PN 符号を利用した観測点検出攻撃のノイズ耐性向上に関する一考察

成田 匡輝 †　　ベッド バハドゥール ビスタ †　　高田 豊雄 †

† 岩手県立大学 ソフトウェア情報学研究科
020-0193 岩手県岩手郡滝沢村滝沢字巣子 152 番地 52

g236j201@s.iwate-pu.ac.jp, {bbb, takata}@iwate-pu.ac.jp

あらまし インターネット上で発生している攻撃の動向を早期に把握するため，インターネット観測システムの研究・開発が行われている．その一方で，攻撃者が観測システムに捕捉されずに攻撃を行うための，観測点の配置位置を事前に検出する観測点検出攻撃が知られている．PN 符号を利用した最新の観測点検出攻撃では，従来手法よりも少量の偵察パケットで観測点の検出が可能であるが，通常の観測パケットが強力なノイズとなった場合に観測点検出性能は低下する．本稿では，今後攻撃者がノイズ耐性を高めるため，1 観測点の検出に複数ポートを利用した攻撃の改良を行うことを想定し，その攻撃手法の考案とシミュレーションによる観測点検出性能を示す．

A Study on Improving Noise Tolerance of PN Code-Based Localization Attacks to Internet Threat Monitors

Masaki Narita†　　Bhed Bahadur Bista†　　Toyoo Takata†

†Iwate Prefectural University, Graduate School of Software and Information Science
152-52 Sugo, Takizawa, Iwate 020-0193 Japan

g236j201@s.iwate-pu.ac.jp, {bbb, takata}@iwate-pu.ac.jp

Abstract Internet threat monitoring systems are studied and developed to comprehend the malicious activities on the Internet. On the other hand, attackers devise a technique that locates sensors' position to evade sensors when they launch attacks. The latest PN code-based method enables attackers to detect sensors with low scanning traffic volume. However, detection accuracy decreases when other monitoring packets interfere as strong noise. Thus, we predict attackers improve noise tolerance of the existing method by exploiting multiple ports for detecting a sensor. In this paper, we devise such method and demonstrate the detection performance via simulation results.

1　はじめに

近年，インターネットの利用はあらゆる世代に浸透し，利用目的の公私を問わず，欠くことのできないものとなった．しかし，悪意を持ったインターネット利用者もまた激増しており，個人情報を収集するマルウェアの出現，特定組織に対するサービス拒否攻撃のように，インターネットは常に悪意を持った活動に晒されている．

こうした背景から，インターネット上で発生している攻撃の動向を早期に把握するため，インターネット観測システムの研究･開発が行われている．インターネット観測システムは，観測点と呼ばれる計算機をインターネット上の広域に配置し，到着するパケットを観測する．そし

て各観測点から収集したパケットを解析し，得られた観測結果をインターネット上の脅威から身を守るために有益な情報として一般公開する．

一方，攻撃者がインターネット観測システムの観測点の配置状況を事前に検出し，観測点を迂回しながら攻撃を行うための，観測点検出攻撃が知られている．最新の観測点検出攻撃では，スペクトラム拡散通信の考え方に基づく PN (Pseudo Noise) 符号を利用しており，従来の観測点検出攻撃と比較して少量の偵察パケットで観測点の検出が可能となっている．しかし，少量の偵察パケットで攻撃が可能な反面，他の通常の観測パケットが偵察パケットへの強力なノイズとなった場合，観測点の検出性能は低下する．

そこで我々は，今後攻撃者がノイズ耐性を高めるため，観測点検出攻撃の改良を行うことを想定し，その具体的な攻撃手法を考案した．本稿では，考案した攻撃手法を実際に稼働中のインターネット観測システムで取得された観測データに適用し，観測点検出性能について議論する．

2　インターネット観測システム

現在，国内外で多くのインターネット観測システムが稼働している．国内の例では，警察庁が運用する@police [1]，NICT が運用する nicter [2]，JPCERT/CC が運用する ISDAS [3]，国外の例では，多国間で観測点の情報を共有する WOMBAT [4]，世界中の有志の協力によって観測網を構築する DShield [5] 等が知られている．

