概　　要

異常型の侵入検出は、システム常態を述べる変量（観察対象）を基について、悪意まだ合法的な行動バターンを区別する。システム常態時々には限られる常態行動バターンのサンプルを述べられる、システムの本質は動態的（ユーザ・ドライバー）と共に段々複雑になって行くことを考えてない、だから、異常探知器時々過度の誤った警戒を発生する。本論文は、異常型の侵入検出のために有効的なモデル、方法と技術の開発を中心として論じる。これらのモデル、方法と技術の特徴は、適応性を主に条件として開発される。我々の研究は、３つの部分を含まれて、以下で詳しく述べます。

まず、最初の部分は動機つけ、異常探知器についての動く環境の基本的の了解は、このモデルの開発過程中にも基礎的不可欠な一つステップである。異常検出問題と誘導参照問題の類似性によって、私達は一つフレームワークを提出して、異常探知器の観察対象の角度から異常探知器の一般的行動を分析する。フレームワークを提出するの目的は、これからの具体的な異常探知器のモデルを作ると開発の理論的な基礎を作る。フレームワークを充実にするために、現在研究領域内のチャレンジ的な問題を調べて、解決方法を提出する。そのチャレンジ的な問題は、ホストベース、ネットワークベースの常態を述べる、異常探知器の品質評価などを含まれる。フレームワークは、ケーススタディーと数個典型的な異常探知器を比較と分析を含まれる。正式な方法を提供することによって、異常探知器の操作特性を了解、そして、異常探知器をもっと広く操作環境で使用される。

構築するのフレームワークを出発点として、ユーザーあるいはコンビュータ・システム本体によって起こるのシステム常態ドリフトを捕られるのために、私達は、３種類のＳＶＭベース探知器を開発される。この３種類の探知器は、3 種類改善されたサポートベクトルマシンを核心として検査方法を利用。この改善は、伝統的な仮定を破るの目的にした。伝統的な仮定は、異常探知器の訓練データ時々バッチで高品質的なデータを獲得する。私達の改善はこの異常探知器は定期的オンラインを訓練される、新しい検査環境に適応して、そして、過度な誤った警戒の発生を減少する。これらの異常探知器の性能を検証するために、私達は MIT のリンカーン研究室の 1998　DARPA BSM　データ集を利用して実験した、その同時にオリジナルのアルゴリズムを比較して分析した。実験の結果によって、新しい異常探知器は以下の方面でオリジナルの異常探知器より優れている：より少ないサポートベクトル、検出精密度を犠牲しないの同時により少ないトレーニングタイム。

最初部分の研究の観察と結論を基にして、数個異なる観察対象の異常探知器を関連するというもう一つフレームワークを提出する。私たちの望みは、特定の操作環境に基づく一つよりシンプルなグループ異常探知器お互いに協力して、より広い検出範囲でより少ない過度誤った警戒率の一般的なモデルを作られるということです。提出したフレームワークの実現のために、私たちは防衛ホストベース侵入異常(ADC)という自動検測コーディネータモデルを開発します。四つホストベースを基にするの異常探知器はお互いに関連して多エージェントの部分的に観察可能な Markov 決定プロセス（MPO－MDP）に形成します。モデルは一つ強化学習アルゴリズムの方針勾配を利用して、個々の異常探知器の行動パラメーターを調整して最適な協力方法を探す。コーディネータの行動は一つ報酬信号を設定によって変化している操作環境に適応する。私達は一つホストベースの実験環境を利用して提出するモデルを実現及び確かめる、実験結果（及びコーディネータと独立的な異常探知器の行動比較と分析）は提出したモデルの優位性を確かめる。

モデルを広がって基礎的フレームワークになってから、コンピュータのネットワークの多ステージ組織的攻撃をモデルに作る及び分析する。モデルから引き出されたの定義と特性（保護方の角度と攻撃方の角度から）は正式な方法を提供し防衛対策の開発に役に立て、このような攻撃を緩和また削除にする。防衛方と攻撃方の注目点は違うので、二つアルゴリズムを開発された、攻撃者からの非決定論の方法を探すアルゴリズム（ANTS）と、攻撃者からのビボット発見から遡って発見するアルゴリズム（ＡＰＤ―ＢＳ）である。前者の意義は、攻撃者のために最有効の競作性的な攻撃行動を探す、後者は防衛者のために侵入者最も意義を持てる攻撃（観察）対象を探す。