L-7 ネットワークベース侵入検知システムの性能評価
－高負荷時における性能低下と適用条件－
Performance evaluation of a network base intrusion detection system on a high load network

平石 陽太 Youta Hiraishi
宮内 充 Mituru Miyauchi

1．背景

商用の侵入検知システムは非常に高価でありエンドユーザーや SOHO のような比較的小規模なネットワークでは、フリーの IDS を使用せざるを得ない。本実験ではパケットキャプチャライブラリを使用して実装された、軽量なフリーのネットワークベース侵入検知システムである Snort を用い、侵入検知システムの実装を行う為の指標として追随可能な転送容量を調べ、適用条件を求めた。

2．侵入検知システムの性能評価

侵入検知システムの性能を評価する指標の一つとして処理容量が挙げられる。現行の侵入検知システムの多くはネットワークを流れるパケットをプロミスキャスモードによってキャプチャし入力情報とするネットワークベース侵入検知システムであり、その処理容量は追随可能な転送容量である[1]。一般に高い処理負荷はペイロードよりもプロトコルの解析によるといわれ、秒間のパケット数(p/s)が多いほど検出精度は低下すると言われている[2]。商用、非商用に関わらず、侵入検知システムはその性質上フォールスネガティブは許されない。よって、そのネットワーク上で流れる可能性のあるトラフィック全てを処理できるだけの能力が侵入検知システムには必要である。

3．実験

図 1 は実験の構成である。実験では Client から Server へトラフィックを発生させ、この攻撃を IDS により解析した。各コンピュータは 100Mb/s の Ethernet で接続されている。上記構成でパケットの送信間隔と種類を変動させ IDS の検知精度及び 1 パケットあたりの検知時間の変動を求めた。間隔を制御した通信にはクライアントサーバー型の自作トラフィックジェネレータを用い、Snort のバージョンは 1.8.6 を、パケットキャプチャライブラリには、libpcap0.7.1 を使用した。また、今回の実験では評価基準として 100%の検知精度を期待できる場合のみを「十分な検知精度」と位置付けた。表 1 は実験に用いたトラフィックの構成表である。以後の説明は表 1 の番号を用いて行う。

4．実験結果及び考察

実験 1～4 を行った結果、基本的に秒間のパケット数が増加すると 1 パケットあたりの処理時間が増加する事がわかった。Celeron500MHz の CPU における通常トラフィックの 1 パケットあたりの処理時間は秒間送信パケット数が 1000 パケットの時、約 80～100μs であり、秒間送信パケット数が 5000 パケットの時、90～120μs であった。実験 1、2 よりペイロードのサイズによって 50μs 程度の差異が生じたが、通常のトラフィックにおいてパケットの処理落ちは発生しなかった。下図 2 は実験 3 において、5 万個のパケットを送った場合の各パケットに対する処理時間である。

実験 3 では、秒間送信パケット数が 2000 を超えた点からパケットの処理落ちが発生した。また、通常トラフィックよりも攻撃トラフィックの方が 400～800μs 多くかかることが図よりわかる。また、実験 3 では、トラフィックに TCP を用いていた為実際の処理には ack パケットも含まれるが、図 2 の処理回数には ack パケットの処理は含んでいない。図 2 の検知精度は秒間送信パケット数が増えるに従って低下し、秒間送信パケット数 2000 において、62%、3000 で 39%、4000 で 27%、5000 で 26%であった。しかし、ack パケットのロス率は、攻撃パケットの処理率の低下よりも約 10 倍近くと、非常に大きい値となった。これは、ack パケット自体の処理には攻撃パケットの半分以下の処理時間しかかからないものの、攻撃パケットの処理中に ack がネットワーク上を流れているためだと考えられる。この為、ネットワーク上に流れたパケット全体の処理率は、上記グラフよりも大幅に低下する。また、この結果より処理時間のかかるトラフィックを利用した侵入検知システムに対する新しい形の DoS 攻撃が可能であると考えられる。