2.1　インターネット観測システムの概要

インターネット観測システムは，その観測方法，観測点の配置，観測結果の公開様式等，様々な観点から分類が可能である．しかし，(1) 観測点によるパケットの観測，(2) 観測パケットの集計，(3) 観測結果の公開という 3 つの機能は，どのシステムにも共通する．図 1 に上記 3 つの機能を表したインターネット観測システムの概要を示す．

観測点は通常，インターネット上の広域に配置される．インターネットに直接接続されたホストには，マルウェアによる攻撃パケット等，悪意を持って送出されたパケットが頻繁に到着し

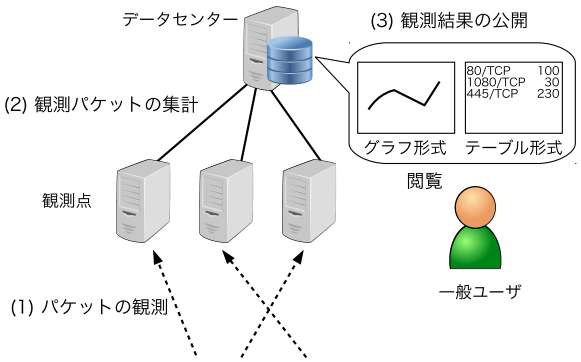

図 1: インターネット観測システムの概要

ている．観測点はこれら到着する攻撃パケットを観測し，観測ログに保存する．

次に，各観測点で保存された観測ログは中央のデータセンターに集積される．集積された観測ログは解析され，例えばパケットが到着したポート番号毎に集計される．

そして，インターネット上の脅威から身を守るために有益な情報として，観測結果は一般公開される．観測結果の公開様式は，観測パケット数の時間推移を表したグラフ形式，単位時間に到着したパケット数を提示するテーブル形式等，観測システムを運用する組織の裁量に委ねられる．

2.2　インターネット観測システムへの攻撃

近年，攻撃者がインターネット上に配置された観測点を検出する，観測点検出攻撃が問題となっている．インターネット観測システムが，最新の攻撃動向の把握という目的を果たすためには，観測点の配置は外部から隠蔽されていなければならない．なぜなら観測点が攻撃者によって検出されてしまった場合，観測点が迂回されてしまうためである．観測点が迂回されれば，仮に新たな手口の攻撃活動がインターネット上で行われていても，その攻撃パケットの観測が困難になる．

さらに，観測点の配置の外部への露呈で，攻撃者が観測点に攻撃パケットを含む任意のパケットを送出することも可能となる．これにより，観測システムは正しい観測結果に基づく情報の公開が困難となる．

こうした理由から，観測点検出攻撃に対する防御手法，あるいは観測点検出攻撃の性能評価に関する研究は急務といえる．本稿では，後者の観測点検出攻撃の性能評価に焦点を当てる．

3　関連研究

観測点検出攻撃は，篠田ら [6]，Bethencourt ら [7] によって初めて明らかにされた．彼らの検出手法では，観測点の存在が疑われるネットワークに対し，一時的に大量の偵察パケットを予め送出する．そして，後にインターネット観測システムが一般公開する観測結果に，予め送出した偵察パケットが含まれるか否かで当該ネットワーク内の観測点の存在を判定する．

しかしこれらの手法は，大量の偵察パケットの送出を必要とした．そのため，インターネット観測システムの運用組織による攻撃検出が比較的容易であり，統計的アプローチによる対策手法が提案された [8]．

その後，Yu らによって秘匿性を高めた観測点検出攻撃が考案された [9, 10]．この手法では，観測点検出のための偵察パケットを，PN 符号の値に合わせて送出することで，観測点の検出が以前の手法に比べ少量の偵察パケットで可能になっている．しかし，送出する偵察パケットが少量であるがゆえに，他の観測パケットが偵察パケットへの強力なノイズとなった場合，観測点の検出性能は低下する．そこで今後攻撃者は，この攻撃手法のノイズ耐性を高めると考えられる．次節では，[9] で述べられた観測点検出攻撃の概略を示した後，この手法のノイズ耐性を高めるための，我々が考案した手法について述べる．

