3-2　ネットワークにおけるデータマイニング

3-2　Data Mining over Network Streams

班　涛　　門林雄基
BAN Tao and KADOBAYASHI Youki

要旨

ネットワーク監視・分析システム（NMASes）は、サイバー攻撃の予防、インターネット上に出現する脅威に対する実用的かつ予防的な防御の提供に関して、有効な役割を果たしてきている。当論文では、トレースバックネットワーク分析システム（TBNAN）の概要を述べる。これは、アルゴリズムに基づく一連のデータマイニングを使用し、サイバーセキュリティのさまざまな局面に対処し、ネットワーク管理を容易にするものである。TBNANのさまざまな構成要素（例：統計分類エンジン、異常値検出およびデータ・クラスタリングモジュールなど）は、監視されているネットワークのステータスの表示およびネットワーク上のさまざまなタイプの攻撃および侵入の検出に役立つ可能性がある。我々の分析は、TBNANによって実装される機能が従来のシグネチャベースのシステムの機能を補完することを示している。そしてこの両者を組み合せることによって、サイバー攻撃の脅威およびネットワークインシデントへの効果的な対策に関する、ネットワーク管理者のツールボックスを拡張する可能性を含んでいる。

Network monitoring and analyzing systems (NMASes) have been playing an active roll for preventing cyber attacks and providing practical and proactive defense against emerging threads over the Internet. This paper provides an overview of the TraceBack Network ANalyzer (TBNAN), which uses a suite of data mining based algorithms to address different aspects of cyber security and facilitate network management. The various components of TBNAN such as the statistical classification engines, anomaly detectors, and data clustering modules, could help to illustrate the status of the monitored network as well as detect different types of attacks and intrusions against the network. Our analysis shows that the functionalities implemented by TBNAN are complementary to those of traditional signature based systems, implying that the both of them can be combined to enlarge the toolbox of a network administrator for efficient cyber threat and network incident countermeasure.

[キーワード]
サイバーセキュリティ，ネットワーク監視・分析システム，トレースバックネットワーク分析システム，トラフィック分類
Cyber security, Network monitoring and analysis system, TraceBack Network Analyzer, Traffic classification

1　序論

コンピュータネットワーク通信およびサイバーインフラストラクチャへの依存が高まった結果、サイバーセキュリティは広範囲な実用的領域において（例：インターネット接続サービス提供、銀行業、電子商取引、および通信における個人情報保護など）非常に重要となってきている。出現する脆弱性および脅威の組合せにより、サイバーセキュリティが現在のサイバー空間の自動化の更なる発展にとって、事実上の障壁となっている。従来のセキュリティソリューションシステム（例：ウイルス対策ソフト、迷惑メールフィルタなど）は通常、新たな脅威の識別、特定の特徴の抽出、および新たに出現した脅威の防止目的でシステムを更新するために、広範囲にわたる人的努力に依存している[1]。幸いにも、計算知能（CI）の研究により、動的な意思決定に関するデータマイニングと

機械学習の汎用性が明らかになった。この結果、サイバーセキュリティ問題への対応に要していた大きな労力の大部分が削減可能となり、高度なデータマイニングと機械学習のアルゴリズムを適用することによって、更に効率的となった[1]-[3]。

インターネット上のトラフィック監視および分析には、ネットワークに影響を与えるサイバーセキュリティ問題に対処する便利なツールが存在していた[4]。代表的なネットワーク監視および分析システム（NMAS）は、知的な手法で監視されたコンピュータネットワーク上の、異常なステータスまたはパフォーマンスの低下を検出する機能を備え、システムの警告をネットワーク管理者に送信する。したがって、NMASは、ネットワークに悪影響を与える脅威からの保護、およびマルウェアまたは重要なインターネットリソースの悪用によって生じるリスクおよび損失の最小化に役立ってきた。NMASは、以下において有益なアプリケーションであると判明することが多い。(1) ネットワークサーバの負荷の監視および管理、(2) 外部侵入に対する侵入検出、(3) IPアドレススプーフィングを使用して、攻撃者の場所を特定するためのIPトレースバック、(4) ウイルスの伝播、マルウェアの活動、ボットネットの動作の追跡のための監視システム。

当論文で紹介されているトレースバックネットワーク分析システム（TBNAN）は、高速ネットワーク環境および複雑なプロトコル向けの汎用性のあるNMASとして開発されてきた。TBNANの主な設計原則の1つは、適応性と汎用性である。TBNANは、異なる目的のネットワークへの複数のアクセスポイントに適用可能と考えられている。以下は、TBNANの用途となる可能性がある、いくつかの典型的なシナリオである。大学のゲートウェイのようなインターネットバックボーンのアクセスポイントに導入される場合、ネットワークの輻輳に関連する大規模なネットワーク攻撃や異常ステータスの検出に役立つ。ローカルネットワークのゲートウェイに適用される場合、P2Pファイル共有クライアントを識別し、容量計画を容易にする。複数の仮想マシンクライアントのホストとなっているクラウドサーバに導入されている場合、マルウェア感染の予防的な検出に関するアプリケーションの動作を監視することができる。パーソナルコンピュータにインストールされる場合、システムの設定ミスを検出したり、マルウェアによって引き起こされる説明のつかないスレッドを識別するために役立つ。このような適応性を実現する主な要因は、監視および分析エンジンの動作が軽いことである。この結果、トラフィックのスループットが非常に高いアクセスポイントの場合でも、監視されているネットワークへの負荷は少ない。一方、この軽さは、調整可能なサンプリングレートをサポートするフロージェネレータに依存する。また、サンプリングレートに対する慎重なシステムパフォーマンスチューニング（すなわち正確さとシステム応答時間）も、主な要因の1つとなる。

