インターネット観測システムへの観測点検出攻撃を考慮した動的観測手法の一検討

成田 匡輝† 小倉 加奈代† 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, {ogura_k, bbb, takata}@iwate-pu.ac.jp

あらまし インターネット上の脅威を正確に把握するためには，攻撃観測を行う観測点の配置は隠蔽される必要がある．一方，攻撃者は観測点検出攻撃を行い，観測点を迂回しながらの活動を試みる．近年の PN 符号を用いた観測点検出攻撃は，少量の偵察パケットで観測点を検出するため，その攻撃検知は非常に困難である．我々はこの攻撃に対し，観測結果に反映させる観測点を切り替えて観測結果を提供する，動的観測手法による対策を提案する．この手法は既存手法と異なり，常に一部の観測点で得られた観測結果を公開する．MWS 2013 データセットの nicter ダークネットで得られた情報を基に，本手法が公開できる観測結果の有用性を検証した．

A Study of the Dynamic Internet Threat Monitoring for Preventing Localization Attacks to Each Sensor

Masaki Narita† Kanayo Ogura† 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, {ogura_k, bbb, takata}@iwate-pu.ac.jp

Abstract To grasp threats on the Internet accurately, sensors capturing packets should be hidden from the outside. However, attackers attempt to detect such sensors for evading them when they plot malicious activities. Recent localization attacks can detect sensors with low probing traffic volume by adopting PN code-based scheme. Here we propose the method of dynamic Internet threat monitoring to counteract such attacks. Unlike the previous method, our method publicizes a part of entire monitoring results at any time. We examined the publicizing results based on the dataset provided by MWS 2013 (nicter darknet).

1 はじめに

インターネットの利用は，既に我々にとって欠くことができないものとなり，今後も企業の経済活動，個々の私生活において，重要な役割を果たしていくことは明らかである．こうした背景から，インターネット上でサービスを提供しているサーバは，悪意を持ったインターネットユーザ (攻撃者) にとって，これまで以上に格好の標的となっている．事実，サーバソフトウェアの脆弱性を攻撃され，商用サイトから個人情報が漏洩する事案は連日のように報道されている．

一般的に，インターネット上でサービスを提

供しているソフトウェアの脆弱性に関する情報は，早急に公開される必要がある．それにより，当該ソフトウェアの脆弱性を修正するセキュリティパッチの開発，運用上の注意喚起等が可能になるためである．こうした脆弱性に関する情報を早期に公開する 1 つの方法として，インターネット上で発生している攻撃の動向を把握し，一般に公開することを目的に開発された，インターネット観測システムの運用が知られている．

インターネット観測システム (図 1) は，観測点 (sensor) と呼ばれる，パケット観測用の計算機をインターネット上の広域に配置する．観測点には，マルウェアが送出した攻撃パケット等，悪意を持って送出されたパケットを含む多数のパケットが到着する．各観測点は，それら到着パケットを観測ログに保存し，その観測ログの内容を集約先となるデータセンター (aggregator) に定期的に報告する．データセンターは，各観測点から収集した情報を分析し，アクセス数が特に増加しているポートを把握する等，観測結果の取りまとめを行う．そうして得られた観測結果は，各観測システムの運用組織のセキュリティポリシーに従い，主に Web サイト上で一般に公開される．

一方，攻撃者は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の攻撃活動を試みる．この観測点の検出は，攻撃者による観測点検出攻撃として知られている．近年の観測点検出攻撃は，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，初期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．観測点の配置状況が攻撃者に既知となることは，観測点が意図的に迂回され，攻撃パケットの観測が困難となる可能性が生じる．また，観測点そのものが DoS 攻撃の対象となり，インターネット観測システムの運用が妨害される可能性も考えられる．