4　観測点検出攻撃

4.1　既存手法

[9] で述べられた観測点検出攻撃は，2 つの Step で構成される．図 2，図 3 で示した例を基に，各 Step の概要を述べる．

Step1　攻撃者はまず，観測点の存在が疑われるネットワーク (図 2:ネットワーク A) に，特定ポートへのポートスキャンとしての偵察パケットを送出する．このとき偵察パケットは，攻撃者が事前に用意した PN 符号の値に合わせて送出される．PN 符号による偵察トラフィックの生成方法については，4.1.1 で述べる．

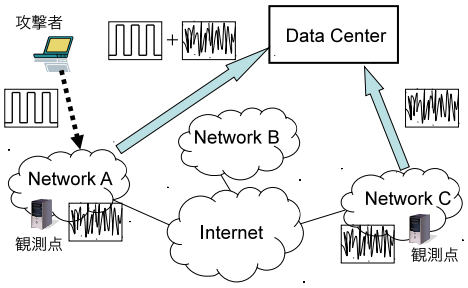

図 2: Step1 (偵察トラフィックの送出)

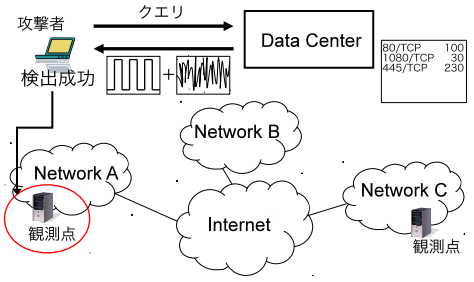

図 3: Step2 (偵察結果の確認)

Step2　攻撃者はその後，善良なユーザを装い，観測システムの運用組織によって一般公開される観測結果にアクセスする．そして攻撃者は，一定の時間間隔で集計・更新される観測パケット数を参照し，自身が偵察に利用したポートで観測されたパケット数と Step1 で利用した PN 符号との相関値を算出する．攻撃者は，この値が事前に決定した観測点の存在判定の閾値を上回る時，ネットワーク A に観測点が存在すると判断する．

4.1.1　偵察トラフィックの生成方法

偵察トラフィックの生成に利用する PN 符号は，+1 と −1 の 2 値がランダムに出現する矩形波であり，長さ L のベクトル $\boldsymbol{C}$ として表現される ($\boldsymbol{C} = \langle C_1, C_2, ..., C_L \rangle \in \{-1, +1\}^L$)．この符号は他のノイズに親和する一方，同じ符号語間でのみ高い相関を示す．そのため，PN 符

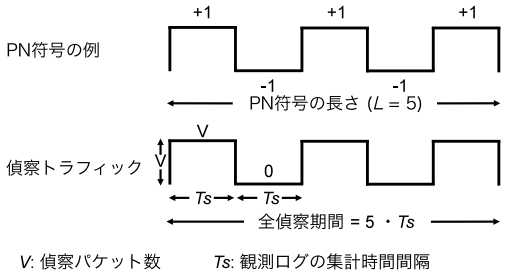

図 4: PN 符号と偵察トラフィックの生成

号を偵察パケットの送出に利用することで，他の観測パケットの中に偵察パケットを隠蔽しつつ観測点の検出が可能となる．PN 符号は通常，線形帰還シフトレジスタ等により生成する．

インターネット観測システムがデータセンターで観測ログを集計する時間間隔を T_s とした時，攻撃者は，各 T_s 毎に偵察パケットの送出，あるいは送出の一時停止のいずれかを行う．図 4 は，PN 符号の例 ($L = 5$) とそれに対応した偵察トラフィックの生成例を示している．攻撃者は，PN 符号の値が $+1$ の T_s では，必要な偵察パケット数 (V) を送出する．一方，PN 符号の値が -1 の T_s では，偵察パケットの送出は一時停止する．T_s の値は観測システムの仕様で決定され，L と V の値は，必要とする観測点の検出精度によって攻撃者が決定する．