当論文では、TBNANの基本的な設計原則およびネットワークの管理と脅威への対応策に適用される代表的なシナリオのいくつかを紹介する。以降、当論文の構成は次のようになっている。**2**：TBNANシステムの全体的な論評の提示。**3**：ケーススタディにより、TBNANに組み込まれた知的分析エンジンの詳細な紹介の提示。**4**：論文の結論。

2　TBNANの概要

図1に説明されているように、TBNANの全体的なシステム構造は、3つのサーバ（すなわちパケットプロセッサ、計算サーバ、データベースおよびウェブサーバ）から構成されている。以下では、3つのコンポーネントサーバに関する簡潔な紹介を行う。

2.1　パケットプロセッサ

パケットプロセッサ（PP）は、アクセスポイントを通過するトラフィックをキャプチャしてトラフィックから統計的な量を抽出した後に、このデータを計算サーバへ転送する。ユーザの個人情報を保護するために、PPはペイロード情報を検査しない（ただし場合によっては、更なる検査のために、ペイロード情報の限られたバイト数がキャッシュされる可能性がある）。ペイロード情報を検査しないことによって、暗号化されたペイロードのプロトコルに関するリバースエンジニアリングを回避し、次世代ブロードバンドネット

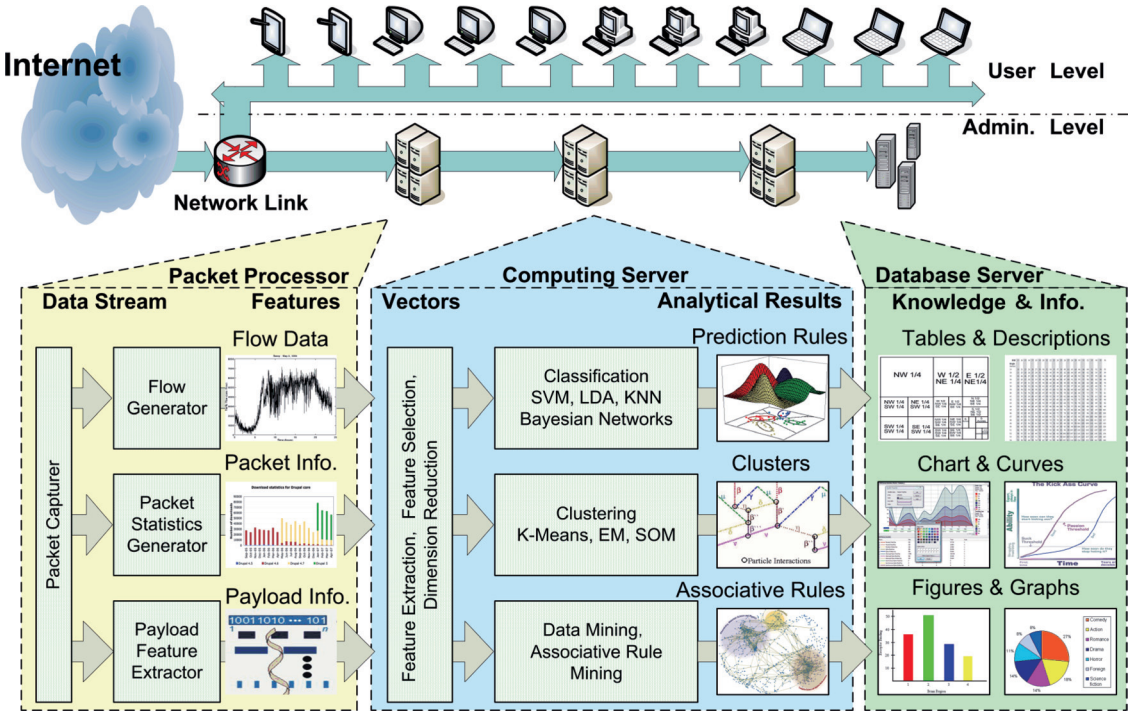


図 1　TBNAN システムの全体的な枠組み

ワークでのリアルタイム監視に関する性能要件を満たすのである。

以下、PP がパケットヘッダ（すなわちデータリンク層、ネットワーク層、およびトランスポート層）から抽出した、空間および時間に関する統計的量を識別値とする。基本的に識別値はネットワーク流に基づいて抽出され、このフローは、ソースコンピュータから送信先までのパケットの順序を意味している。ソース IP、送信先 IP、プロトコル、ソースポート、送信先ポートの 5 つの要素からなる組で、一定の期間内の TCP/IP 通信セッションを一意に識別することができるため、これらの 5 つはフローの実質的な定義に使用される。一般的に受入れられているフローのタイムアウトは、文献 [5] に提言されている 64 秒である。すなわち、特定のフローにパケットが 64 秒間到達しなければ、このフローは無効となる。ホスト分散およびトラフィック量のような識別値は、トラフィックの特性を表すために使用される。ただしフローに基づく識別値が不十分な場合があり、例として P2P ファイル共有ノード識別のために TBNAN を導入する場合が挙げられる（**3.1** を参照）。このような場合、フローレベルを超えてホストレベルに行き、ホストレベルでは通信の全体像が識別値で示される。これを行うために、対象ホストにつながるすべての通信を単一のストリームとして扱い、これに関する識別値を抽出する。TBNAN では、ネットワークトレースの収集をサポートする主な組み込みツールは、移植性のある libpcap C/C++ ライブラリである [6]。このツールは、高速交換ネットワークを監視するための業界標準技術である NetFlow または sFlow から生成されるフローに関する分析も、サポートしている。

2.2　計算サーバ

データを受信するデータマイニングエンジンを導入することによって、計算サーバは予測モデルを作成する。現在 TBNAN では、分析エンジンの以下の 3 タイプを使用している。

2.2.1　統計分類

統計分類とは、統計上の特徴に基づいて既知のクラスにネットワークストリームを分類する処理である。ネットワークへのアクセスポイントおよび学習の目的に応じて、TBNAN は異なる識別値

に異なる分類エンジンを導入する。正規ユーザからP2Pファイル共有クライアントを使用しているユーザを識別する方法のケーススタディに関しては、**3.1**を参照のこと。通常のネットワークトラフィックおよびサイバー攻撃にネットワーク流を分類する方法のケーススタディに関しては、**3.2**を参照のこと。

