ダークネット観測におけるポート毎の動的観測に関する一検討

成田 匡輝 † 鎌田 恵介 ‡ 高田 豊雄 ‡

† 東北文化学園大学 科学技術学部 知能情報システム学科
981-8551 宮城県仙台市青葉区国見 6 丁目 45-1
narita@ait.tbgu.ac.jp
‡ 岩手県立大学大学院 ソフトウェア情報学研究科
020-0693 岩手県滝沢市巣子 152-52
g231m010@s.iwate-pu.ac.jp, takata@iwate-pu.ac.jp

あらまし ダークネット観測システムを構成する観測点の配置 IP アドレスを検出する，観測点検出攻撃が知られている．攻撃者は，標的ネットワークに秘匿シグナルを埋め込んだ偵察トラフィックを送出することで，秘密裏に観測点を検出する．これに対し我々は，公開する観測結果に反映する観測点を動的に切り替える，動的観測手法による対策を提案してきた．本研究では攻撃者が，1 つの観測点上の複数のポート間に，秘匿シグナルの埋め込みを試みた場合を考慮する．そこで我々は，観測するポート毎に動的観測を行う対策手法を提案する．本稿では，提案手法を nicter ダークネットに適用した場合の，公開可能な観測結果への影響を検証した．

A Study of Port-Based Dynamic Darknet Monitoring

Masaki Narita† Keisuke Kamada‡ Toyoo Takata‡

†Tohoku Bunka Gakuen University, Faculty of Science and Technology,
Department of Intelligent Information System
6-45-1 Kunimi, Aoba-ku, Sendai-shi, Miyagi 981-8551, JAPAN
narita@ait.tbgu.ac.jp
‡Iwate Prefectural University, Graduate School of Software and Information Science
152-52 Sugo, Takizawa-shi, Iwate 020-0693, JAPAN
g231m010@s.iwate-pu.ac.jp, takata@iwate-pu.ac.jp

Abstract Localization attack to a darknet monitoring system is detecting sensors that constitute the system. An attacker selects a probing traffic that embeds a secret signal and transmits it to a target network for detecting sensors. To counteract this attack, we have proposed a dynamic darknet monitoring method. It switches sensors, which contribute publicizing monitored results. In this study, we assume that attackers embed a secret signal among multiple ports on one sensor. Therefore we propose an improved dynamic darknet monitoring method. It switches ports as well as sensors, which contribute publicizing monitored results. We examined monitored results obtained by our method using dataset provided by nicter darknet.

1 はじめに

特定の企業や政府機関のシステムには，サービスを妨害するための攻撃パケットが，執拗に到着している．仮に，これらのシステムが未知の脆弱性を利用した攻撃の標的になった場合，保管している個人情報が外部に漏洩する等，深刻なセキュリティ問題が発生する．ダークネット観測システムは，このようなインターネット上での攻撃を早期に把握し，善良なインターネッ

ト利用者に注意を促すシステムである (図 1).

ダークネット観測システムは，インターネット上の未使用の IP アドレス帯に，観測点 (sensor) と呼ばれる多数のコンピュータを分散配置し，その IP アドレス帯に到着するパケットを捕捉する．捕捉したパケットは定期的にデータセンターに集約され，攻撃傾向を表す観測結果が一般公開される．これにより，善良なインターネット利用者に，ソフトウェアの脆弱性情報をはじめ，セキュリティ関連情報を迅速に提供する．

一方攻撃者は，ダークネット観測システムを構成する観測点を事前に検出しておき，観測点を迂回して活動する [1]．観測点が迂回されれば，ダークネット観測システムは正確な観測に基づく情報提供が困難となり，提供するサービスの質は著しく低下する．こうした観測点の検出行為は，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き，PN (Pseudo Noise) 符号を利用する [2] 等，攻撃手法を巧妙化させ，攻撃検知・対処が困難になってきている．

これに対し我々は，公開する観測結果に反映する観測点を動的に切り替える，動的観測手法による対策を提案してきた [3]．上記対策手法は，手法 [2] を想定した場合は有効であるが，攻撃者が，文献 [4] で指摘されている様な複数のポートに，秘匿シグナルの埋め込みを試みた場合を想定していない．そこで我々は，これまでの動的観測手法を改良し，観測するポート毎に動的観測を行う新たな対策手法を提案する．