4.1.2 相関値の算出方法

インターネット観測システムが一定の時間間隔で公開する，特定ポートで観測されたパケット数と，偵察トラフィックに利用した PN 符号との相関値 (Γ) は以下の式により算出する．

$$\Gamma(\boldsymbol{C}, \boldsymbol{\lambda'}) = \frac{\Sigma_{i=1}^{L} C_i \lambda'_i}{L}$$

ここで $\boldsymbol{\lambda'}$ は，偵察に利用したポートに一定の時間間隔で到着したパケット数をベクトル $\boldsymbol{\lambda} = \langle \lambda_1, \lambda_2, ..., \lambda_L \rangle$ で表した時，$\boldsymbol{\lambda}$ の各成分から $\boldsymbol{\lambda}$ の各成分の平均値を減算して得られたベクトルである．また，$\boldsymbol{C}$ は攻撃者が偵察に利用した PN 符号のベクトルである．

この相関値 (Γ) が事前に決定した観測点の存在判定の閾値を上回る時，攻撃者は偵察対象のネットワークに観測点が存在すると判断する．

4.2 ノイズ耐性向上手法

4.1 で示した既存手法は，PN 符号の利用により，初期の手法 [6, 7] と比較して偵察トラフィックを削減できる手法として考案された．しかし，この手法は観測点検出攻撃に無関係なパケットが偵察トラフィックへの強力なノイズとなった場合，検出性能が低下する手法となっており，その対策が講じられていない．

そこで我々は，4.1 で示した既存手法のノイズ耐性向上手法を考案した．対策対象のノイズは，短期間に特定のポートに大量のパケットが到着するスパイク型のノイズと特定ポートでトラフィック流量の変化が起こり，長期間に渡って到着パケット数が増加するノイズである．

4.2.1 スパイク型のノイズへの対策

まず，スパイク型のノイズへの対策について述べる．4.1.2 で示した相関値 (Γ) の算出式が示す通り，インターネット観測システムにより一般公開された観測結果に，1 つでも強力なスパイク型のノイズが含まれた場合，相関値はそのノイズの影響を大きく受けてしまう．

そこでスパイク型のノイズへの対策としては，相関値の算出を行う前に，そのノイズの除去を行う．具体的には，スパイク型のノイズを，その観測システムにおける平常時の観測パケット数からの外れ値と考える．そして，外れ値が観測された期間を相関値の算出から除外する．この時，相関値の算出から除外した期間の分だけ L の値は短縮される．外れ値の検定には，スミルノフ・グラブス検定を有意水準 1%で用いることとした．図 5 は，スパイク型のノイズの除去の一例である．この例では，スパイク型のノイズが発生した 2 期間を相関値の算出から除外し，本来の $L = 16$ を $L = 14$ とみなして相関値を算出する．

4.2.2 トラフィック流量の変化によるノイズへの対策

次に特定ポートでトラフィック流量の変化が起こり，長期間に渡って到着パケット数が増加

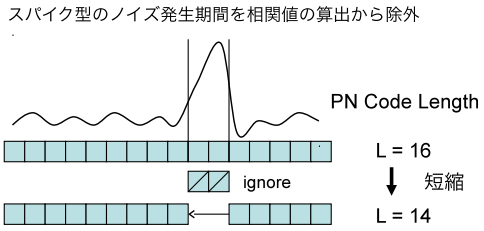

図 5: スパイク型のノイズの除去

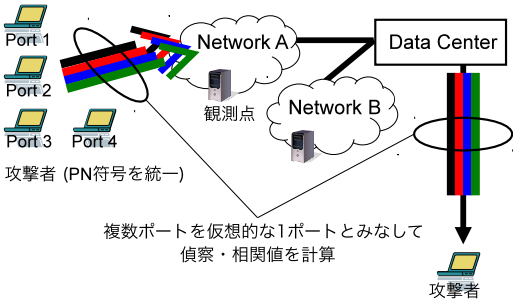

図 6: 複数ポートを仮想 1 ポートとみなした偵察

するノイズへの対策について述べる．このノイズに偵察トラフィックが埋没してしまった場合，正しい相関値を算出することが困難となる．そこでこのノイズに対しては，1 観測点の偵察に 1 ポートを利用するのではなく，複数ポートを利用することでノイズ耐性を高める．複数ポートを偵察に利用するため，我々は以下の 2 つの手法を考案した．