2.2.2 異常値検出

異常値検出とは、設定された通常の動作と合致しないパターンを、特定のデータにて検出することを意味する[7][8]。したがって検出される異常なパターンを異常値と呼び、これはアプリケーション領域において重大で利用可能な情報につながることが多い。TBNANの異常値検出エンジンは通常のネットワークストリームのモデルを構築し、監視されたストリームにおける通常のモデルとのずれを検出し、これを異常ステータスとして予測する。ネットワークスキャンを識別するための異常値検出の例については、**3.3**を参照のこと。

2.2.3 クラスタリング

クラスタリングまたはクラスタ分析は、サブセット（クラスタとも呼ばれる）に対する一連の監視の割り当てである。これによって同じクラスタにおける監視は、類似の基準値によって同じように計測される。データにおけるアイテム数を削減し、個別の簡潔なプロファイルを提供することによって、クラスタリングはデータを手早く確認するために適した方法である。ネットワーク攻撃タイプの分析に関するクラスタリングの例については、**3.4**を参照のこと。

2.3 データベースおよびウェブサーバ

データベースおよびウェブサーバによって、ユーザにインポートされたデータの索引作業および可視化サービスおよび計算サーバから取得された分析結果（例：グラフィックスおよびサマリレポート）が提供される。このサーバのキーポイントの1つは、ストレージ内のデータの整理方法で、これはユーザの問い合わせへの回答のパフォーマンスを最適化するためのものである。データベース管理技術は、コンピュータ科学および工学の様々な分野で幅広く研究され、当論文の範囲を超えるものである。

3 分析エンジンおよびケーススタディ

ここでは、さまざまなサイバーセキュリティの目的ごとに異なる分析エンジンの、ケーススタディおよびパフォーマンス評価について記述する。

3.1 P2Pファイル共有ノード分類

最近の電気通信ネットワークの統計的研究では、ピアツーピア（P2P）ファイル共有が増加し続け、現在ではインターネット上のトラフィック全体の50～80%を占めていることが概説されている[9]。更に、ストリーミングメディア、インターネット電話およびインスタントメッセージングといったより多くの電気通信ネットワークアプリケーションが、P2Pの形式をとっている。帯域集中型の性質をもつP2Pアプリケーションは、基盤となるネットワークにP2Pトラフィックが甚大な影響を与える可能性を示唆している。したがってこの種のトラフィックを分析および特徴づけることは、ネットワークトラフィック技術および容量計画における効率の改善への作業負荷モデルを開発するための不可欠なステップである。ここでは、P2Pファイル共有ノードを識別するための、分類技術のアプリケーションについて記述する。

前述のように、我々の分析ではパケットヘッダからのみ抽出された識別値を使用する。ヘッダ情報のみを使用して、代替署名に基づくアプローチの収集および計算コストを減らし、トラフィックペイロードを検査することによって生じる可能性があるプライバシー関連の問題を回避する。

トラフィック量、パケットサイズ、保持される接続といった基準値に基づくトラフィック特性は、P2Pアプリケーションの適切な指標であることが多い。従来は、このような特性はネットワーク流に由来することが多かった。しかし最近のP2Pアプリケーションはウェブブラウジングや FTPファイル転送のような通常のネットワーク送信のように偽装することによって、本来の姿を隠す傾向にある。したがってフローレベルの統計は、通常のクライアントサーバタイプのアプリケーションに関連するフローからP2Pのフローを識別するための十分な情報を提供できない可能性がある。このケーススタディにおいて我々は、ノー

