は 2 もしくは 3 次元）ベクトル $\boldsymbol{Y}=(\boldsymbol{y}_1,...,\boldsymbol{y}_N)$ に写像する．これにより，Y について散布図を描くことで，データ点同士の関係性を把握することが可能になる．この次元削減手法の中でも，t-SNE は，元のデータが非線形で高次元のクラスタ構造を持つ場合に有効であることが知られている．

t-SNE の特徴は 2 点間の近さを確率分布で表すところにある．t-SNE では，基準となる点 $\boldsymbol{x}_i$ を中心とした正規分布を考える．まず，点 $\boldsymbol{x}_i$ から見た点 $\boldsymbol{x}_j$ の近さを表す確率 $p_{j|i}$ を定義し，それを元に，対称化した確率 p_{ij} を定義する．

$$p_{j|i} = \frac{\exp(-\,||\,\boldsymbol{x}_i-\boldsymbol{x}_j\,||^2/2{\sigma_i}^2)}{\sum_{k\neq i}\exp(-\,||\,\boldsymbol{x}_i-\boldsymbol{x}_k\,||^2/2{\sigma_i}^2)}, p_{i|i}=0 \quad (1)$$

$$p_{ij} = \frac{p_{j|i}+p_{i|j}}{2N} \quad (2)$$

${\sigma_i}^2$ は分散を表す．これにより，$\boldsymbol{x}_i$ の近くにある点ほど p_{ij} は大きくなり，遠くにある点ほど p_{ij} は小さくなる．

次に，次元圧縮後の点 $\boldsymbol{y}_i$ と点 $\boldsymbol{y}_j$ の近さを表す確立 q_{ij} を考える．これらは次元圧縮前の $\boldsymbol{x}_i$ と $\boldsymbol{x}_j$ に対応している．次元圧縮後の近さも同様に確率分布で表現するが，正規分布ではなく，自由度 1 の t 分布で考える．

$$q_{ij} = \frac{(1+||\,\boldsymbol{y}_i-\boldsymbol{y}_j\,||^2)^{-1}}{\sum_{k\neq l}(1+||\,\boldsymbol{y}_k-\boldsymbol{y}_l\,||^2)^{-1}}, q_{ii}=0 \quad (3)$$

次元圧縮後の点 $\boldsymbol{y}_i$ の位置は，次元圧縮前の確率分布 p_{ij} と

次元圧縮後の確率分布 q_{ij} の KL(カルバック・ライブラー)情報量を計算し，これを最小化することで求められる．この KL 情報量を損失関数 C とする．

$$C = \mathrm{KL}(P||Q) = \sum_{i \neq j} p_{ij} \log \frac{p_{ij}}{q_{ij}} \tag{4}$$

正規分布よりも裾の重い t 分布を用いることによって，圧縮前の点 $\boldsymbol{x}_i$ と点 $\boldsymbol{x}_j$ がある程度離れているデータであった場合，圧縮後の点 $\boldsymbol{y}_i$ と点 $\boldsymbol{y}_j$ をより遠くに配置することになる．つまり，t 分布を用いることで，圧縮前と圧縮後のデータ点の位置関係として近いデータ同士は近いまま，離れているデータ同士はより遠くの位置に写像することになる．これにより，高次元データを低次元に圧縮する際に問題となる crowding problem [2] を軽減することが出来る．これが，t-SNE が元のデータが特に高次元の場合に有効な理由とされる．より詳細な議論は [2] を参照されたい．

損失関数 C の最小化は，勾配

$$\frac{\partial C}{\partial \boldsymbol{y}_i} = 4 \sum_j \frac{(p_{ij} - q_{ij})(\boldsymbol{y}_i - \boldsymbol{y}_j)}{1 + || \boldsymbol{y}_i - \boldsymbol{y}_j ||^2} \tag{5}$$