動的観測手法は，常に一部の観測点で得られた情報を公開する手法であるという特性上，全ての観測点で得られた情報と比較した場合，公開できる情報は減少する．本稿では，提案手法を nicter ダークネットに適用した場合の，公開可能な観測結果への影響を検証した．

2　関連研究

ダークネット観測システムの例には，UCSD Network Telescope [5]，DShield [6]，NICT の nicter [7] 等がある．

攻撃者が，ダークネット観測システムを構成する観測点を検出・迂回する観測点検出攻撃の問題は，文献 [8, 9] によって明らかにされた．

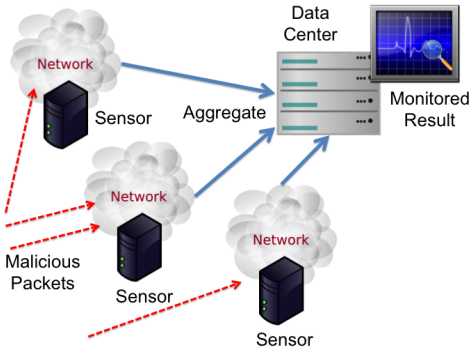


図 1: ダークネット観測システムの概要

近年の観測点検出攻撃は，攻撃者が偵察トラフィック送出の際に秘匿シグナル (例えば，PN 符号) を予め埋め込み，後に観測システムが公開する観測結果とこの秘匿シグナルとの相関の有無を検証する [2] 等，手口が巧妙化している．

上記攻撃への対策には，観測した時系列データの順序をランダムに入れ替える手法 [10]，観測結果の公開までに遅延時間を与える手法 [11] 等が提案されている．しかし，これらの対策では，ダークネット観測システムの提供する情報の一貫性，利便性を損なう問題がある．

我々はこの問題に対し，公開する観測結果に反映する観測点を動的に切り替える，動的観測手法による対策を提案した [3]．これにより，観測システムが公開する観測結果と攻撃者が埋め込んだ PN 符号との時間領域での相関値の算出を困難にした．本研究では，文献 [4] では考慮されていなかった，ある観測点上の複数のポート間に秘匿シグナルの埋め込みが行われる攻撃を想定し，動的観測手法の改良を検討する．

3　対象とする観測点検出攻撃

観測点検出攻撃は，偵察フェイズと偵察結果確認フェイズで構成される (図 2).

1. 偵察フェイズ　まず，偵察フェイズでは，攻撃者が偵察トラフィックのエンコードを行う．攻撃者は秘匿シグナルを生成し，それに基づき偵察トラフィックを変調する．このように秘匿シグナルが埋め込まれた偵察トラフィックは，観測点の存在が疑われる標的ネットワークに対して送出される．観測点が実際にそのネットワークに存在した場合，偵察トラフィックは，それ

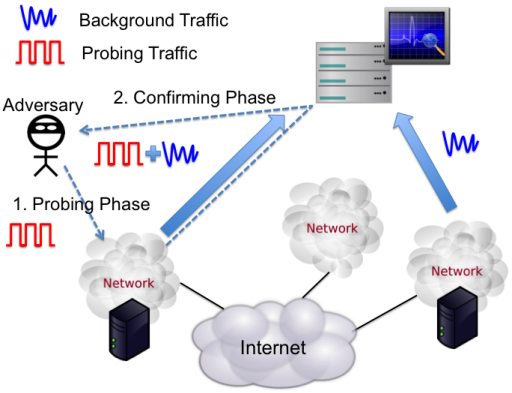


図 2: 対象とする観測点検出攻撃の概要

以外の無関係な観測パケットに混じってパケット観測ログに保存される．パケット観測ログは定期的にデータセンターで集約され，一定の時間間隔で観測結果として一般公開・更新される．

2. 偵察結果確認フェイズ　次に攻撃者は，善良なユーザを装いデータセンターにアクセスし，一般公開されている観測結果を取得する．攻撃者は，偵察フェイズで埋め込んだ秘匿シグナルがその観測結果に含まれているかどうかを判定するため，取得した観測結果と秘匿シグナル間で関連性を検証し，秘匿シグナルのデコードを試みる．秘匿シグナルが観測結果に確認できた場合，攻撃者は観測点が存在すると判定する．

