1A4-01

データマイニングとセキュリティ

Data Mining and Security

山西　健司
Kenji Yamanishi

NECインターネットシステム研究所
NEC Internet Systems Research Laboratories

In the area of network/computer security, novel data mining techniques such as anomaly detection have recently been recognized to be very important for cyber thereat analysis, network monitoring, open mission critical system realization, etc. They are complementary to conventional signature/policy-based approaches to the security issues, and are expected to lead a significant step toward realization of security intelligence. This paper surveys the latest trend of data mining techniques for security applications, specifically, focusing on anomaly detection, change-point detection, and anomolous behavior detection.

1. はじめに

ネットワークセキュリティの分野では、サイバーテロ対策を目的として、ネットワーク侵入検出の技術が重要性を増している。また、コンピュータセキュリティの分野では、なりすまし検出やシステムコールを用いた侵入検出の需要が高まってきている。さらに、ネットワークやWeb上の行動監視において不審行動や状況変化を検出する技術が要求されるようになってきた。こうした技術の多くは、データマイニングにおける異常検出、変化点検出、時系列マイニング、異常行動分析などといった技術と関連が深い。そこで本稿では、データマイニング技術とセキュリティの関わりについての最新動向を紹介する。

2. 署名ベース、ポリシーベース、異常検出

ネットワークセキュリティにおける、アクセスログからの侵入検出を考える。ネットワーク侵入検出技術には大きく分けて、署名ベース検出、ポリシーベース検出、異常検出の３種類がある。署名ベース検出は、既知の侵入/攻撃から定義ファイルを構成し、これとパタンマッチングを行なうことで侵入検出を行なう (例：[14])。しかし、この手法は、既知の侵入/攻撃を確定的に検出できるが、未知の侵入に対応できない。また、既知の侵入/攻撃の数だけパタンマッチングを行なう必要があり、計算量やメモリ量が膨大になるといった問題がある。

ポリシーベース検出は、一定のポリシーを設定して、これに反するアクセスを侵入と見なす方式である。この手法は、未知の侵入/攻撃も検出できる場合があるが、誤報率が多い、ポリシーを守る侵入が検出できない、といった問題がある。

異常検出は、データに基づいて通常のパタンを学習し、これから大きく外れるデータを検出してアラームを出すデータマイニングの手法である。まさに未知の侵入/攻撃の検出に適するが、ある程度誤報がでることは避けられない。学習が適応的であれば、未知の侵入も適応的に発見することができ、ポリシーベース検出よりも柔軟性をもつ。異常検出は、通常、署名ベース検出やポリシーベース検出と組み合わせて使われることが多い。

これらをまとめると以下の表のようになる。

連絡先: 山西健司，NECインターネットシステム研究所，216-8555 川崎市宮前区宮崎４－１－１，tel:044-856-2143, fax:044-856-2235，k-yamanishi@cw.jp.nec.com

	検出方法	確定性	備考
署名ベース検出	登録された特徴情報とパタンマッチング	確定的	登録されている侵入しか検知できない
ポリシーベース検出	ポリシーに反するデータを検出	確定的	ポリシーを満たす侵入は検出不可
異常検出	正常パタンと異なるデータを検出	確定/確率的	適応性あり未知侵入検知向け

表 1: 侵入検出技術の分類

3. 異常検出とネットワーク侵入検出

異常検出の実運用に際しては、以下の３点が要求される。１）オンラインでリアルタイムに処理されなければならない。２）ノイズに対してロバストであり、パタンの時間的変化に対して適応的でなければならない。３）「異常性」が統計的に意味のあるスコアに基いて判定されなければならない。

筆者らは統計的外れ値検出（図１参照）に基づく異常検出エンジンSmartSifterを提案し、上記３点を満足する侵入検出を実現してきた[10]。SmartSifterは以下の特徴をもつ。

A）ログ空間の確率密度関数を、カテゴリカル変数に関してはヒストグラムで、連続値変数に関してはガウス混合モデルで表現し、同時分布をそれらの直積で表す。

B) データを逐次的に取り込む毎にオンライン忘却型学習アルゴリズムでモデルを学習する。これは過去のデータほど影響を小さくすることでデータの非定常性に適応するものである。

C) 各データの異常値スコアを学習されたモデルに対する情報量として計算する。これにより高いスコアのもつデータの中に高い確率で実際の侵入を検出できることがKDDCup99[13]のベンチマークデータを用いて確かめられている[10]。

例えば、アパッチのセキュリティホールを狙ったBackとよばれるDos攻撃[13]は、サーバへの情報発信量が異常に多く、これらの発生を検出することができる。また、スキャニング行為や、CodeRedやSlammerなどのワームについても異常値として検出することが可能である。

さらに[11]では、SmartSifterが高いスコアを与えたデータを正例とし、低いスコアを与えたデータを負例として、これらを識別するルールを教師あり学習で求める方法を提案している。得られたルールは異常値パタンの特徴を捉えることができる。また、これを異常値フィルタリングルールとしてSmartSifterの前処理に用いることで、侵入検出の精度を有意

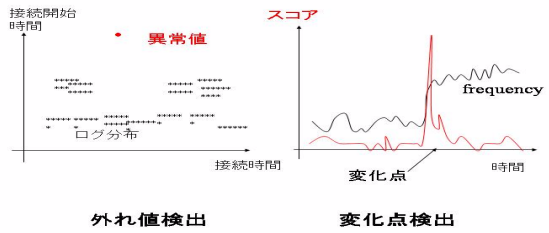

図 1: 外れ値検出と変化点検出

に高めることができることが報告されている [11]。

他にも異常検出の方法は、k-Nearest Neighbor などのクラスタリング手法、教師なし SVM などの機械学習手法や、マハラノビス距離などに基づく外れ値検出の方法などが適用され、その効果が実証されている（例; [4])。