を用いて最急降下法等によって行われる．

2.3 t-SNE のオンライン更新

本稿で提案する t-SNE による可視化結果の更新アルゴリズムを Algorithm 1 に示す．

Algorithm 1 t-SNE のオンライン更新

Input: 入力データ $\boldsymbol{X}$

1: t-SNE により可視化
2: 新たに観測されたデータを追加
3: 前回結果から初期値を設定
4: 再び t-SNE を行い可視化結果の更新
5: スケーリング
6: 2〜5 を繰り返しデータが追加されるごとに更新

まず，いくらかのデータを t-SNE により次元削減を行い，2 次元に可視化する．次に，その時点から新しく観測されたデータを追加し，前回扱ったデータとまとめて t-SNE で次元削減を行う．この時，前回の可視化結果を初期値として計算することで，前回結果からデータの位置関係をなるべく保ちながら更新する．最後にスケーリングを行うことで，より前回結果に近づけ新しい可視化結果との比較を視覚的に容易にする．この手順を新たなデータが観測されると逐次的に行い，可視化結果を更新していくことで，ダークネットトラフィックのモニタリングを行う．

3. 実験

3.1 実験設定

実験に用いるデータセットには，NICT のダークネットで観測されたパケットデータのうち，2014 年 2 月 1 日のデータ，その中の TCP 通信における SYN パケットのスキャンと UDP 通信におけるスキャンパケットを使用した．実験に用いたデータセットと特徴ベクトル数の詳細は表 1 と表 2 に示す．

表 1: 使用したデータの詳細

データセット	ホスト数	特徴ベクトル数
TCP(SYN)	1970	1996
UDP	47	48
合計	2017	2044

表 2: 時間帯ごとの特徴ベクトル数

観測された時間帯	特徴ベクトル数
0 時	50
1 時	45
2 時	29
3 時	25
4 時	31
5 時	28
6 時	28
7 時	20
8 時	13
9 時	19
10 時	47
11 時	14
12 時	12
13 時	21
14 時	15
15 時	11
16 時	24
17 時	265
18 時	231
19 時	242
20 時	221
21 時	230
22 時	214
23 時	209

スキャンであるかどうかの判断は，特徴ベクトルごとに可視化されたパケットの送信元のホストから送信先のダークネットの IP やポート等の情報を含む図に基づいて，専門的な知識による判断によって与えられる [7]．ラベル付けに用いたホストの活動を表す図の一例を図 1 に示す．

図の左半分の縦軸は送信元のポート番号，横軸はパケットの送信された時間を表す．右半分の縦軸は送信先のポート番号，横軸は送信先の IP アドレスを表す．この 2 点を結ぶことでパケットごとの送信された時間，送信元のポート番号，送信先のポート番号，送信先の IP アドレスを表す．線の色はパケットのプロトコル，TCP 制御フラグを表わす．青色は SYN パケットを表わす．