近年の PN 符号を用いた観測点検出攻撃は，少量の偵察パケットで観測点検出が可能であるため，直接的な攻撃検知は非常に困難である．しかし，この攻撃手法が有効であるのは，標的とする観測システムの観測点の構成が変化しない場合に，攻撃者が連続的な観測結果を得られる場合である．そこで我々は，この攻撃手法に対し，観測結果に反映させる観測点を切り替えながら観測結果を公開する，動的観測手法による対策を提案する．提案手法によって公開可能な観測結果の有用性の検証は，MWS 2013 データセットの nicter ダークネットによって提供された情報を基に行い，本手法によってどれだけの攻撃動向を把握できるかを明らかにする．

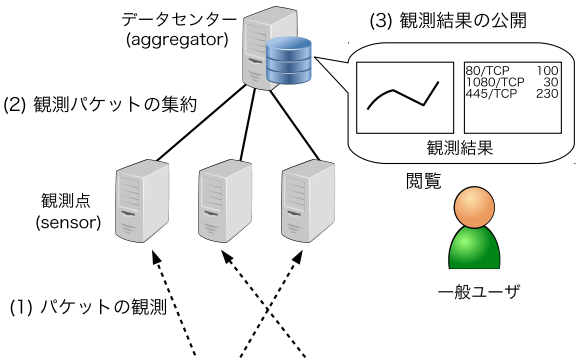


図 1: インターネット観測システム

2 関連研究

インターネット上に悪意を持って送出されたパケットを観測し，最新の攻撃の動向を把握するためのインターネット観測システムに関する研究は世界中で行われている．

例えば国内では，(独) 情報通信研究機構が未使用のグローバル IP アドレス空間 (ダークネット) を利用し，インターネット観測システムである nicter (Network Incident analysis Center for Tactical Emergency Response) [1] を運用している．nicter は国内で最大のインターネット観測網であり [2]，一般ユーザに対して詳細な設定が可能な分析用 Web ユーザインタフェースを提供している．また，JPCERT/CC (Japan Computer Emergency Response Team Coordination Center) による TSUBAME [3] は，国内だけでなく，アジア・太平洋地域にまたがる 23 組織 [1] と連携し，この地域一帯にインターネット観測網を構築している．

[1] 2012 年 10 月 1 日現在

海外では，CAIDA (Cooperative Association for Internet Data Analysis) [4] が IPv4 アドレス空間の約 1/256 に相当する /8 規模の広大なダークネットをインターネット観測に利用する等，大規模なインターネット観測を行っている．また，DShield [5] は多くの観測点をより広域に確保するため，プロジェクトに賛同した有志各々に観測点の設置を依頼するアプローチを採用している．DShield はこの方法で，世界中の有志からパケットの観測ログを募り，広大なコミュニティベースのインターネット観測網の構築に成功している．

こうしたインターネット観測システムに対し，攻撃者が観測点検出攻撃を行う可能性を最初に示唆したのが，篠田ら [6]，Bethencourt [7] らの研究である．彼らの手法は，まず攻撃者が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送出する．そして，インターネット観測システムが公開する観測結果に，大量に送出しておいた偵察パケットの痕跡が現れれば，攻撃者が当該ネットワーク内に観測点の存在を確認できるという手法である．しかし，この手法は大量の偵察パケットの送出を必要としており，たとえ厳密に検知することは困難であっても，統計的な異常値として対処する手法は既に考案されている [8]．

一方，Yu らは，より秘匿性を高めた観測点検出攻撃を提示した [9, 10]．この攻撃手法は，スペクトラム拡散通信の考え方に基づく，PN 符号を偵察に利用し，少量の偵察パケットで観測点の検出を実現する．攻撃者は，PN 符号の値に合わせ少量の偵察パケットを観測点の存在が疑われるネットワークに対し長期的に送出する．そして，後にインターネット観測システムによって公開される観測結果と自らが利用した符号語との相関値を算出することで観測点の存在を判定する．この攻撃手法は，偵察パケットが少量であるため，偵察パケットを検知・対処することが容易ではなく，未だ有効な技術的対策が確立されていない．そこで本稿では，次節でまずこの攻撃手法の概要を述べ，その後に我々の提案する対策手法を示す．