ドのステータス（すなわち固有の通信の特徴よりもP2Pファイル共有を行っているかどうか）に一層関心を持っている。P2Pネットワークの分散化された性質を更に適切にキャプチャするために、フローレベルを超えてホストレベルに行き、ホストレベルでは通信の全体像が即座に利用できる。これを行うために、対象ホストにつながるすべての通信を単一のストリームとして扱い、識別値は異なるホストから収集されたストリームに関して定義される。

トレースを収集するためにTBNANは、文献[10]にて紹介されたP2Pトラフィック作成システムに基づく仮想化に適応しており、これはキャプチャされたP2Pトレースへの安価なデータラベリングをサポートするものである。バックグラウンドトラフィックと最も一般的な2つのP2Pプロトコル、すなわちBitTorrent（世界で最も普及しているP2Pファイル共有プロトコル）と、PPLive（P2PTVとして知られる、新世代P2Pアプリケーションの代表的なプロトコル）の間で、分類が実行される。訓練とテストは、同じネットワーク環境で収集されるトレースデータに関して実行される。

最初の実験では、システムの一般化実行時の時間ウィンドウサイズ、wの影響を考察する。クライアントがP2Pノードであるかどうかを証明するには、このクライアントに関連するトラフィックが少なくともw秒間監視対象となる必要があり、これによって識別値はこの期間にキャプチャされたトレースに関して抽出される可能性がある。訓練および予測はこのような識別値に基づき作成される。この意味で、時間ウィンドウのサイズはシステムの応答パフォーマンスと密接に関連している。実験では、wは$\{1,2,4,8,16,32,64\}$秒から選択される。wの値が変化すると、テストセットに関する分類の正確さの変化が記録され、これが図2(a)に示されている。

図にあるように、wの増加に伴い、識別値における判別子情報が徐々に増加する。サンプリングレートが1の場合、すなわちすべてのキャプチャされたデータが特徴の抽出のために使用され、分類レートが95.56%（w=1s）から99.60%（w=64s）に増加する。サンプリングレート（以降、rパラメータで表す）を下げると、正確さがある程度低下する。それでもなお、すべてのケースにおいて、ウィンドウサイズが大きくなると正確さが向上する。w=64s、サンプリングレート1では正確さが99.53%に、サンプリングレートが1/8の場合は正確さが97.44%にそれぞれ達している。高速交換ネットワークを監視する際に、ネットワークトレースのサンプリングレートrが監視システムの拡張性を決定する別の重要なパラメータとなる。一般的には、費用対効果の大きいトラフィックデータ収集、ストレージおよび分析を目的とするサンプリングレートを減らすことが望ましい。実験の第2グループは、予測の正確さに関するサンプリングレートの影響を検証するために計画されている。これを行うには、最初に完全なサンプリングすな

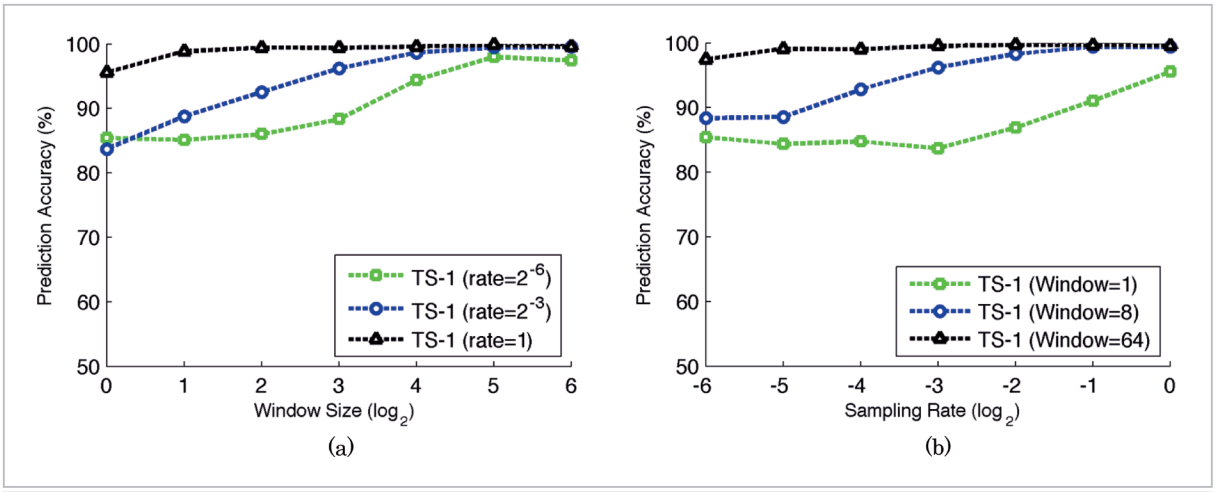


図2 予測の正確さ v.s. ウィンドウサイズ

わち $r=1$ を使用してトレースをキャプチャし、次に $\{1/64, 1/32, 1/16, 1/8, 1/4, 1/2, 1\}$ から選択した異なる r パラメータを使用して、副標本を抽出する。それから識別値を副標本のトレースから抽出し、訓練の分類器へ転送する。図 2 (b) ではテストセットに関してサンプリングレートに対する予測の正確さの曲線が示されている。この図は、図 2 (a) のものと類似している。この時点で、サンプリングレートの増加は予測の正確さの向上につながっている。$w=1$s の場合、正確さは $r=1/64$ にて 85.43% から開始し、$r=1/8$ では 83.71% の最小までわずかに減少し、$r=1$ では徐々に 95.56% まで増加している。$w=8$s の場合、正確さは $r=1/64$ での 88.34% から常に増加し、$r=1$ では 99.37% となる。$w=64$s の場合は、$r=1$ での開始点を除き、他のすべての r 値の正確性は 99.00% を上回っている。