まず 2 月 1 日の 12 時までに観測されたデータを用いて

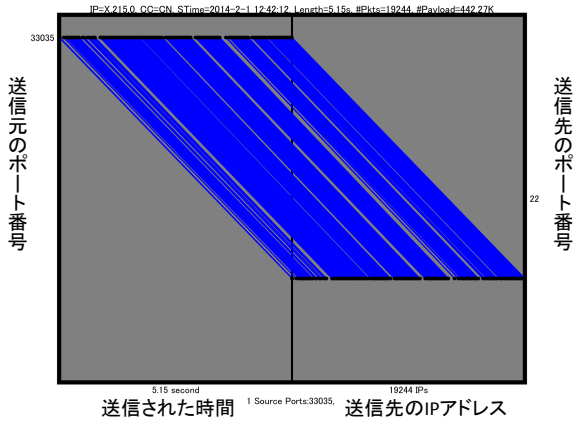


図 1: ホストの活動の例

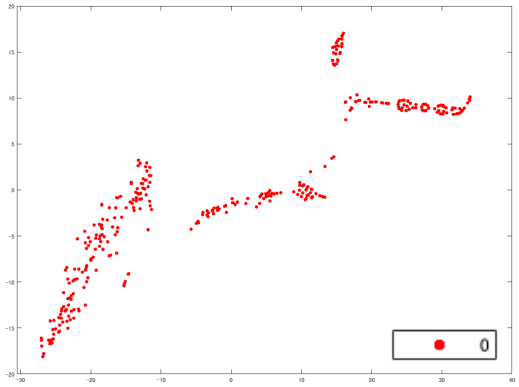


図 2: 2014 年 2 月 1 日 12:00 までに観測されたデータの可視化結果.

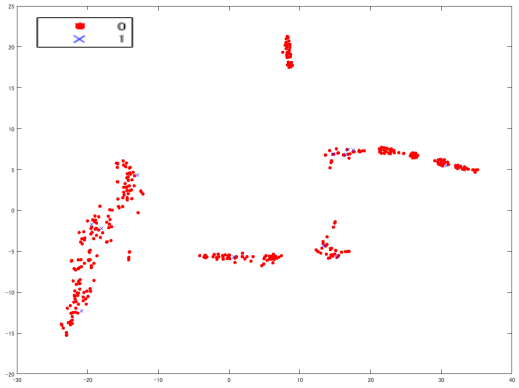


図 3: 2014 年 2 月 1 日 12 時までのデータに 12 時台に観測されたデータを追加し更新した可視化結果．赤色の点が 12 時までのデータ，青色の×の点が 12 時台のデータを表す．

t-SNE により次元削減を行い，可視化する．次に 2 月 1 日 12 時台に観測されたデータを追加し，合わせて次元削減を行い可視化結果を更新する．これを繰り返し，13 時台のデータ，14 時台のデータと順に追加，可視化を行い，散布図を逐次更新していくことで，ダークネットトラフィックのモニタリングを行う．

新しく観測されたデータを追加し，次元削減を行う際に，前回の結果をなるべく保ちながら更新するために，前回結果の座標を初期値として与え次の計算を行う．新しく追加したデータの初期値は，元の高次元空間において最も近い距離にある確率が高い前回データの座標を初期値として与える．また視覚的に前回結果との比較を容易にするためスケーリングを行うことで，より前回結果に近づける．スケーリングは，前回結果の座標の値を新しい結果の座標の値で割り，さらにその値の平均を取り，新しい結果の座標にかけることで前回結果の座標位置に合わせる．

3.2 実験結果

図 2 は 2104 年 2 月 1 日 12 時までに観測されたのデータを可視化した結果を示す．次に，図 3 は 2 月 1 日 12 時台に観測されたデータを 2 月 1 日 12 時までのデータに追加し，合わせて次元削減を行い，可視化した結果を示す．ラベルが 0 で赤色の点が前回のデータ，ラベルが 1 で青色の×で表示されているものが新たに追加したデータを表す．図 2 と図 3 より，新しく観測されたデータを追加しても，前回の結果をある程度保ちながら可視化結果の更新が出来ているといえる．

図 4a〜図 4k は，さらに 1 時間ごとにデータを追加し，可視化結果を更新したものを示す．これらの図からも前回の結果を保ちながら可視化結果の更新が出来ているといえる．

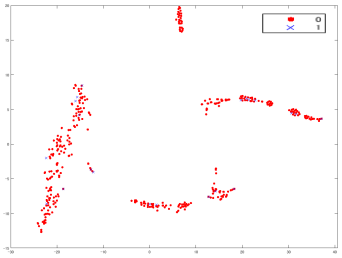
4. 考察

3.2 節より，前回結果を初期値として与え計算し，スケーリングを行うことで，前回結果をほぼ保ちながら可視化結果の更新が可能であった．これにより，可視化結果を更新した際に，前回のものと比べ，新しい場所にクラスタが形成されていた場合，それらのデータは，なにか新しい攻撃の特徴を持っている可能性があることを示せる．