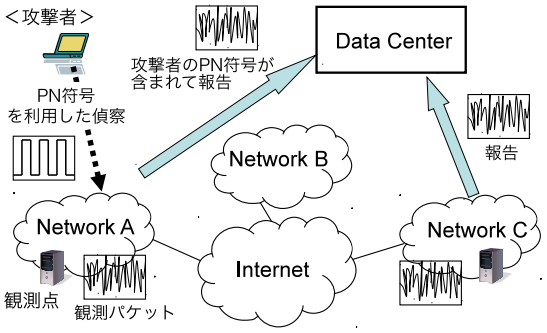


図 2: Step 1 (偵察トラフィックの送出)

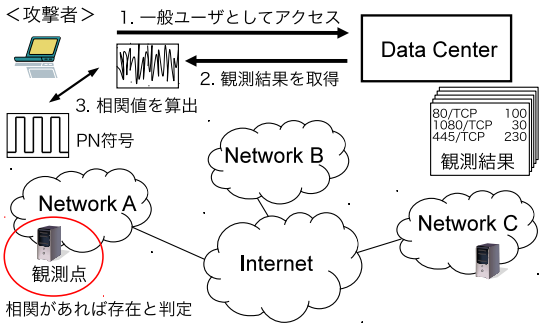


図 3: Step 2 (偵察結果の確認)

3 PN 符号を利用した観測点検出攻撃

本節では，我々が対策手法を提案する PN 符号を利用した観測点検出攻撃の概要を文献 [9] を基に述べる．この手法は，2 つの Step で構成される (図 2，図 3)．以下，各 Step の詳細，偵察トラフィックの生成，攻撃者が観測点の存在を判定するための相関値の算出方法を順に述べる．

Step 1　攻撃者は最初に，標的とするインターネット観測システムの運用組織に関する情報を収集し，観測点が配置されている可能性が高いネットワークを複数絞り込む．仮に図 2 のネットワーク A が，そうしたネットワークの 1 つであった場合，攻撃者は，例えばマルウェアが行う特定ポートへのポートスキャンを装い，ネットワーク A に偵察パケットを送出する．偵察パケットは，攻撃者自身が事前に用意した PN 符号の値に合わせて送出され，これが 1 つの符号

語に対応する偵察トラフィックとなる．

Step 2　攻撃者はその後，一般ユーザを装い，標的とするインターネット観測システムによって公開される観測結果にアクセスする．そして攻撃者は，一定の時間間隔で公開・更新される，偵察に利用したポートで観測されたパケット数と Step 1 で利用した符号語との相関値を算出する．攻撃者は，この相関値が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定する．

3.1　偵察トラフィックの生成

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 2 進乱数として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 ($\boldsymbol{C} = \langle C_1, C_2, ..., C_L \rangle \in \{-1, +1\}^L$)．PN 符号は通常，線形帰還シフトレジスタ等により生成が可能である．この符号は他のノイズに親和する一方，同符号語間でのみ高い相関を示す．そのため，PN 符号を偵察パケットの送出に利用することで，観測点に到着する他のパケットに偵察パケットを隠蔽しながら観測点の検出が可能となる．

偵察トラフィックの生成手順は以下の通りである．標的とするシステムがデータセンターで観測パケットを集約する時間間隔を T_s とした時，攻撃者は，各 T_s 毎に偵察パケットの送出，あるいは送出を一時停止する．図 4 は，PN 符号の例 ($L = 5$) とそれに対応する偵察トラフィックの生成例である．攻撃者は，各 T_s と PN 符号の 1 bit を対応させ，PN 符号の値が +1 の T_s では，必要な偵察パケット数 V を送出し，PN 符号の値が −1 の T_s では，偵察パケットの送出を一時停止する．T_s の値は標的とするシステムの観測結果の更新間隔に合わせて定め，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．