概括すると、ウィンドウサイズおよびサンプリングレートに関する上記の実験では、計算リソースが豊富なほど、すなわち測定時間が長くおよび (または) サンプリングレートが高いほど、クライアントの動作を熟知することができ、あらゆるコンピュータ科学関連分野において一般的に経験されるように、この結果予測の正確さが高くなる。非常に重要な発見は、測定のウィンドウサイズの増加というプラスの影響が、サンプリングレートの減少というマイナスの影響を上回ることである。これによって識別の正確さの向上およびシステムパフォーマンス低下の緩和が提示される。ネットワークパフォーマンスへの影響を少なくするためにサンプリングレートをかなり小さくすることができるが、納得のいく一般化パフォーマンスが保証されるまでは、ウィンドウサイズを増加する。とりわけ、$w=64$s および $r=1/32$ は P2P ユーザの予測 (テストセットに関しては 99.04%) に関して適切な正確さをサポートするだけでなく、ネットワークリソースのコスト削減にも役立つ、適切なパラメータの組合せと思われる。

3.2 HMEB によるネットワーク攻撃の分類

ここではホストレベルでの分析からフローレベルでの分析に移ることによって、フローレベルのネットワークトラフィック分類に関するケーススタディとして、多重ラベルの侵入検出分類に関する階層化された最小密閉ボール (HMEB) [11] のアプリケーションを紹介する。

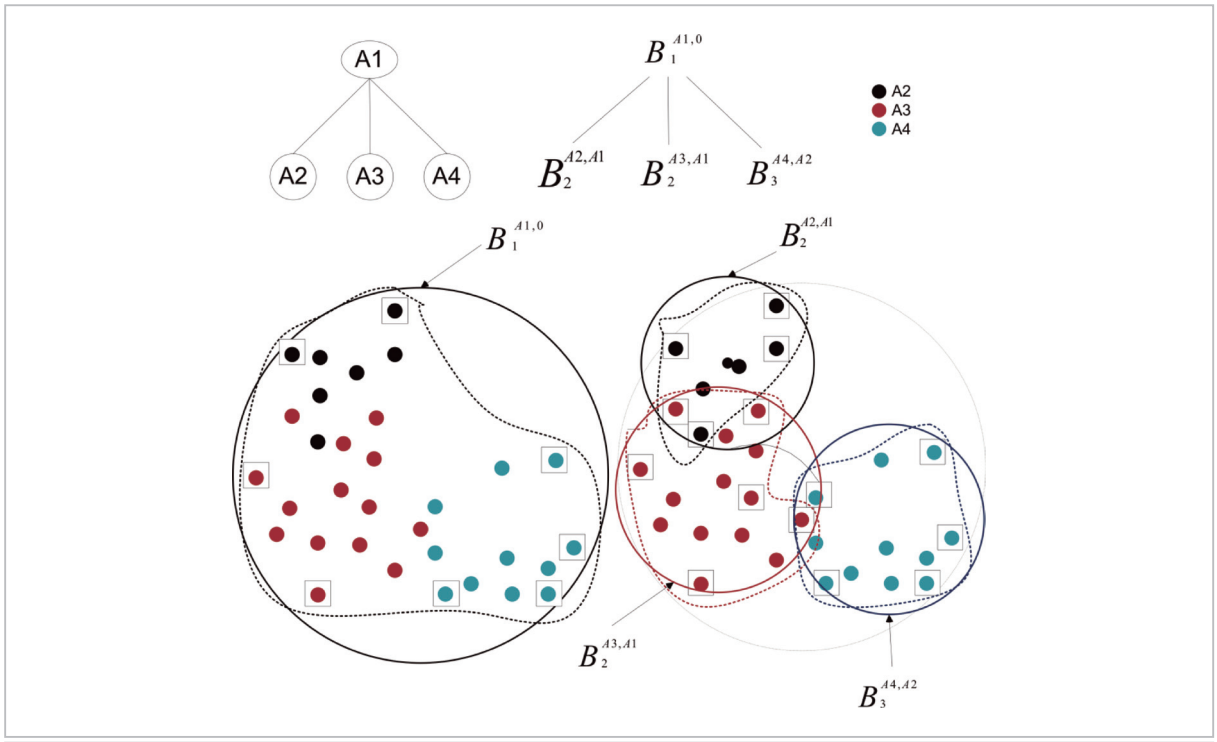


図 3 2D の例における HMEB 構造

HMEBの研究は、階層構造におけるように、ネットワーク侵入が多重ラベルに通常は関連するという事実によって触発されたものである。この結果、ネットワーク侵入の分類は通常、階層的多重ラベル分類（HMC）の問題を示す[12]。この問題では、すべてのインスタンスが複数のクラスに属している。従来の調査では一般的に、複数の主なクラスタへの排他的なグループネットワーク攻撃に焦点を当てている。これによって、侵入攻撃に関する重要な下位レベルの情報を逃しているために、検出の効率が下がる場合があった。

