平成 25 年度卒業論文

論文題目

群知能の振る舞いを用いたセキュリティシステム

神奈川大学 工学部 電子情報フロンティア学科

学籍番号　201002684

小野　翔太郎

指導担当者　木下宏揚　教授

目 次

図 目 次

第1章　序論

1.1　背景

近年、アクセス制御や暗号技術などのコンピューターセキュリティの発達により、安全な通信をすることができている。
しかし、セキュリティ技術の発達は逆に言うと攻撃者の手口が進化してることを表している。特にDDoS攻撃に対しては発信源を特定することが難しく、各地で現段階も研究が続けられている。

まずDoS攻撃(Denial of Service attack)とは大量のパケットなどのリクエストを送信して、相手側の通信量を増大させて通信を処理している回線やサーバの処理能力（リソース）システムを使用困難にしたり、ダウンさせたり、過負荷によってサーバの機材そのものを誤動作させたり破壊したりして企業や政府機関などのサービスそのものを妨害することである。
そしてDDoS攻撃(Distributed Denial of Service attack)はDoS攻撃を行うホストがネットワーク上に分散している攻撃手法である。あらかじめ、攻撃者はセキュリティ対策をしていない各ホストコンピューターを乗っ取り、DoS攻撃をするコンピューターを大量に生成する。また乗っ取った際に攻撃する時間を設定をすることで同時刻に一斉に対象を攻撃することが可能となる。
そのため、攻撃を受けたホストはどこから攻撃されてるのかがわからない上に乗っ取った真の攻撃者の特定が非常に困難である。

これらの対策としてIDS(Intrusion Detection System)やIPS(Intrusion Prevention System)の開発されている。これらのシステムはDoS攻撃やウイルス攻撃などの様々の攻撃を検知したり、加えて通信も遮断するものもある。
検知の仕方として、普段のトラフィック（通信量）と比較して攻撃を検知するアノマリー型と予め設定したパケットの特徴に基づいて攻撃を検知するシグネチャ型がある。しかしこれらにも欠点があり、検知の仕方によっては未知の攻撃に対応できなかったり、通常の通信接続に対しても誤って検知してしまう場合もあり、検知システム自体に余計な負荷が掛ってしまう。

そのための研究として、先程述べたアノマリー型とシグネチャ型を組み合わせた検知を使った研究[1]やIDS自体に機械学習の一種である遺伝的アルゴリズムやSVMを用いて学習機能を持たせることによって未知の攻撃を防ぐ研究がされている。[2][3] [2]の研究では[3]の研究より良い検出結果が出ている。
しかし、あくまでHTTPとTCPのみの実験結果であり、他のプロトコルでの実

験は行っていない。

また TCP/IP のトランスポート層で用いられる UDP は同じ階層の TCP と同じくらい最も使われるプロトコルであるが、TCP の輻輳制御やウィンドウサイズ制御などといったパケット制御はなく、オーバヘッドもかからないため、攻撃者の手間が少なく、攻撃者にとって都合がいいプロトコルである。　そこで本研究では生き物の群れの振る舞いに着目して遺伝的アルゴリズムで用いる新たな評価関数を作っていき、各プロトコルの中で DoS 攻撃が多発している UDP において遺伝的アルゴリズムを用いた学習機能と SVM を用いた学習機能を比較していき、遺伝的アルゴリズムの有用性を証明していく。さらには LEGOMindStorms に遺伝的アルゴリズムを入れることで本研究の可視化を実現していく。

1.2　問題点

DoS 攻撃対策に用いられる IDS や IPS は検知の仕方によって、検知機能が左右されるという欠点がある。そのため学習機能を持たせてパケットの特徴を学習させることで、いかに未知の攻撃の対処や誤検出を防ぐかが課題となっている。

1.3　研究の目的

本研究の目的としては遺伝的アルゴリズムを用いて、その振る舞いによって通常のパケットと DoS 攻撃のパケットを分けて効率的な IDS の学習をするための評価関数を作っていき、LEGOMindStorms に遺伝的アルゴリズムを入れることで本研究の可視化を実現していく。