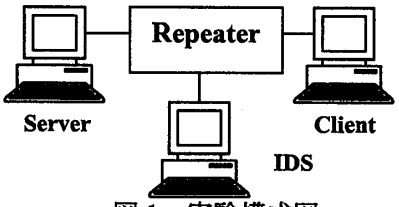

図 1 実験構成図

表 1 実験に用いたトラフィックの種類

実験番号	種類	備考
実験 1	通常トラフィック	TCP 1000byte
実験 2		TCP 73byte
実験 3	攻撃トラフィック	TCP
実験 4		UDP

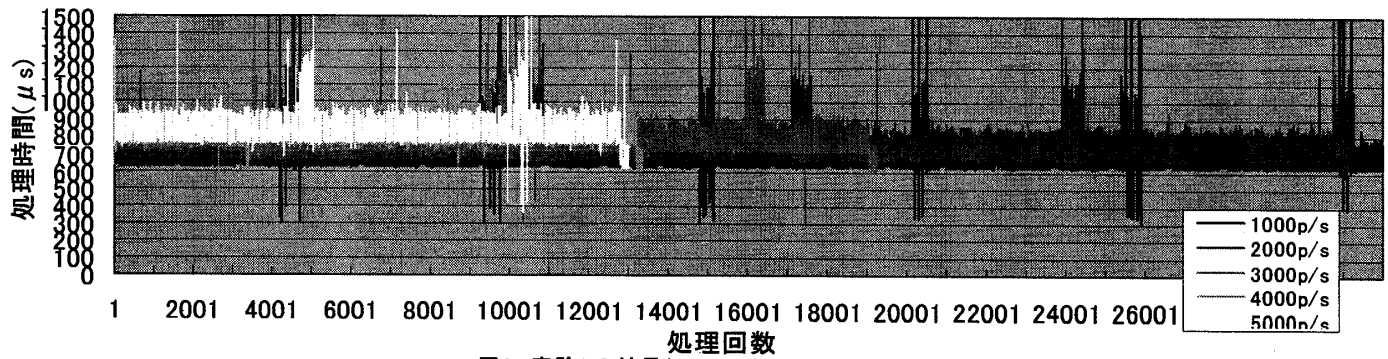

図2 実験3の結果(CPU:Celeron500MHz)

右下の図3は実験4におけるCPU別検知精度である。図3に示されている理論値は、実験結果から求めた秒間パケット処理量の推移を表す以下の式1を元にした値である。

$$y = \frac{a}{x} + b \cdots\cdots\cdots\cdots (1)$$

(y:検知精度、x:秒間送信パケット数、a, b:ハードウェア固有の定数)

式1は非常に単純な反比例の式であるが、図3より実験結果に非常に近似している事がわかる。この式を用いる事により異なったハードウェアを用いても検知精度が低下する点を2ヵ所計測すれば、ハードウェア構成の秒間パケット処理量の上限を求める事ができる。実験4はUDPを用いたトラフィックの為、TCPトラフィックに比べヘッダ構造が単純であることから、TCPで同じ通信を行った場合に比べ300～400μs程度1パケットあたりの処理速度が速くなり、それに伴い、検知精度も向上している。

次に、検知精度低下の要因を実験結果より考えると、パケットが処理落ちし検知精度の低下が始まった時、CPUの使用率は常に99%以上の高い値となった。つまり、パケットの解析に処理能力を費やすため、パケットをキャプチャできなくなっていることがわかった。反対に物理メモリ量に関しては128Mbyte程度あれば十分であり、ネットワークが高負荷でもスワップする事無く侵入検知システムを動作させられる事がわかった。

CPU性能が高速ならば短期的にはより高速のネットワークに対応できるが、秒間1000回程度の攻撃でも、30分程攻撃を続けるとログファイルのサイズが500Mbyte以上と非常に大きくなる。図4に示されるようにログファイルのサイズが非常に大きくなっても多少の揺らぎはあるもののほとんど検知精度は変化しない。しかし、ログファイルの肥大化によりハードディスクの容量が圧迫された場合は当然攻撃を検知できなくなる。この事から、ログファイルを記録するパーティションは必ずシステムが存在するパーティションと分け、可能な限り多くの領域を割り当てることが望ましい。また、ログファイルのサイズは処理速度にはほとんど影響しないので、検知精度を優先しログのローテートはなるべく頻度を抑え、トラフィックが集中していない時に行うなど、極力控えるべきである。