図3では、多重ラベル$A_1 \supset A_2, A_3, A_4$（すなわち$A_1$が$A_2$、$A_3$、$A_4$の親クラス）の2層の階層で組合せのデータセットに関するHMEBデータ概略の例を示している。HMEBは最小密閉ボール（MEBs）を構築し、これは、互いに分離するか、あるいは包囲する、木のような分類構造を形成する。ラベルのない例を想定する場合、HMEBはサンプルを囲むMEBをシークし、MEB階層におけるMEBの位置に応じてサンプルにラベルを付ける。

HMEBアルゴリズムを収集されたネットワークトレースに適用するには、フローレベルの識別値が抽出され、複数クラスに属するサンプルの一部またはすべてによって、正しいクラスラベルでラベル付けされる。次に、ラベルと共にサンプルがHMC問題として示され、HMEBによって解決される。他のメソッドと共にHMEBのパフォーマンスを評価するために我々は、この分野において広く使用されているベンチマークのKDD'99侵入検出データセットを使用する。

表1に見られるように、Bernhard（1999）は通常の接続タイプで99.5%という、分類の非常に高い正確さを実現した。ただし彼の分類器はU2RおよびR2Lに関しては不十分な分類パフォーマンスを示し、いずれも15%を上回らなかった。これは、これらの2つのクラスのサイズが他のクラスよりも非常に小さかったことによるものである。HMEBの全体的な分類の正確さが、通常の接続タイプおよびサービス妨害（DoS）タイプの攻撃に関するBernhardの手法のものよりもわずかに低いが、最も重要な2つのクラスの分類に関して、HMEBはBernhardの手法よりも優れている。特にHMEBでは、U2RとR2Lの分類の正確さがそれぞれ70%および35%増加している。この結果によってHMEBの優位が示されている。該当クラスのすべてのサンプルを包囲することによってHMEBは、偏りがあるクラスの場合でも、クラスの境界にて更に正確な近似値を可能とする。

要約としては、実験結果では、以前に発表されたベンチマーク作業よりもHMEBが大幅に向上していることが示されている。特にHMEBではKDD'99と比べて、U2Rの正確さが13.2%から

表1　Bernhardによる分類の正確さの比較（1999）

実績VS予測	実績（通常）	実績DOS	実績U2R	実績R2L	実績プローブ
Bern.予測（通常）	60262	5299	168	14527	511
HMEB予測（通常）	920431	36818	9845	2603	2084
Bern.予測DOS	78	223226	0	0	184
HMEB予測DOS	153064	3619301	10341	14732	85932
Bern.予測U2R	4	0	30	8	0
HMEB予測U2R	6	3	43	0	0
Bern.予測R2L	6	0	10	1360	0
HMEB予測R2L	321	193	44	517	0
Bern.予測プローブ	243	1328	20	294	3471
HMEB予測プローブ	2843	2104	412	506	35237
Bern.正確さの合計	99.5%	97.1%	13.2%	8.4%	83.3%
HMEB正確さの合計	94.6%	93.2%	82.7%	45.9%	85.7%

82.7%に、R2Lの正確さが8.4%から45.9%へと向上している。訓練データが大幅に増加しても計算時間が一定しているため、HMEBの結果が計算コストを削減することも、注目に値する。

3.3 異常値検出エンジン

TBNANに組み込まれている2番目のデータマイニングツールは、異常値検出エンジンである。TBNANは、異常なネットワークステータスの検出にOne Class SVMアルゴリズム（OCSVM）[13]を適用する。OCSVMアルゴリズムは最初に、高次元特徴空間（いわゆるカーネルトリック経由で）に入力データをマッピングし、2次の最適化問題の解決によって、起点から訓練データを最適に分割する最大周囲の超平面を検出する。カーネルによって誘導された特徴空間からマップバックされると、入力スペースのクラスタ境界に超平面が一致する。

図4は、該当するネットワークポートスキャンの異常ステータスを検出するために、TBNANで異常値検出を適用するケーススタディとして、監視されているストリームに（ホストレベルで）異常値検出が適用されている例を示している。この手法は、通常のネットワークストリームのモデルを構築し、監視されているストリームにおける通常モデルとのずれを検出し、これを異常ステータスとして予測する。このケーススタディでは、OCSVMは以下の2つの識別値に基づいている。単位時間枠に表示されたソースポート数（x軸）と、同じ時間のウィンドウに表示されたTCPフラグのタイプ（y軸）。図における閾値平面（平面の下は通常のトラフィック、平面の上はポートスキャンとなっている）によって示されている決定関数を基準として、ポートスキャン中に異常な箇所が検出可能である。

3.4 クラスタリング

TBNANにおける次の分析ツールは、クラスタリングエンジンである。クラスタリングは、スループットが大量のアクセスポイントにて継続的な監視をすることにより作成された大規模リポジトリを更に理解するための、トラフィックパターンの