偵察経路の冗長化　1 つ目の手法は，偵察経路の完全なる冗長化である．1 観測点の偵察を行うため，偵察トラフィックを 3 ポート以上の奇数ポートに対して送出する．その後，偵察に利用した各ポートで相関値の算出を従来通り行い，観測点の存在判定の閾値を上回るポートが全体の過半数を占めた時，攻撃者は観測点が存在すると判断する．この手法は，高いノイズ耐性を実現できると考えられる反面，送出する偵察トラフィック量も増加してしまうことから，観測システムの運用組織が偵察トラフィックを検出できる可能性も高まると考えられる．

複数ポートを 1 ポートとみなしての偵察　2 つ目の手法は，複数ポート (n) を束ねて仮想的な 1 ポートとみなし，偵察に複数ポートを利用する手法である (図 6)．送出する偵察トラフィック量は，仮想ポート全体のトラフィック流量を基に決定し，各ポートに偵察トラフィックを振り分ける．即ちこの手法は，複数ポートの利用による，各ポートへ送出する偵察トラフィック量の削減とノイズ耐性向上の両立を目的とする．

相関値の算出方法は，まず従来通り各ポートで相関値を算出する．この時，各ポートへ送出した偵察トラフィック量は正規化し，それぞれの相関値 Γ_{Port_i} を得る．その後，相関値を全て加算し，合計の相関値 (Γ_{sum}) が既定の閾値を上回る時，攻撃者は偵察対象のネットワークに観測点が存在すると判断する．

$$\Gamma_{sum} = \Sigma_{i=1}^{n} \Gamma_{Port_i}$$

図 6 の例では，4 ポートを仮想 1 ポートとみなし，偵察を行っている．

5　性能評価

5.1　評価実験の目的

既存研究 [9] で示された PN 符号を利用した観測点検出攻撃の検出性能は，主に理論的な枠組みの中での性能である．つまり，事前予測が困難かつ検出性能へ大きな影響を及ぼすほどのノイズ (観測点検出攻撃に無関係な観測パケット) の混入といった，現実の状況を踏まえた性能評価によるものとはいえない．

そこで本稿では，現実に即したノイズの発生状況を想定した上で，攻撃者が既存の PN 符号を利用した観測点検出攻撃のノイズ耐性を向上させるため，前節で示した複数ポートを利用した偵察を行った際の検出性能について評価した．

比較を行う観測点検出攻撃は，(1) 単独ポートのみを利用する手法，(2) 複数ポートを利用して偵察経路を冗長化する手法，(3) 複数ポートを仮想 1 ポートとみなす手法の 3 手法である．4.2.1 で述べたスパイク型のノイズへの対策は，予め上記の 3 手法に適用することとした．これは予備実験で，スパイク型のノイズへの対策が全体的に有効に作用したためである．つまり本稿で

表 1: 実験パラメータ

トラフィック流量確認期間	48 時間
偵察利用ポート数 (n)	5
偵察パケット数 (V)	1.0σ
PN 符号の長さ (L)	64
観測ログの集計時間間隔 (T_s)	4 時間

は，スパイク型のノイズへの対策を施した上で，複数ポートを偵察に利用することが，ノイズ耐性向上にどの程度有効であるかを評価した．

検出性能は，偵察対象に観測点が存在する場合の観測点検出率 (True Positive Rate)，観測点が存在しない場合の誤検出率 (False Positive Rate) で評価した．また，偵察トラフィックの秘匿性評価の観点から，観測システムの運用組織が，トラフィック流量の統計的異常に基づき発生させうるアラート回数も検証した．

5.2 実験内容と実験パラメータ

我々が性能評価のために行った実験は，あるネットワークに対し，攻撃者が偵察トラフィックを送出し，観測点の存在判定を行う状況を想定したシミュレーションである．実験は全て，必要な機能を実装した単一の計算機上で行った．そのため，実際にインターネット上で偵察行為は行わず，JPCERT/CC が実運用中の観測システムで取得した，2011 年の実観測データに偵察トラフィックを適用することで検証した．