第2章　基礎知識

2.1　群知能

群知能とは生き物の群れみたいに個々の簡単なやり取りを通じて、集団として高度な動きを見せる現象（振る舞い）を用いた計算手法のことである。

2.1.1　遺伝的アルゴリズム

遺伝的アルゴリズム [9] とは自然界の生物のように環境に適応出来なかったものが絶滅し、自然淘汰されるようにシステムの中でこの考えを取り入れ、評価関数によって染色体それぞれに評価度を点け、その評価度に基づき染色体の一部を交叉、淘汰、突然変異を繰り返すことで最適解をさがす計算手法である。遺伝的アルゴリズムにおける染色体は遺伝子の集まりであり、遺伝子とはある問題に対する解の候補 (データ) である。

- 交叉：染色体同士を交配させて親に似た染色体を作る。

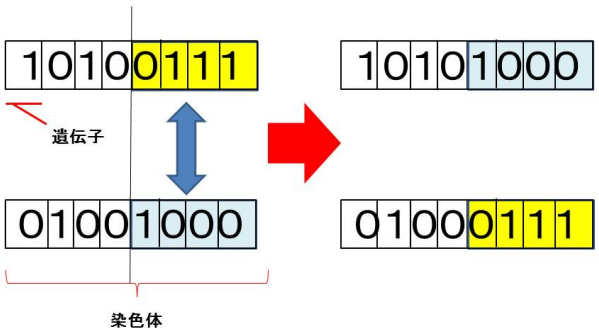

図 2.1: 遺伝的アルゴリズム：交叉の例

- 淘汰：染色体そのものを消去する。

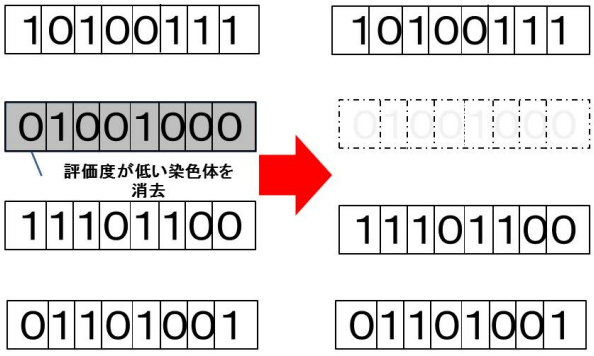

図 2.2: 遺伝的アルゴリズム：淘汰の例

- 突然変異：染色体の中身を変える。

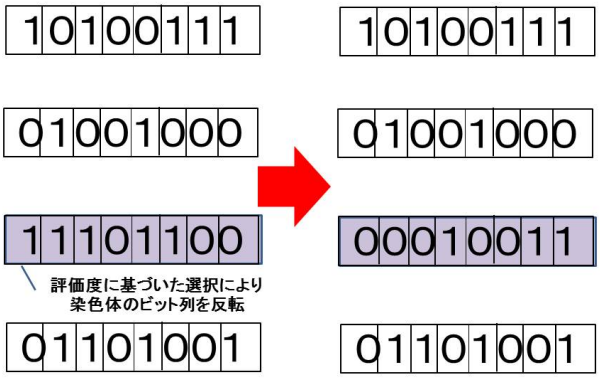

図 2.3: 遺伝的アルゴリズム：突然変異の例

遺伝的アルゴリズムを使う利点としては比較的優れた解を求めるのに時間効率が良いのとどの問題に対しても適用できることなどがある。　ただし遺伝的アルゴリズムは全ての問題に対して、適用できるような一般的な方法がなく、解く問題によっては評価度の付け方が変わったり、親を選択する際の選択法が変わったり、交叉・淘汰・突然変異の仕方が変わってきたりと色々異なってくる。そのため遺伝的アルゴリズムは一般的な方法を見つけるため様々な手法が研究・提案されている。