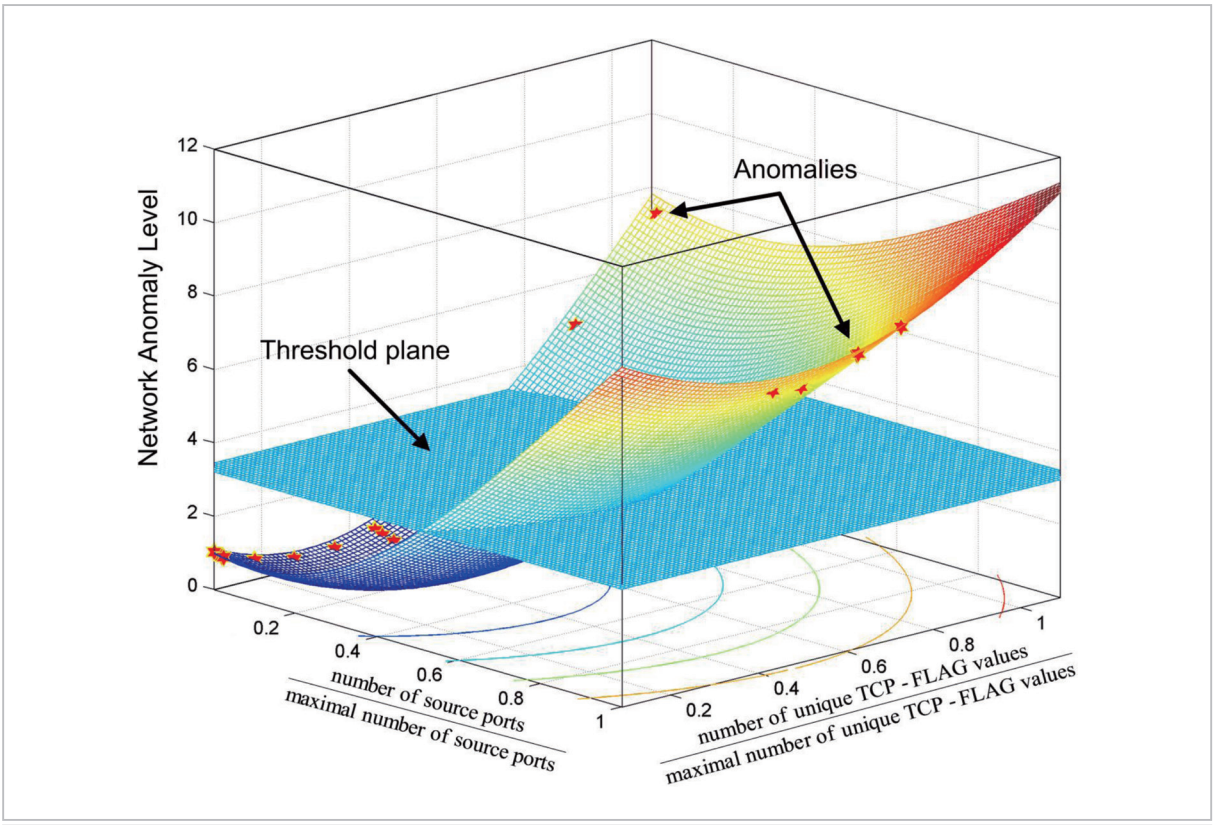


図4 OCSVMによるネットワーク異常ステータス検出

簡潔な表示に役立つ。資料によると、従来のクラスタリング技術である*K*平均法は、利点もあるが、実際のネットワークトレース分析に関するアプリケーションを妨げるという短所がある。特に*K*平均法における*K*の値、すなわちクラスタ数がヒューリスティックに決定され、これが一般的に検出の正確さに悪影響を及ぼす。以下では、*G*平均法[14]と呼ばれるヒューリスティックなクラスタリングアルゴリズムが侵入検出向けに提示されている。*G*平均法は、適切な*K*パラメータを選択するための前処理ステップとして記録密度ベースを使用するクラスタリング手法を使用しており、*K*平均法に関する前述の問題に対処している。

*G*平均法は、クラスタを構築するための訓練段階と侵入を検出するための検出段階という2つの段階に分けられる。訓練段階の最初のステップで、我々のケースでは効率の良さから採用した記録密度ベースのクラスタリングアルゴリズム（すなわちOPTICSアルゴリズム[15]）が、クラスタ配列および各サンプルのクラスタ構成といった情報を取得するための入力データに関して最初に実行される。次に、カーネルがクラスタの核においてデータポイントとなっている配列から、クラスタ数とカーネル構成要素が、抽出される。最後に、*K*平均法クラスタリングが前のステップからの従属的な情報と共に実行される。検出段階では、重心がクエリインスタンスに最も近いクラスタに、不明なデータを割り当てることによって侵入検出が実行される。

以下にて、KDD'99データセットから無作為にサンプリングされた100,000のサンプルの一部に関して、*G*平均法、*K*平均法およびOPTICSのパフォーマンスを評価する。*K*平均法は異なる*K*値にて実行される。比較結果は、表2に示されている。この表では、*G*平均法は3つのパラメータ設定に関して申し分ない結果を得たが、*K*平均法は最適な*K*を算出するために異なる*K*値で複数回の実行が必要であった。*G*平均法および*K*平均法の両方が、検出率およびフォールスポジティブ率に関してOPTICSよりも性能が優れていた。OPTICSの結果を綿密に検査したところ、検出率における不足は主にデータセットの区分が準最適であることによって生じ、結果として一部の訓練サンプルを認識せずにノイズと見なしたことがわかった