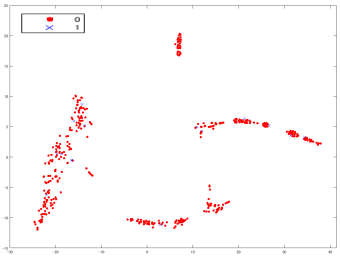
実際に，図 4e を見ると，青色で表されている追加したデータが，赤色で表されている前回のデータとは，異なる位置にクラスタを形成している．このことから，2014 年 2 月 1 日の 17 時までに観測されたデータには無かった新しい特徴を持った可能性があるデータが同日の 18 時台に観測されたといえる．つまり，この新しいデータは，前回までのデータとは違った特徴を持っており新しい攻撃のパターンの可能性があるといえる．

5. まとめ

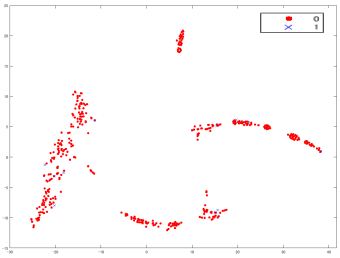
本稿では，ダークネットで観測されたスキャンパケットを可視化し，モニタリングの手法を提案した．提案手法では，ダークネットから観測されたパケットのデータをホス