2.2 SVM(Sapport Vector Machine)

サポートベクターマシン [2] とは，1995 年に，ATT の V.Vapnik によって統計的学習理論の枠組みで提案された学習機械のことである．SVM は，特にパターン認識の能力において，最も優秀な学習モデルの 1 つである。仕組みとしては数多くある入力データを二つに分類して学習する手法である。特徴としては学習したデータの最大マージンの中間に線引きをして新たなデータの誤学習を防ぎ未知のデータに対しても対応することができる。

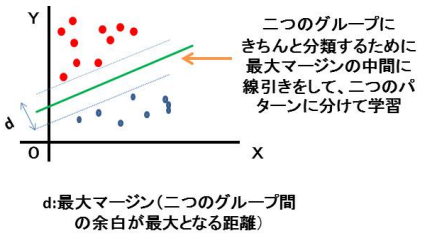

図 2.4: SVM の例

2.3 LEGOMindStorms

Mindstorms[10] とは，ブロックで有名なデンマークの LEGO 社の LEGO ブロックを，プログラミングを用いて作るロボットのキットのことであり 12 歳以上の児童向けになっているだけあり，容易にロボットの組み立てからプログラミン

グまでを行うことができる.

今回は2006年10月から発売になったLEGOMindStormsNXTを使用する。NXTは様々なファームウェア（LEGOのような機械に入れるOS）を入れることができ、今回はleJOSというファームウェアを使用する。またプログラム言語はJavaを用いる。

図 2.5: LEGOMindstormsの組み立て例 [11] より引用

2.4 TCP/IP参照モデル

TCP/IP(別名：インターネット・プロトコル・スイート)[4][5]とは現在、最も普及している通信プロトコルの一式である。通信プロトコルとはインターネットにつなげる際に接続先との通信に信頼性を持たせるために作られた通信規約である。

現在では通信プロトコルの一式に合わせてＯＳやハードウェアなども作られて、さらにどのインターネットも通信プロトコル一式に従って構築されている。TCP/IPは４つの階層に分かれていて各層はそれぞれの役割を果たす。

- 第４層アプリケーション層：接続に対する送信要求やそれに対する応答を行ったり、またはソフトウェアの動作を保障するための規約。

- 第３層トランスポート層：データの転送の制御をする。
- 第２層インターネット層：IP アドレスの割り当て、データの伝送経路の選択（ルーティングという）などを主に司る。
- 第１層リンク層：文字列や数字などのデータを電気信号に変え電気信号の転送の制御をする。

各層のプロトコルはそれぞれ数種類あり、基本的にはメールやウェブなどに用いる、HTTP や SMTP などのアプリケーション層に属するどのプロトコルを使うかによって下位層のプロトコルも決まってくる。また上位層（数字が大きい層）に近いほど下位層（数字が小さい層）の通信制御に影響される。

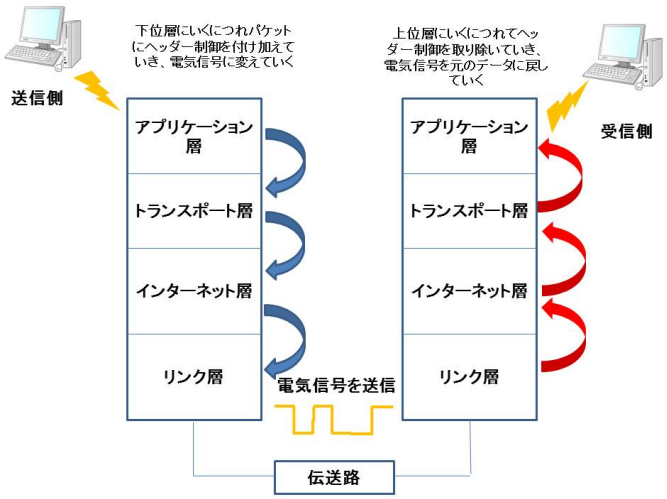

図 2.6: TCP/IP 参照モデルの仕組み

2.4.1 UDP(User Datagram Protocol)

TCP/IP 参照モデルの第３層に属するプロトコルでデータの転送を制御するプロトコルの一つである。
UDP は TCP と同じようにデータ転送によく用いられるプロトコルだが TCP とは違う点は一対一の通信路を作成しないことやデータの欠落があっても再送要求をしない点である。
UDP は通信の信頼性はないが TCP よりも通信速度が速いので、主に音声や画像などに用いられる。