攻撃者が偵察トラフィックを変調する場合，時間領域，周波数領域での変調が考えられる．過去に我々が対策手法を開発した PN 符号を利用した観測点検出攻撃は，時間領域での変調が行われている．本研究では，特に周波数領域での変調による偵察を想定する．

周波数領域での変調による偵察では，偵察トラフィックを特定の周波数 f で発生させ，標的ネットワークに送出する．偵察結果の確認は，取得した観測結果に高速フーリエ変換を適用し，特定のスペクトル密度にスパイクを発生させることで行う．偵察トラフィックは，攻撃者のみが知り得るホッピングパターンによって第三者から隠蔽される．

文献 [4] の手法では，ホッピングパターンに主に Space Hopping を用いており，攻撃者が生成したホッピングパターンによって，偵察トラフィックの送出先ポート番号を切り替え，観測点の検出を行う (図 3)．しかし，偵察トラフィックを送出するポート番号を切り替えるだけならば，常に同じ観測点で得られた観測結果を一般公開しない手法，即ち我々が文献 [3] で示した動的観測手法で対処できる．

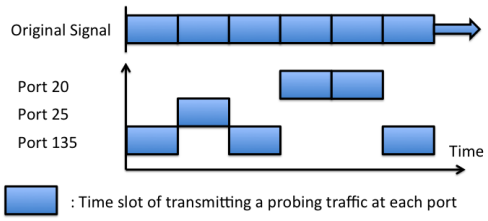


図 3: Space Hopping の例

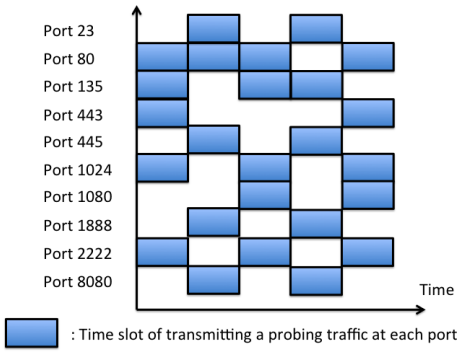


図 4: 複数ポートへの Space Hopping の例

しかし我々は，文献 [4] では明示されていないものの，図 4 に示すような 1 つの観測点上で観測されているポートの集合を $P = \{p_i\}$ (例えば図 4 の場合，$P = \{23, 80, 135, ...\}$) とするとき，P を複数のポートの集合 $P_1, P_2, ..., P_k$ に分割し (すなわち，$P = \cup P_i$，各 $i \neq j$ について $P_i \cap P_j = \phi$)，各 $P_i = \{p_{i1}, p_{i2}, ...\}$ 毎に独立に Space Hopping を適用する攻撃手法を考える．この攻撃手法は，我々の従来手法では対処を想定していない．

4　ポート毎の動的観測の提案

4.1　これまでの動的観測手法

過去に我々が対策した観測点検出攻撃 [2] は，偵察に利用した符号語とデータセンターで一般公開された観測結果との時間領域での相関により行われていた．そこで我々は，常に同一の観

