平成22年度 情報工学コース卒業研究報告要旨

高倉 研究室	氏　　名	鐘 揚
卒業研究題目	トラフィック変動に適応した 高速クラスタリングによる不正検知	

侵入検知システム (Intrusion Detection System:IDS) は増大するコンピュータネットワークへの脅威に対する防御策として大きな役割を果たしている．IDS には 2 種類の検知メカニズムがあり，一つはマルウェアや攻撃プログラムなどの特徴パターンを記述したシグネチャを基に攻撃を判別するミスユース検知であり，もう一つは正常トラフィックのパターンを学習し，そのパターンと異なれば攻撃と判別するアノマリ検知である．ミスユース検出では，存在を知られていない未知の攻撃をシグネチャで記述できないため，これを検知することが困難であるという問題がある．一方，アノマリ検知ではシグネチャを必要としないため導入のコストが少なく，また未知攻撃を検知することが可能である．しかし現状として，アノマリ検知では，正常トラフィックを厳密に定義することが難しいため誤検知が多く，まだ実験段階の手法と言える．

アノマリ検知手法として，すでに教師なし学習である K-means クラスタリング法に基づいた検知手法などが提案されているが，K-means 法の問題は初期クラスタ中心の生成及びその数によってクラスタリング結果が大きく変化し，検知性能が影響されるという問題がある．提案手法は，高次元空間を探索木構造のグリッドで分割し，分割された空間 (セル) を用いてクラスタ中心を決定する．さらに分割を各次元軸垂直方向に行い，要素の分布を的確に識別できる分割のみを採用することで，特徴量の数が多い場合でも計算量を抑えることが可能となる．図 1 に提案する分割法，図 2 に作成される中心の例を示す．攻撃の検知では攻撃モデルとして，少量のトラフィックによる侵入攻撃，および，サーバをダウンさせる，スキャンを目的とした大量トラフィック攻撃の 2 種類に注目し，空間に分布する要素の密度に基づいた検知メカニズムを提案する．

実ネットワーク環境で作成された京都大学ハニーポットネットワークのデータセット及び仮想環境で作成された KDD Cup 1999 のデータセットを用いて提案手法に対する評価を行った．実験結果ではハニーポットデータセットに対して誤検知率 2% ～ 5%，検知率 70% ～ 80% の高精度な検知が可能である．また，従来手法と比較して，提案手法ではより少数のクラスタで判定を行うため，判定に要する時間が半分以上に短縮され，汎用的な PC 環境を用いても 100Mbps 程度の流量に対応可能であることを示した．

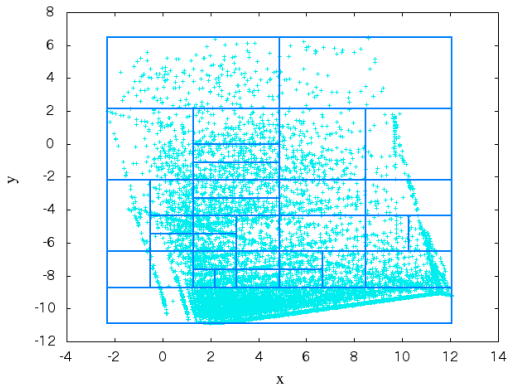

図 1：セル構築

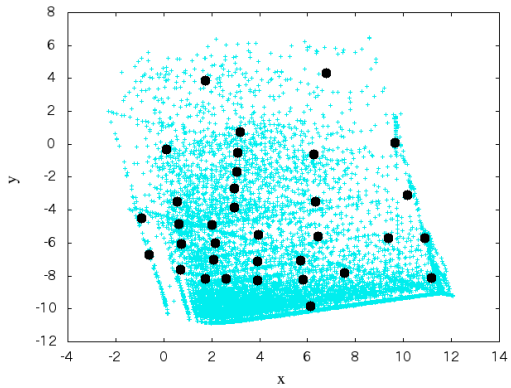

図 2：生成されたクラスタ中心