主な実験パラメータを表 1 に示す．表中のトラフィック流量確認期間とは，攻撃者が偵察トラフィックを送出する前に，攻撃する観測システムの観測動向を調査し，偵察計画を立てるための期間である．この期間に攻撃者は，偵察に利用するポートの選定を行う．本実験では，各ポートをトラフィック流量で降順にソートし，パケットが継続的に到着しているポートの中から，トラフィック流量の変動が少ない上位 5 ポートを偵察に利用した．本稿で述べた観測点検出攻撃の性質上，トラフィック流量が多く，その変動が少ないポートを選定することが，偵察の秘匿性と検出性能に有利となるためである．偵察パケット数 (V) は，偵察に利用するポートにおけるトラフィック流量の変動の標準偏差 (σ) を基に決定する．

観測点の存在判定の閾値は，ノイズとなる観測パケットの到着はガウス分布に基づくと仮定して導出された既存研究 [9] の攻撃パラメータ決定のための定理に $L = 64$，$V = 1.0\sigma$ を適用し，理論上の観測点検出率が 99.18%，誤検出率が 5.47%となるよう設定した．また，実観測データ (1 年分) は，毎月 1 日午前 0 時開始の月別観測データとして 12 分割し，それぞれに偵察トラフィックを適用した．

いずれの実験においても，攻撃者が使用する PN 符号を変化させて 1 万回の試行を行い，3 種類の観測点検出攻撃を比較した．

5.3 実験結果と考察

観測点検出率　まず，偵察対象のネットワークに，観測点が存在した場合の観測点検出率 (True Positive Rate) について述べる (図 7 左)．グラフの横軸は，比較する 3 手法を適用する 2011 年の月別観測データに対応しており，縦軸は観測点検出率である．単独ポートのみを利用する手法 (Single Port) による評価結果は，5 ポートそれぞれを単独で偵察に利用した場合の平均検出率であり，5 ポートを単独で利用することによる，検出率の変動幅も示している．

この評価結果では，偵察経路を冗長化する手法 (Multi Ports (Redundancy)) が非常に高い観測点検出率を示している．いずれの月に取得された観測データへこの手法を適用したとしても，ほぼノイズの影響を受けることなく観測点検出が可能であった．一方，単独ポートのみを利用する手法の平均検出率と複数ポートを仮想 1 ポートとみなす手法 (Multi Ports (Virtual One Port)) の検出率では，どちらの手法も 8〜9 割程度の検出率を示したが，後者の手法が全体的にやや低い結果となった．しかし，単独ポートのみを利用する手法は，非常に高い検出率を示す場合もある反面，強力なノイズが混入した場合に，検出率が著しく低下しているのが分かる．そのため，複数ポートを仮想 1 ポートとみなす手法は，こうした検出率の著しい低下を抑制し

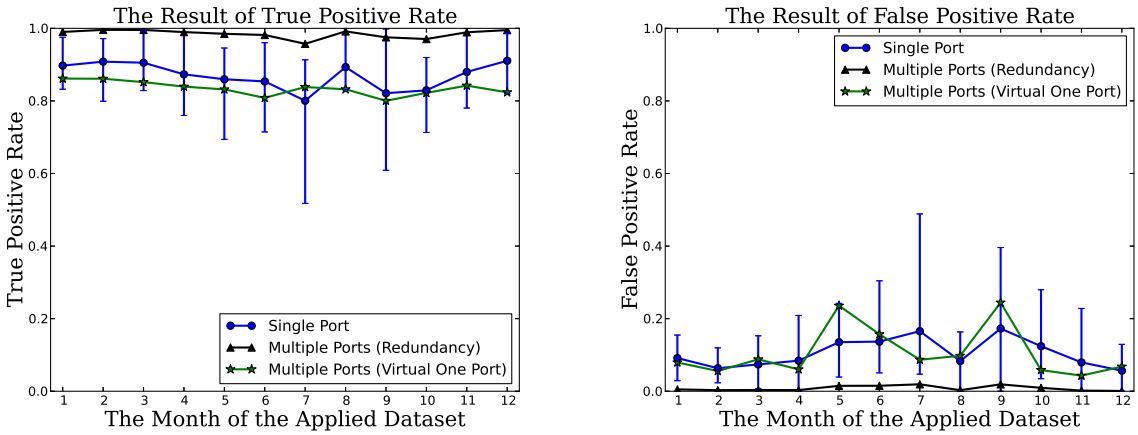

図 7: 比較する 3 手法を月別観測データに適用した際の観測点検出率 (左)，観測点誤検出率 (右)