3.2　相関値の算出

攻撃者が観測点の存在を判定するための相関値の算出方法は以下の通りである．まず攻撃者は，標的とするシステムによって一定の時間間隔で公開される，自身が偵察に利用したポートで観測された観測パケット数を時系列に沿って保存し，ベクトル $\boldsymbol{\lambda}$ を得る．

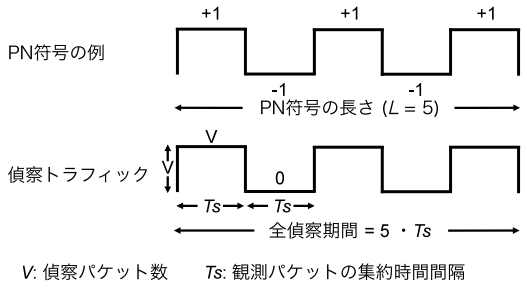


図 4: PN 符号と偵察トラフィックの生成

$$\boldsymbol{\lambda} = \langle \lambda_1, \lambda_2, ..., \lambda_L \rangle$$

次に $\boldsymbol{\lambda}$ の各成分から各成分の平均値 $E(\boldsymbol{\lambda})$ を減算し，新たなベクトル $\boldsymbol{\lambda'}$ を得る．

$$\boldsymbol{\lambda'} = \langle \lambda_1 - E(\boldsymbol{\lambda}), \lambda_2 - E(\boldsymbol{\lambda}), ..., \lambda_L - E(\boldsymbol{\lambda}) \rangle$$

攻撃者が偵察に利用した PN 符号のベクトルを $\boldsymbol{C}$ とした時，相関値 Γ はベクトル $\boldsymbol{C}$ とベクトル $\boldsymbol{\lambda'}$ の内積として以下の式で算出する．

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

得られた相関値 Γ が，観測点の存在判定の閾値を上回る時，攻撃者は対象のネットワーク内に観測点が存在すると判定する．以上が PN 符号を利用した観測点検出攻撃の概要である．

4　動的観測手法の提案

PN 符号を利用した観測点検出攻撃は，攻撃者が偵察に利用した符号語とデータセンターによって公開される観測結果との相関により観測点の検出を行っている．すなわちこの攻撃は，標的とするシステムが常に同一の観測点で観測した観測パケット数を一定の時間間隔で更新し，連続的な値として公開することを前提としている．ゆえに，この攻撃に対しては，常に同一の観測点での観測パケットを観測結果に反映せず，観測結果に反映させる観測点を切り替える対策が有効と考えられる．

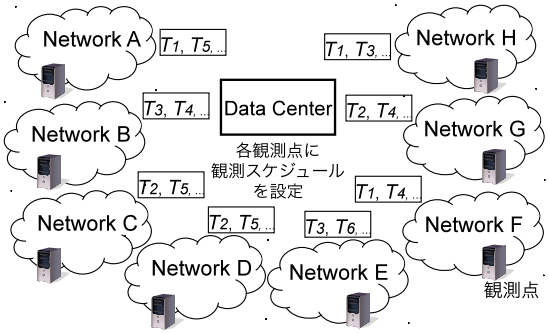


図 5: 各観測点への観測スケジュールの設定

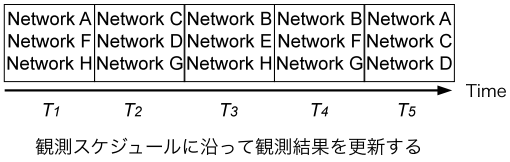


図 6: 観測スケジュールに沿った観測結果の公開

そこで我々は，観測結果に反映させる観測点を動的に変更するため，各観測点にパケットの観測を行う時間帯をスケジューリングし，それに基づき得られた観測結果を公開する動的観測手法を提案する．