5．まとめ

今回の実験で使用したトラフィック量は常識的に起こり得ない量の攻撃であるが、IDSに対するDoS攻撃ツールを用いた場合、表2からわかるように、現在の広帯域常時接続環境は十分IDSに対するDoS攻撃となり得る通信を行える事がわかる。また、図3でパケットの処理落ちが発生していない1000p/sにおいて、1パケットあたりの処理時間の最大値800μsを考えると、1000000[μs]/800[μs]=1250となり、パケットのキャプチャにかかるCPU時間を無視すれば秒間1250パケット処理できる事になる。この秒間1250パケットという処理能力は実測値とほぼ等しいことから、パケットのキャプチャによる処理時間は極めて小さく、無視できる値であることがわかる。また、小さいパケットで負荷を発生させた場合、送信ホストはより大量のパケットを発生させる事ができる為、悪意のあるユーザーにより大量のパケットを送信されると回線負荷が10Mb/s以下でも検知精度が大きく低下する。バースト的な攻撃が日常的に発生するとは考え難く、このような攻撃を想定しない場合100Mb/sの回線において、それほど性能の高くないCeleron500MHz程度のCPUでも十分な検知精度を得られることがわかった。しかし、現実的には流れ得る危険なトラフィックが存在する以上そのことを考慮に入れてIDSを運用するハードウェアを選定するべきである。

表2　実験3、4における回線負荷

秒間送信パケット数	トラフィック量
1000 p/s	0.6Mb/s
2000 p/s	1.2Mb/s
3000 p/s	1.8Mb/s
4000 p/s	2.3Mb/s
5000 p/s	2.9Mb/s

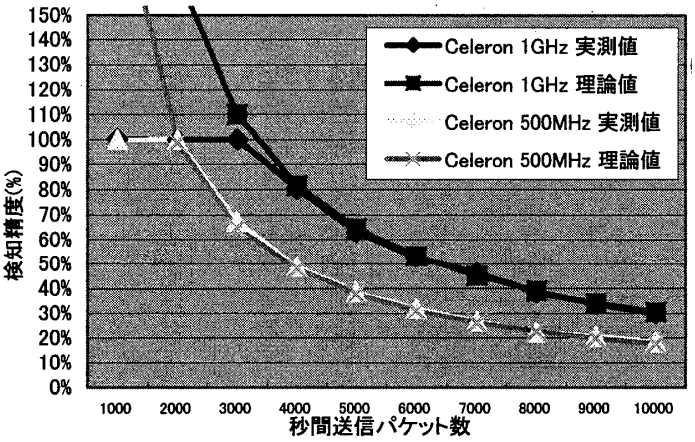

図3　CPU別検知精度の推移と理論値(UDP)

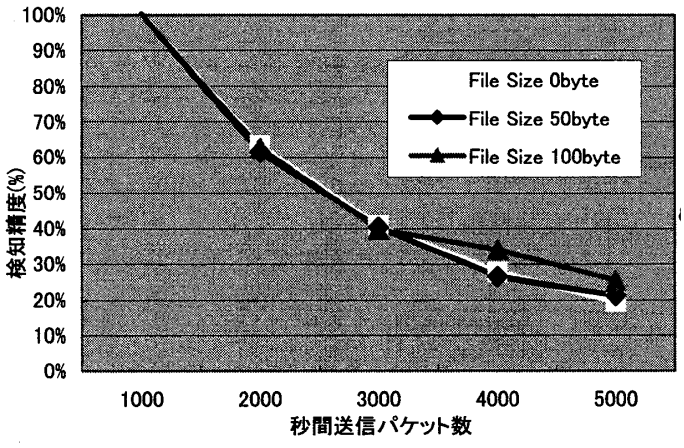

図4　ログファイルのサイズによる検知精度の変化

参考文献

[1] 武井 洋介、他:"ﾄﾗﾋｯｸﾊﾟﾀｰﾝを用いた不正ｱｸｾｽ検出及び追跡方式" 電子情報通信学会論文誌B Vol.J84-B, No8(2001-8)

[2] S.Northcutt, 他: "ﾈｯﾄﾜｰｸ不正侵入検知" 翔泳社(2001-11)