2.5 DoS 攻撃

DoS 攻撃 [4][5][6] とは大量のパケットやリクエストを送りつけたり、またはバグ等を利用して誤作動などで負荷を重くし、企業や政府機関などの提供するサービスを妨害したり、停止させる攻撃を指し、様々な攻撃手法がある。
その中でも最近多いのが DDoS 攻撃である。DoS 攻撃は攻撃側と相手側の 1 対 1 で行われる。しかし、DDoS は攻撃側が複数存在し、1 台のサーバに攻撃を仕掛ける。
たとえば、1,000 台が 1 台のサーバを攻撃を仕掛けたとする。DDoS の防御が難しい点は、この 1,000 台がどこにあるのか見当がつかない点である。そして、真の攻撃者を特定することは非常に難しい。
DDoS 攻撃は、踏み台となるホストが必要であるため、まずインターネット上にあるサーバに侵入し、DDoS のモジュールを埋め込む。特に、インターネット上でサービスを提供するサーバは、時刻の同期が行われていることが多いため、DDoS のモジュールに対し、何日の何時何分にどのホストを攻撃するのか設定を行っておく。
これによって設定した日時に指定されたホストを一斉に攻撃することができる。また攻撃の指令を出したホストは IP アドレスを偽装して他のコンピューターを乗っ取ってるのでたとえ攻撃したホストを特定したとしても攻撃の指令元を特定することはできない。
そのため現在の対策としては一番多く用いられる DoS 攻撃の手法をあらかじめ予測して対策をしている。

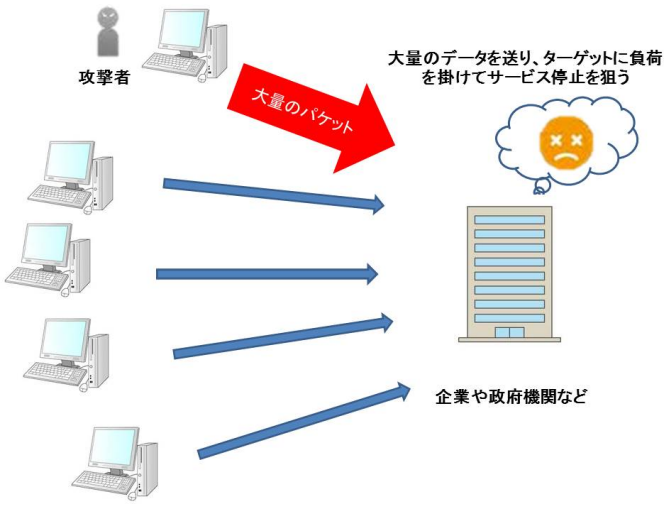

図 2.7: DoS 攻撃の仕組み

2.5.1 UDPflood 攻撃

DoS 攻撃の一種であり、トランスポート層における UDP で絶大なサイズのパケットを送ったり、少量のサイズのパケットを DDoS 攻撃と組み合わせて一斉に送りつけたりして、ターゲットとなったサーバやファイヤウォールの負荷をかけて機能を著しく落としたり、または停止させてしまう。

UDP はコネクションレス型で TCP みたいに様々なパケット制御によってオーバヘッドが掛からない上に、攻撃者側の手間が掛からないことから主に攻撃するプロトコルの一つである。

2.6 IDS(Intrusion Detection System)

DoS 攻撃やウイルス攻撃などの対策の一環として開発されたシステムがこの IDS[1][4][5] である。IDS は予めの設定に基づいて各階層のパケットの中身を確認し、攻撃を検知した時にネットワーク管理者に警告をだすシステムである。
ファイヤーウォールが IP アドレスやポート番号でパケットをフィルタリングするのに対し、IDS は全プロトコルのデータを確認、検知することができる。
検知の仕方は 2 種類あり、それぞれは一長一短である。