4.1 動的観測の実現方法

本提案手法は，データセンターと観測点に以下に示す変更を加えることで従来のシステム上で実現可能である．

データセンターの役割 データセンターの役割は，従来のシステムと同様，観測パケットの集約及び一般ユーザに対する観測結果の公開である．しかし，次の点が従来手法と異なる．データセンターは配置されている観測点に，予めそれぞれの観測点が実際にパケットの観測を行う複数の時間帯 Tx を観測スケジュールとして設定する (図 5)．データセンターは，この観測スケジュールに基づき観測パケットを集約する．すなわち，本手法でのデータセンターは，観測スケジュールに沿って一部の観測点から報告された観測パケットを集約し，観測結果として一般に公開する (図 6)．

観測点の役割 本手法における観測点は，データセンターから観測スケジュールを受け取り，そのスケジュールに従い，到着するパケットの観測を行う．1 つの Tx で観測が完了する度，観測点はデータセンターに対し，観測パケットの報告を行う．観測点は必ずしも常時パケットの観測を行う必要はなく，観測スケジュールに従い動作する．

4.2 動的観測に必要な設定項目

今後本手法の検証を行う上で特に重要となる設定項目の議論を以下に述べる．

観測スケジューリング 公開する観測結果に反映させる観測点の選択をいかにスケジューリングするかという議論である．仮に一定の規則に基づきスケジューリングを行った場合，その選択規則が攻撃者に解析され，観測点の配置が推測されてしまう可能性が生じる．セキュアな観測点の選択として，攻撃者によって推測されることのない疑似乱数を用いて一様ランダムに観測点を選択する方式が有効と考えられる．

観測パケットの集約時間間隔 従来のシステムと同様に，観測結果の更新が頻繁に行われるほど，PN 符号を利用した観測点検出攻撃に限らず，攻撃者による偵察パケットの痕跡の確認が容易となる状況となる．観測結果の速報性と観測点検出攻撃への耐性の両面から観測パケットの集約時間間隔を定める必要がある．

観測結果に反映させる観測点数 本手法は，全観測点での観測結果は公開せず，その一部を公開する．一般的に観測結果に反映させる観測点数を増やすことで，より精密な攻撃情報を公開可能である．しかし同時に，攻撃者に与える情報も増えることとなり，観測点検出攻撃には脆弱となる．全観測点数に応じた，観測結果に反映させる適切な観測点数を定める必要がある．

4.3 本提案手法の利点と欠点

本手法の利点は，PN 符号を利用した観測点検出攻撃への耐性を獲得できる可能性が高い点である．公開する観測結果に反映する観測点を動的に変更し，常に同一の観測点での観測パケット数を公開しない本手法は，仮に攻撃者の偵察

表 1: 実験環境の設定

観測パケットの集約時間間隔	1 hour, 12 hours，24 hours
観測結果に反映させる観測点数	25，50，75，100，125，150
実験に適用するデータセット	2011 年取得分，2012 年取得分，2013 年取得分 (7 月 17 日現在)
観測パケットの種別	TCP，UDP

トラフィックが観測点に到達していたとしても，それが公開される観測結果に反映されるとは限らない．そのため攻撃者は，偵察に利用した符号語と公開される観測結果との間で相関値を算出することが困難となる．これは PN 符号を利用した観測点検出攻撃への有効な対策となる．

一方，従来のシステムでは，全観測点で取得した観測パケットを全て観測結果として公開するため，本手法が得られる情報量は，従来のシステムのそれと比較して劣る可能性がある．しかし，本手法がインターネット観測システムの運用意義を損なう程の情報量の減少となるか否かは明らかではない．よって次節では，インターネット上で多発している攻撃の動向を把握・周知するといった目的が達成可能であるかどうかについて評価する．

5 性能評価

本節では，提案手法の性能評価について述べる．これまで述べた通り，本手法は全体の観測点で得られた観測結果ではなく，常に一部の観測点により得られた観測結果を公開する．そのため，全体の観測点を利用すれば公開できるはずの情報に対して，本手法がそれにどれだけ近い情報を公開できるかが，本手法の有用性を示す指標の 1 つになると考えられる．