たい際に有効であると考えられる．

観測点誤検出率　次に，偵察対象のネットワークに，観測点が存在しなかった場合の観測点誤検出率 (False Positive Rate) について述べる (図 7 右)．このグラフは，縦軸に観測点誤検出率を示している．横軸，凡例は観測点検出率のグラフと同様である．

この評価結果においても，偵察経路を冗長化する手法は際立って高い性能を示し，いずれの観測データに適用した場合でも非常に低い誤検出率となった．一方，単独ポートのみを利用する手法の平均誤検出率と複数ポートを仮想 1 ポートとみなす手法の評価結果は，どちらも偵察経路を冗長化する手法には劣り，1〜2 割程度の誤検出が発生している．しかし，観測点検出率の結果とは若干異なり，単独ポートのみを利用する手法の平均誤検出率が，複数ポートを仮想 1 ポートとみなす手法に比べて，必ずしも高い性能を示していない．また，単独ポートのみを利用する手法は，ノイズ混入の影響による誤検出率の大幅な変動を避けることができない．複数ポートを仮想 1 ポートとみなす手法は，こうした著しい誤検出率の増加を抑制できるといえる．

観測システム側による偵察の検知　最後に，比較する 3 手法の秘匿性に関する評価結果を示す．観測点検出攻撃による偵察トラフィックを直接的に検知する手法は，未だ確立されておらず，その検知は専ら観測パケット数の統計的異常値に基づいて行われる．

そこで本稿でも，攻撃者が偵察に利用するポートにおいて，偵察トラフィックが含まれていない状態のトラフィック量とその変動の標準偏差 (σ) をそのポートの平常時のプロファイルとして異常値の判定に使用する．そして観測ログの各集計時間間隔に，偵察に利用したポートに到着したパケット数が 3σ の値を超えた場合，観測点検出攻撃の発生とみなし，アラートが発生するものとする．つまり，発生アラート数が少ないほど秘匿性が高い偵察手法となる．

図 8 の各グラフは，比較する 3 手法それぞれの評価結果である．横軸は 2011 年の月別観測データ，縦軸は発生アラート数である．発生アラートは，実験の偵察トラフィックにより発生したものだけを集計し，無関係なトラフィックにより発生したアラートは集計から除外した．

これまで高い観測点検出性能を示してきた偵察経路を冗長化する手法は，他の 2 手法に比べ，最も多くのアラートが発生した．これは，偵察経路を冗長化する分だけ偵察トラフィック量も増加するためである．しかし，複数ポートを仮想 1 ポートとみなす手法は，必要な偵察パケット数が複数ポートに分散されることとなるため，全体的な発生アラート数が減少し，発生アラート数の変動も少ない結果となった．

次に 3 手法を同一のグラフ上で比較するため，図 9 に各手法の平均値をプロットした．このとき，単独ポートのみを利用する手法の結果は，最もアラート数が少なかった単独ポート (Best Case) での結果と最も多かった単独ポー