- アノマリー型：
  予め”正常な通信”の定義をして、定義に当てはまらないようなパケットが来た時に警告を通知する方式である。ここでいう”正常な通信”とは個々が行うサービスによって変わってくる。長所として、”正常な通信”を定義するので一回設定しまえば、あとは余程のことがない限り設定しなおす必要がない。逆に短所は IDS における”正常な通信”の前提は不変なものとして扱ってることから例え本来なら正常なパケットでも定義から外れていると誤って検知してしまうことである。

- シグネチャ型：
  予め攻撃パケットの特徴を定義して, その定義に当てはまったパケットが来た時に警告を通知する方式である。長所としては攻撃パケットの特徴から検知するのでアノマリー型ほど誤検知が多くなくて済む。しかし逆に短所として未知の攻撃に弱く、攻撃パケットの特徴を定期的に更新する必要がある。

これらの検知方式の短所をなくすために両方の検知方式を合した研究や機械学習機能を組み合わせた研究などがされている。
また IDS が検知しかしないため、通信接続の遮断などをするときは管理者が手動で行わなければいけなかったがそれを解決するために IPS[4][5](Intrusion Prevention System) が開発された。

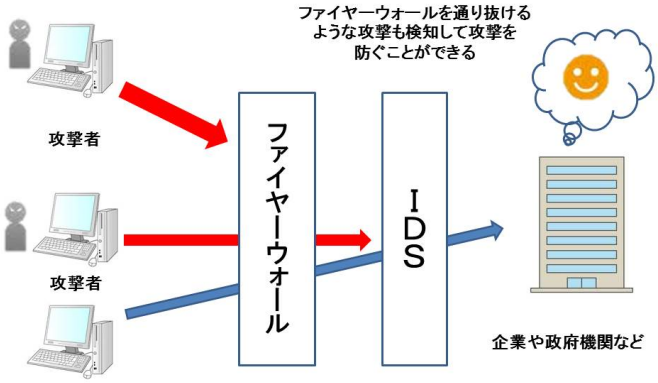
ファイヤーウォールを通り抜ける
ような攻撃も検知して攻撃を
防ぐことができる
攻撃者
攻撃者
ファイヤーウォール
IDS
企業や政府機関など

図 2.8: IDS の仕組み

第3章　提案

3.1　提案システム

参考文献

[1] 宮澤僚太、阿部公輝：”攻撃履歴を利用したシグネチャ型 IDS の DoS 耐性の向上”、電気通信大学情報工学科 2008

[2] 中野　孝彦：サポートベクターマシンを利用した不正侵入検出について、三重大学大学院工学研究科博士前期課程情報工学専攻、2012

[3] 森仁美，中野孝彦，太田義勝，鈴木秀智:“遺伝的アルゴリズムを利用した不正侵入検出について”,2010 年度電気関係学会東海支部連合大会 (D2-5)，2010.8.30.

[4] ITpro：http://itpro.nikkeibp.co.jp/

[5] atmarkIT：http://www.atmarkit.co.jp/index.html

[6] ”DDoS 攻撃の防御対策について”, 警察庁技術対策課サイバーテロ対策技術室、平成１５年６月３日

[7] 金久保　正明：静岡理工科大学総合情報学部人間情報デザイン学科・知能インタラクション研究室ホームページ
http://www.sist.ac.jp/ kanakubo/research/swarm$_i$*ntelligence.html*

[8] 村上　研二、一色　正晴、　木下　浩二：愛媛大学村上研究室ホームページ、http://ipr20.cs.ehime-u.ac.jp/index.html

[9] Dimple Juneja、Neha Arora:”An Ant Based Framework for Preventing DDoS Attack in Wireless Sensor Networks”、International Journal of Advancements in Technology http://ijict.org/ ISSN 0976-4860(2010)

[10] LEGOMindstorms　ホームページ：http://www.lego.com/ja-jp/mindstorms/?domainredir=mindstorms.lego.com

[11] ROBOHiTec ホームページ：http://www.robohitec.com/en/robot-kits-/11-lego-mindstorms-education-nxt-base-set.html