5.1 実験環境と評価方法

評価実験は，MWS 2013 のために用意されたデータセットの内，nicter ダークネットによって提供されたデータセットを基にしたシミュレーションによって行った．このデータセットには，連続した 4096 個のユニークな IP アドレスに到着したパケットが保存されている．本手法は本来であれば，インターネット上の異なるネットワークに配置された観測点で取得された観測パケットを基に検証されるべきであるが，本稿では実験環境の制約から，データセット内の各 IP アドレスそれぞれを別個の観測点とみなし，計 4096 個の観測点で構成されるインターネット観測システムを想定した．

本稿では提案手法を，全観測点の観測パケットを集約して得られた，観測パケット数が多い上位 20 ポートまでが含まれるポート番号の集合 A と，本手法で得られた上位 20 ポートまでが含まれるポート番号の集合 P が，平均してどれだけ一致するかを攻撃トレンドのカバー率 $(n(A \cap P)/n(A) * 100)$ とみなして評価した．

5.2 実験条件及びパラメータ

本実験では，各観測点への観測スケジュールの設定を，疑似乱数を用いて決定し，全ての観測点が一様ランダムに利用される設定とした．

観測パケットの集約時間間隔，観測結果に反映させる観測点数等の設定を表 1 に示す．表 1 が示す通り，評価実験に適用するデータセットは，2011 年，2012 年，2013 年 (7 月 17 日現在) の取得分として観測年別に 3 種類用意した．上記のデータセットにおいて，パケットの観測が停止されていたと考えられる期間は，実験時に除外した．また，観測パケットを TCP と UDP で区別し，観測パケットのプロトコル別の特徴の分析も試みた．

5.3 評価結果と考察

2011 年，2012 年，2013 年に nicter ダークネットで取得された各データセットに，本観測手法を適用した際の評価結果を示す．図 7 は，本手法を TCP パケットの観測に，図 8 は，UDP パケットの観測に適用した際の結果である．各グラフの横軸は，公開する観測結果に反映する観測点数である．また縦軸は，本手法による攻撃

トレンドのカバー率を示している．各グラフには，観測パケットを集約する時間間隔を 1 時間，12 時間，24 時間とした場合の結果をそれぞれプロットした．

図 7，図 8 に示した結果で最も重要なのは，TCP パケットの観測結果と UDP パケットの観測結果との性能差である．TCP パケットの観測結果のほうが良好であるのは，攻撃に利用される TCP ポートが，ある程度固定されていることが原因と推察される．一方，UDP ポートは，特定のサービスポートが定められていないことが多く，TCP ポートに比べて広範なポートが利用される．そうした傾向を踏まえた場合，この性能差は妥当な結果であると考えられる．

データセットの取得年別の結果については，2011 年のデータセット適用時に全体の性能が低下した．この点は，今後公開されるデータセットとともに追跡調査が必要と考えている．

観測パケットを集約する時間間隔については，TCP パケットの観測において，観測パケットを 12 時間，24 時間で集約した場合，攻撃トレンドを 7 割から 8 割程度把握できるという良好な結果を示した．また，1 時間の集約時間間隔という，早期の攻撃検出を試みても，約半分の攻撃トレンドの把握は可能であった．一方，UDP パケットの観測については，集約時間間隔に関わらず，いずれも結果が 3 割を下回った．

結論として本手法は，TCP パケットの観測では，容易にインターネット上の攻撃トレンドを把握することが可能である．一方，UDP パケットの観測では，TCP パケットによる結果には及ばない結果となったが，これは UDP プロトコルの利用傾向に起因するものであり，サービスポートが固定されている 2 割程度の攻撃トレンドは，本手法でも把握が可能であった．