概括すると、この実験結果により*G*平均法は侵入検出に効果的であり、高い検出率と低いフォールスポジティブ率が出たことが示されている。また、データセットにおいてクラスタ数を自動的に示しクラスタ重心に対する適切な初期化を行うことにより、*G*平均法は*K*平均法よりも更に速くて良い最適条件で収束する。

4　結論

TBNANは、台頭するサイバー攻撃の脅威および起こり得るインシデントからネットワークを防衛するために、ネットワーク分析者によってツールとして使用可能な、一連のデータマイニングアルゴリズムリズムから構成されている。TBNANのさまざまな構成要素（前述のホストレベルおよびフローレベル分類エンジン、異常値検出に基づくスキャン検出エンジン、*G*平均法によるクラスタリングエンジンなど）では、ネットワーク上で発生したさまざまな攻撃および侵入を検出したり、ネットワークユーザおよびネットワークアプリケーションの動作の分析といった分析目的を容易にすることに役立つ。当論文に記述した分析エンジンに加え、監視されているネットワーク環境の性質を更に理解し、悪用とサイバー攻撃の脅威を防ぐために、現在では他の知的な統計分析ツールを積極的に組み込んでいるところである。

表2　検出率（DR）とフォールスポジティブ率（FPR）の比較

	*G*平均法			*K*平均法			OPTICS
#クラスタ	621	5	23	300	600	700	621
DR	99.12%	96.2579%	97.5292%	98.9820%	99.1953%	99.1166%	94.6456%
FPR	1.4107%	0.3264%	3.0951%	0.9001%	1.5054%	1.9213%	24.5815%

参考文献

1 Barbar, D. and Jajodia, S. (eds.), “Applications of Data Mining in Computer Security,” Kluwer, Dordrecht, 2002.

2 Chan, P. K. and Lippmann, R. P., “Machine learning for computer security,” Journal of Machine Learning Research, 7, pp. 2669–2672, 2006.

3 Maloof, M. (ed.): “Machine Learning and Data Mining for Computer Security,” Springer, Heidelberg, 2006.

4 Inoue, D., Yoshioka, K., Eto, M., Yamagata, M., Nishino, E., Takeuchi, J., Ohkouchi, K., and Nakao, K., “An Incident Analysis System NICTER and Its Analysis Engines Based on Data Mining Techniques,” LNCS, 2009, Vol. 5506, pp. 579–586, 2009.

5 Claffy, K., Braun, H. W., and Polyzos, G., “A Parametrizable Methodology for Internet Traffic Flow Profiling,” IEEE JSAC, 13(8): 1481–1494, 1995.

6 http://www.tcpdump.org/

7 Kriegel, H. P., Kroger, P., and Zimek, A., “Outlier Detection Techniques (Tutorial),” PAKDD, Bangkok, Thailand, 2009.

8 Chandola, V., Banerjee, A., and Kumar, V., “Anomaly Detection: A Survey,” ACM Computing Surveys, Vol. 41(3), Article 15, 2009.

9 http://www.ipoque.com/news & events/internet studies/internet

10 Ban, T., Ando, R., and Kadobayashi, Y., “Monitoring and Analysis of Network Traffic in P2P Environment,” Journal of the National Institute of Information and Communications Technology, Vol. 55, Nos. 2/3, 2008.

11 Chen, Y., Pang, S., Kasabov, N., Ban, T., and Kadobayashi, Y., “Hierarchical Core Vector Machines for Network Intrusion Detection,” ICONIP 2009, Part II, LNCS 5864, pp. 520–529, 2009.

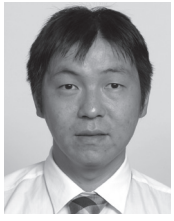
12 Boutell, M. R., “Learning multi-label scene classification,” Pattern Recognition, Vol. 37, No. 9, pp. 1757–1771, 2004.

13 Scholkopf, B., Platt, J., Shawe-Taylor, J., Smola, A., and Williamson, R., “Estimating the support of a high dimensional distribution,” Neural Computation, 13(7): 1443–1472, 2001.

14 Zhao, Z., Guo, S., Xu, Q., and Ban, T., “G-Means: A Clustering Algorithm for Intrusion Detection,” ICONIP 2008, Part I, LNCS 5506, pp. 563–570, 2009.

15 Mihael, A., Markus, M. B., Hans-Peter, K., and Jorg, S., “OPTICS: Ordering Points to Identify the Clustering Structure,” ACM SIGMOD 1999 International Conference on Management of Data, pp. 49–60. ACM Press, Philadelphia, 1999.

（平成23年6月15日 採録）



班　涛（Tao Ban）
ネットワークセキュリティ研究所
サイバーセキュリティ研究室専攻研究員　博士（工学）
サイバーセキュリティ、データマイニング

門林雄基（かどばやしゆうき）
ネットワークセキュリティ研究所
専攻研究員／
奈良先端科学技術大学院大学
情報科学研究科准教授　工学博士
IP トレースバック、サイバーセキュリティ