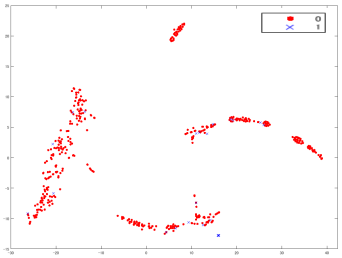
(a) 2014 年 2 月 1 日 14:00



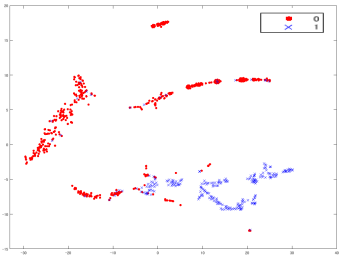
(b) 2014 年 2 月 1 日 15:00



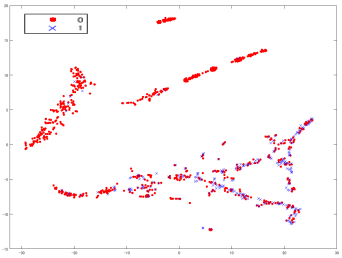
(c) 2014 年 2 月 1 日 16:00



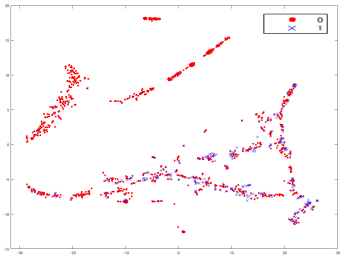
(d) 2014 年 2 月 1 日 17:00



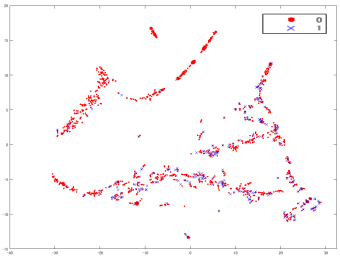
(e) 2014 年 2 月 1 日 18:00



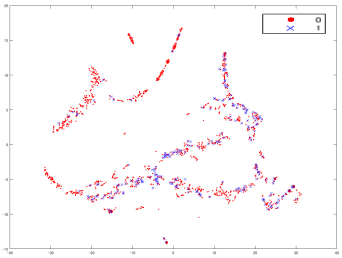
(f) 2014 年 2 月 1 日 19:00



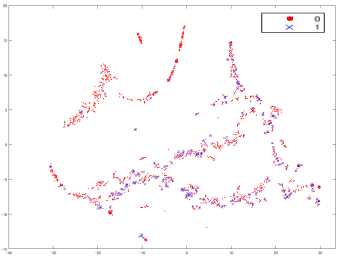
(g) 2014 年 2 月 1 日 20:00



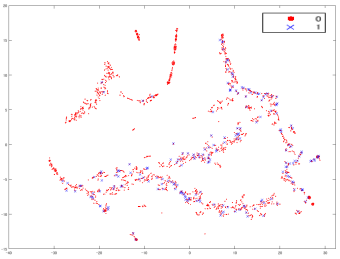
(h) 2014 年 2 月 1 日 21:00



(i) 2014 年 2 月 1 日 22:00



(j) 2014 年 2 月 1 日 23:00



(k) 2014 年 2 月 1 日 24:00

図 4: 2 月 1 日 13 時以降のデータを 1 時間ごとに追加した可視化結果．赤色の点が前回までのデータ，青色の×の点が新たに追加したデータを表す．

トごとに分割し，最初のパケットが観測されてから短い時間のパケットを用いて，特徴ベクトルを作成した．そして，作成した特徴ベクトルは 17 次元なので t-SNE を用いて次元削減を行い 2 次元のデータにすることで，可視化を行った．次に，新しく観測されたデータを追加し，合わせて次元削減を行い可視化した．この時に，前回結果を初期値として与えて計算することで，前回の結果を保ちながら可視化結果を更新した．されにスケーリングを行いより前回の結果に近づけることで視覚的な比較を容易にした．

実験結果より，可視化結果の更新において，前回の結果を保ちながら更新することができた．また，更新した際に，追加したデータが新しい位置にクラスタを形成していた部分が存在したことから，提案法によって，従来とは異なる新たな攻撃パターンを検知可能となることが期待される．

今回の実験には，1 日分のデータを用いたが，今後は，さらに長い期間でモニタリングを目指す．ただ新たなデータを追加していくだけでは，いずれデータ量が莫大になり上手く可視化できないことが予想されるので，データの追

加と同時にデータの消去を行っていく必要が考えられる．

参考文献

[1] D. Moore, C. Shannon, G. Voelker, and S. Savage, "Network Telescopes: Techical Report", Department of Computer Science and Engineering, University of California, San Diego, 2004.

[2] L. van der Maaten, G. Hinton, "Visualizing Data using t-SNE," Journal of Machine Learning Research, vol. 9, pp. 2579-2605, 2008.

[3] Tenenbaum, J.B., De Silva, V., Langford, J.C., "A Global Geometric Framework for Nonlinear Dimensionality Reduction," Science, vol. 290(5500), pp.23192323, 2000.

[4] Roweis, S.T., Saul, L.K., "Nonlinear Dimensionality Reduction by Locally Linear Embedding," Science, vol. 290(5500), pp.23232326, 2000.

[5] Belkin, M., Niyogi, P., "Laplacian Eigenmaps for Dimensionality Reduction and Data Representation," Neural Computation, vol. 15(6), pp.13731396, 2003.

[6] Lafon, S., Lee, A.B.: Diffusion Maps and Coarse-graining: A Unified Framework for Dimensionality Reduction, Graph Partitioning, and Data Set Parameterization. Pattern Analysis and Machine Intelligence, IEEE Transactions on 28(9), 13931403 (2006)

[7] N. Furutani, T. Ban, J. Nakazato, J. Shima-mura, J. Kitazono, and S. Ozawa,"Detection of DDoS Backscatter Based on Traffic Features of Darknet TCP Packets, " 2014 Ninth Asia Joint Conference on Information Security, pp. 39-43, 2014

[8] N. Furutani, T. Ban, J. Nakazato, J. Shima-mura, J. Kitazono, and S. Ozawa,"Adaptive DDoS-Event Detection from Big Darknet Traffic Data, " 2015 International Conference on Neural Information Processing, pp. 376-383, 2015