6 おわりに

本稿では，PN 符号を利用した観測点検出攻撃への対策を行うため，全体の観測点の一部で得られた観測結果を公開するという，従来のシステムとは異なる観測手法を提案した．また，評価実験の結果から，一部の観測点で得られた観測結果を公開したとしても，インターネット上でアクセスが多発しているポートの情報を公開できる等，公開する情報の有用性は確保し得ることを示した．

本手法は，PN 符号を利用した観測点検出攻撃の仕組みに対し，理論上はセキュアであると考えられる．しかし，本手法であっても，攻撃者に好条件が揃った場合，あるいは過剰に観測情報を公開した場合に攻撃者が観測点の検出に成功する可能性は考えられる．今後，本手法の運用時のパラメータをより詳細に想定した上で，観測点検出攻撃をシミュレートし，本手法の安全性の定量的評価を行う予定である．

参考文献

[1] M. Eto, D. Inoue, J. Song, J. Nakazato, K. Ohtaka, and K. Nakao, “nicter: A Large-Scale Network Incident Analysis System: Case Studies for Understanding Threat Landscape,” *Proc. 1st Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)*, pp.37–45, April 2011.

[2] 井上大介, サイバー攻撃観測網について. http://www.ituaj.jp/archive/2013_04-3_sp-inoue.pdf

[3] TSUBAME. http://www.jpcert.or.jp/tsubame/

[4] CAIDA. http://www.caida.org/home/

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

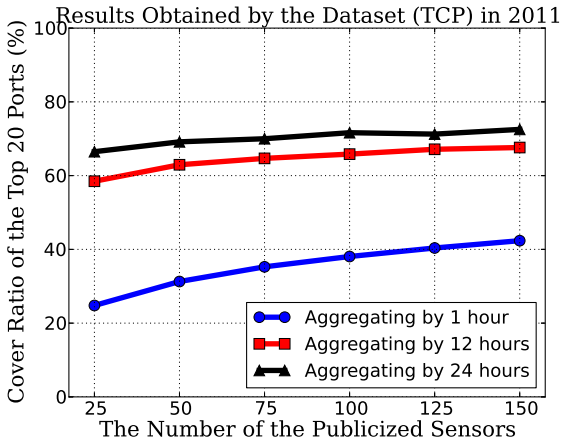
[6] Y. Shinoda, K. Ikai, and M. Itoh, “Vulnerabilities of Passive Internet Threat Monitors,” *Proc. 14th USENIX Security Symposium (SEC)*, pp.209–224, July 2005.

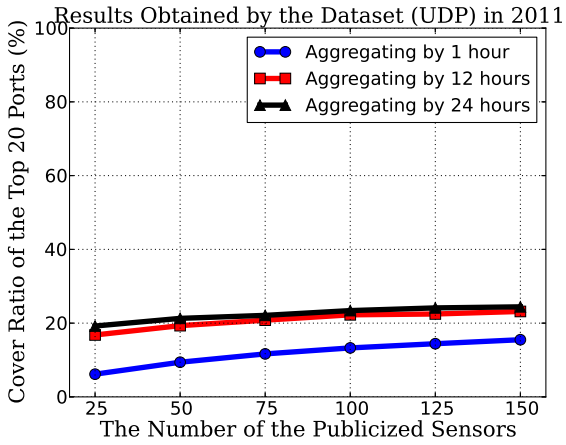
[7] J. Bethencourt, J. Franklin, and M. Vernon, “Mapping Internet Sensors with Probe Response Attacks,” *Proc. 14th USENIX Security Symposium (SEC)*, pp.193–208, July 2005.

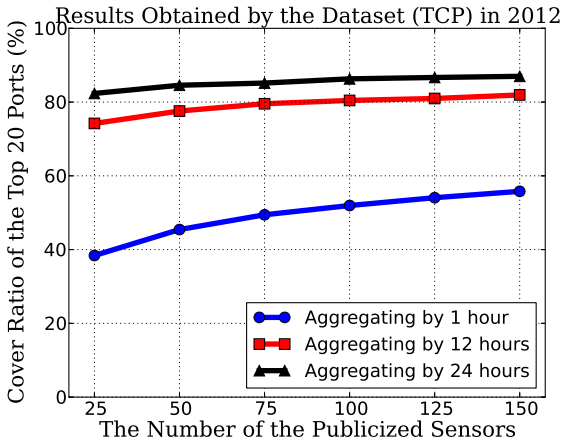
[8] K. Uchida, and Y. Shinoda, “The Statistical Protection for Internet Threat Monitors,” *Technical Report of IEICE. Information Networks*, vol.105, no.472, pp.85–90, December 2005.