4. 変化点検出と集中攻撃検出

実際の侵入/攻撃は単発で起こる場合よりは、むしろバースト的に発生する場合が多い。そこで、ログの時系列から変化点を検出することにより (図 1 参照)、バースト的に発生する攻撃や侵入の開始点を検出する手法が考えられる。

時系列の変化点を検出する方法は、時系列のセグメンテーションを行なう方法 [2], 一定ウインドウ内に属するログの外れ値度合いの大きさを調べる方法 [6] などが知られている。

また、筆者らは、時系列モデルの学習と異常検出を 2 段階で行なうことにより変化点検出を行なう手法を提案している [12]。具体的には、以下の手順で行なう。

A) 統計モデルとして AR モデルのような時系列モデルを SmartSifter と同様なオンライン忘却型学習アルゴリズムで学習して、異常値スコアを各データに対して計算する。

B) 一定サイズのウインドウ内のデータの異常値スコアの平均値を求め、移動平均スコアの時系列を新たに構成する。

C) 再度この時系列のモデルを学習し、異常値が出現する点を変化点として検出する。

例えば、なりまし ID を用いて TCP の中途半端な接続を大量に作ることを特徴とする SYN Flood とよばれる攻撃 [13] は、単位時間あたりの頻度が極めて高く、これらの集中発生を上記の変化点検出手法によって検出することができる。

5. 異常行動の検出

個々の異常値の検出ではなく異常行動のパタンを検出するデータマイニング技術もまた、セキュリティに応用されている。そのような応用例として、コマンド履歴を用いたなりすまし検出とシステムコール系列を用いた侵入検出を取り上げる。

5.1 コマンド履歴を用いたなりすまし検出

ユーザのコマンド履歴を用いたなりすまし検出では、先ずユーザのコマンド履歴の統計モデルを学習し、新しいコマンド履歴が入力されると、このモデルとなりすまし者のモデル（一様分布等が仮定される）の間で統計的検定を行なう方式が一般的に用いられている [7]。

コマンド履歴のモデルとして、マルコフモデルや、Naive Bayes モデル、データ圧縮モデル等が用いられているが、特に Naive Bayes モデルが Schonlau 等のベンチマーク [7] に対して、最も高い検出精度を達成することが報告されている [5]。

5.2 システムコール系列を用いた侵入検出

コンピュータの実行プログラムが内部で呼び出すシステムコール系列を用いて、トロイの木馬などの侵入を検出する試みがなされている。その際、システムコール系列のトレースから行動パタンのプロファイルを学習し、それから大きく異なるトレースを検出する方式が一般に用いられている。

その際、プロファイルを表現するモデルとして、マルコフモデル [1] や隠れマルコフモデル [8] が用いられている。また、*stide* や *t-stide* [3]、Teiresias[9] などといった行動パタンのマッチング手法も用いられている。

6. おわりに

データマイニングとセキュリティの関わりについて、特に異常検出技術、変化点検出技術、異常行動検出技術を中心に紹介してきた。近年、データマイニングの分野においてセキュリティ応用は一つの大きな流れを形成している。セキュリティ領域はビジネスチャンスであるばかりでなく、データマイニング技術や機械学習技術が試され、洗練されていくための格好の舞台として位置付けられていくだろう。

参考文献

[1] E.Eskin: Anomaly detection over noisy data using learned probability distributions, in *Proc. of ICML2000*, pp:255-262, 2000.

[2] V.Guralnik and J.Srivastava: Event detection from time series data, in *Proc. of KDD99*, pp:32-42, 1999.

[3] S. A. Hofmeyr, S. Forrest, and A. Somayaji: Intrusion detection using sequences of system calls, *Jounal of Computer Security*, 6:151-180, 1998.

[4] A.Leozarevic, L.Ertoz, A.Ozgur, J.Srivastava, and V.Kumar: A comparative study of anomaly detection scheme, in *Proc. of 3rd SIAM Conf. on Data Mining*, 2003.

[5] R.A.Maxion and T.N.Townsend: Masquerade detection using truncated command lines in *Proc. of Int. Conf. on Dependable Systems and Networks*, pp:219-228, 2002.

[6] V.Puttagunta and K.Kalpakis: Adaptive methods for activity monitoring of streaming data, in *Proc. of ICMLA '02*, pp:197-203, 2002.

[7] M.Schonlau, W.DuMouchel, W-H Ju, A.F.Karr, M.Theus, Y.Vardi: Computer Intrusion: Detecting masquerades, *Statistical Science*, 16(1), pp:58-74, 2001.

[8] C. Warrender, S. Forrest, B. Pearlmutter: Detecting intrusions using system calls: alternative data models, in *Proc. of the 1999 IEEE Symposium on Security and Privacy*, pp:133-145, 1999.

[9] A.Wespi, M.Dacier, and H.Debar: Intrusion detection using variable-length audit trail patterns, in *Proc. of RAID2000*, pp:110-129, 2000.

[10] K.Yamanishi, J.Takeuchi, G.Willams, and P.Milne: Online outlier detection using finite mixtures with discounting learning algorithms in *Proc. of KDD2000*, ACM Press, pp:320-324, 2000. A full version is to appear in *Data Mining and Knowledge Discovery Journal*.

[11] K.Yamanishi and J. Takeuchi, Discovering outlier filtering rules from unlabeled data, in *Proc. of KDD2001*, ACM Press, pp:389-394, 2001.

[12] K.Yamanishi and J.Takeuchi: A unifying framework for detecting outliers and change-points from non-stationary time series data, in *Proc. of KDD2002*, ACM Press, 2002.

[13] http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[14] http://www.snort.org