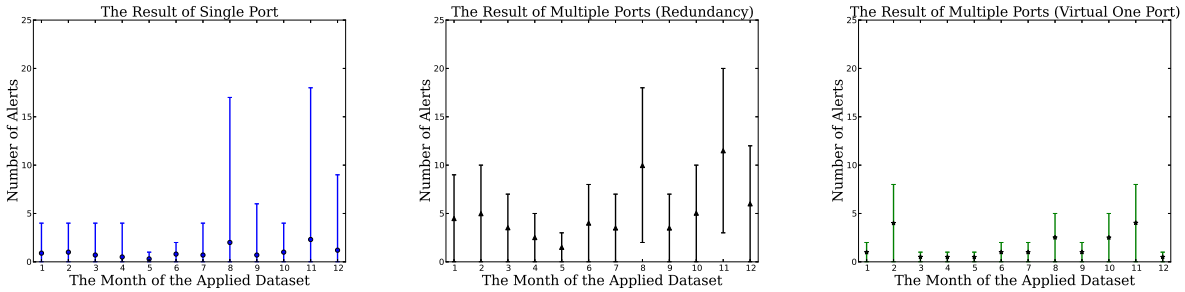

図 8: 単独ポートのみを利用する手法 (左)，偵察経路を冗長化する手法 (中)， 複数ポートを仮想 1 ポートとみなす手法 (右) における発生アラート数の変動幅

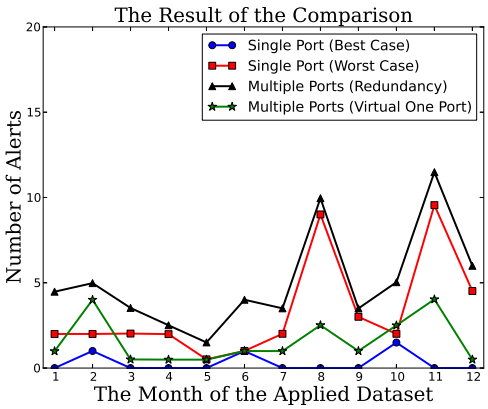

図 9: 各手法間での平均発生アラート数の比較

ト (Worst Case) での結果を分けて示した．単独ポートのみを利用する手法では，アラートが全く発生しない場合もあったが，偵察経路を冗長化する手法と同等のアラートが発生する場合も確認された．このように，従来の単独ポートのみを利用する手法が，偵察の秘匿性で必ずしも有利な結果とはなっていない．偵察経路を完全に冗長化する手法は秘匿性の面で不利な結果となったが，複数ポートを仮想 1 ポートとみなす手法のように，適切に偵察パケットを各ポートに分散できれば，秘匿性を保ちつつ複数ポートを偵察に利用することは十分に可能である．

6 おわりに

本稿では，主に攻撃者側の観点から既存の PN 符号を利用した観測点検出攻撃のノイズ耐性向上手法を考案し，実観測データを基にした評価結果を示した．これにより，攻撃者が 1 観測点の検出に複数ポートを利用した場合の検出性能，偵察の秘匿性への影響を明らかにした．

謝辞

本研究を進めるにあたり，インターネット上での実観測データを提供してくださった一般社団法人 JPCERT/CC に心より感謝申し上げる．また，本研究は一部科研費 (基盤研究 (C)23500094) の助成を受けたものである．

参考文献

[1] @police. http://www.cyberpolice.go.jp/

[2] nicter. http://www.nict.go.jp/

[3] ISDAS. http://www.jpcert.or.jp/isdas/

[4] WOMBAT. http://www.wombat-project.eu/

[5] DShield. http://www.dshield.org/

[6] Y. Shinoda, K. Ikai, and M. Itoh, “Vulnerabilities of Passive Internet Threat Monitors,” Proc. 14th USENIX Security Symposium (SEC), pp.209–224, July 2005.

[7] J. Bethencourt, J. Franklin, and M. Vernon, “Mapping Internet Sensors with Probe Response Attacks,” Proc. 14th USENIX Security Symposium (SEC), pp.193–208, July 2005.

[8] 内田幸治，篠田陽一，“標準偏差フィルタによるインターネット定点観測システムのアドレス探索の保護,” 電子情報通信学会技術研究報告. IN, 情報ネットワーク，vol.105，no.472，pp.85–90，Dec. 2005.

[9] W. Yu, X. Wang, X. Fu, D. Xuan, and W. Zhao, “An Invisible Localization Attack to Internet Threat Monitors,” IEEE Trans. Parallel and Distributed Systems, vol.20, no.11, pp.1611–1625, Nov. 2009.

[10] W. Yu, N. Zhang, X. Fu, R. Bettati, and W. Zhao, “Localization Attacks to Internet Threat Monitors: Modeling and Countermeasures,” IEEE Trans. Computers, vol.59, no.12, pp.1655–1668, Dec. 2010.