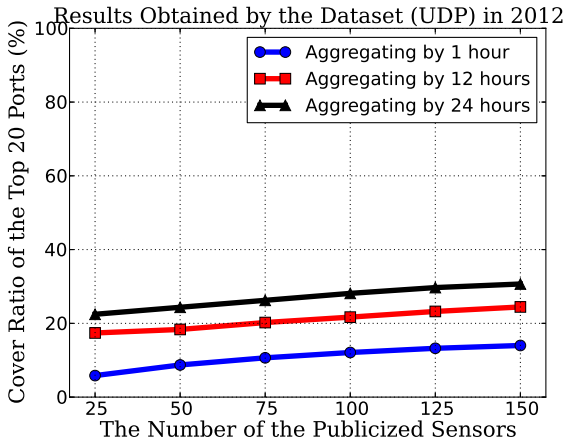
[9] W. Yu, X. Wang, X. Fu, D. Xuan, and W. Zhao, “An Invisible Localization Attack to Internet Threat Monitors,” *IEEE Trans. Parallel and Distributed Systems*, vol.20, no.11, pp.1611–1625, November 2009.

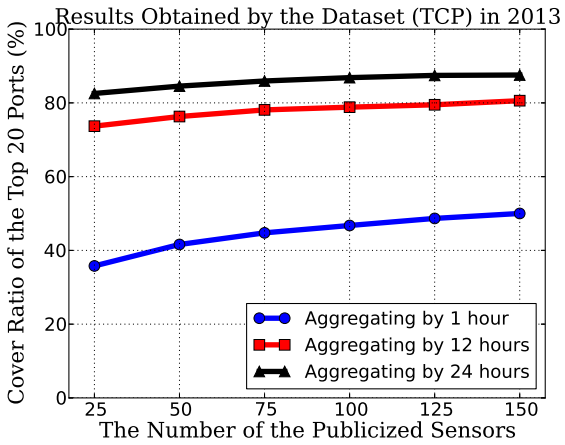
[10] W. Yu, N. Zhang, X. Fu, R. Bettati, and W. Zhao, “Localization Attacks to Internet Threat Monitors: Modeling and Countermeasures,” *IEEE Trans. Computers*, vol.59, no.12, pp.1655–1668, December 2010.











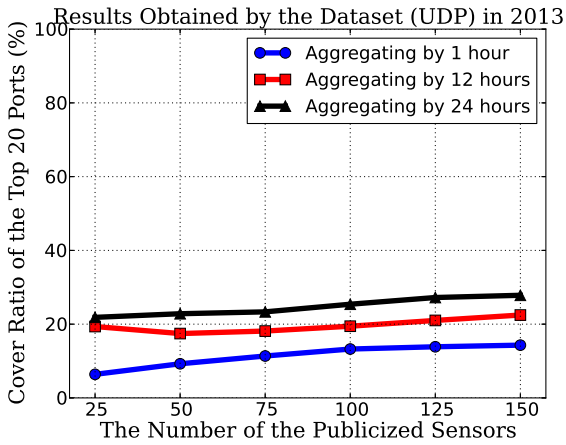


図 7: 2011 年，2012 年，2013 年に取得された各データセットを基に提案手法で TCP パケットの観測を行った場合のシミュレーション結果

図 8: 2011 年，2012 年，2013 年に取得された各データセットを基に提案手法で UDP パケットの観測を行った場合のシミュレーション結果