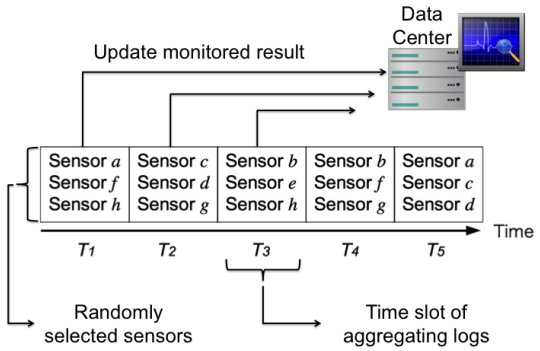


図 5: 動的観測手法の概要

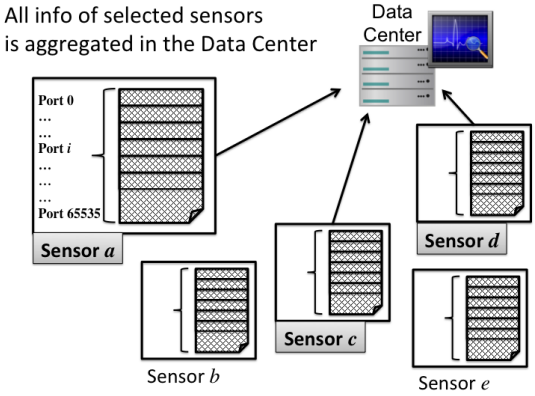


図 6: これまでの観測ログの集約方法

測点で得られた観測結果を公開せず，観測結果に反映させる観測点を切り替える動的観測手法 (図 5) を提案し，良好な防御結果を得た．

この手法でデータセンターは，観測結果に反映させる観測点を選択するため，観測スケジュールを予め各観測点に配布する．各観測点はその観測スケジュールに従って到着パケットの観測を行う．1 つの集約タイムスロットが経過する度，観測点はデータセンターに観測パケットの報告を行う．データセンターは，その観測ログを集約し，観測結果として一般公開する．本手法の運用面での議論は以下の通りである．

観測点の選択方法　一般公開する観測結果に反映させる観測点は，攻撃者に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選択する方式とする．

観測パケットの集約時間間隔　観測パケットの集約が早いほど速報性に優れる一方，攻撃者の偵察にも有利となる．文献 [12] のガイドラインに基づき，最長でも 24 時間とする．

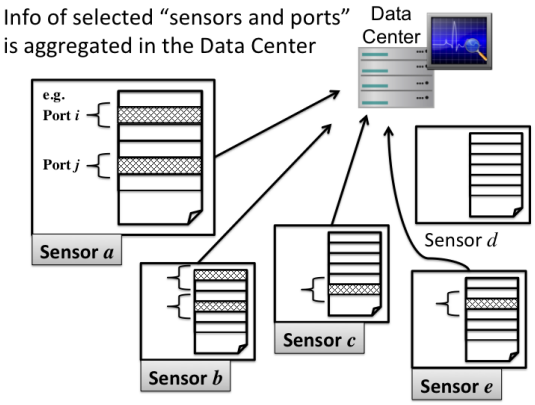


図 7: 提案する観測ログの集約方法

観測結果に反映させる観測点数　一般公開する観測結果に反映させる観測点数を増加させれば，より精密な攻撃情報を公開できる．一方，攻撃者の偵察に与える情報も増加する．全観測点数に応じた，適切な観測点数は検討中である．

4.2　これまでの動的観測手法の問題点

上記手法は，ある観測点で得られた観測ログを，一般公開する観測結果に反映させるか否かという観測点ベースの切り替えである．これは図 6 が示す通り，ある観測点が選択された場合，その観測点で得られた全ての観測ログが，データセンターで集約・公開される．この手法は，攻撃者が時間領域を利用した偵察を行う場合は有効である．

しかし，攻撃者の秘匿シグナルが，ある観測点の複数ポートに対して Space Hopping によって埋め込まれた場合，その観測点がデータセンターに選択される度，秘匿シグナルが定期的にデコードされてしまう可能性がある．ゆえに，秘匿シグナルが Space Hopping によって埋め込まれる可能性まで想定するならば，従来の動的観測手法には改良が必要である．

4.3　提案手法

そこで本稿では，観測点単位で情報を切り替えるだけでなく，観測点を選択した上で観測するポート番号まで切り替える，ポート単位での動的観測手法を提案する (図 7)．本手法は，我々

の従来の手法を踏襲しつつ，各観測点から観測ログを集約する方法を変更することで実現する．

具体的には，ある特定のポート番号 x で観測された観測パケットを集約したい場合，ポート番号 x での観測結果を集約するための観測スケジュールを作成する．即ち選択された観測点は，図 6 のように全てのポート番号の観測ログは報告せず，予め指定されたポート番号の観測ログを報告する．例えば，図 7 の Sensor a は，データセンターにポート番号 i，ポート番号 j だけの観測ログを報告している．

4.4 提案手法に関する議論

提案手法は，過去に対策した観測点検出攻撃 [2] への耐性に加え，攻撃者の秘匿シグナルが，ある観測点の複数ポートに対して Space Hopping によって埋め込まれた場合にも対応した防御手法である．観測ログを集約するタイムスロット毎に観測点を切り替え，時間領域への秘匿パターンの埋め込みを困難とし，報告すべきポート番号もランダムに決定するため，ある特定の観測点のポート番号の空間に秘匿パターンを埋め込むことも困難とする．

一方，本提案手法も従来の動的観測手法と同様，常に一部の観測点で得られた観測結果を一般公開するため，公開可能な情報が減少することが懸念される．さらに，ある観測点とその観測点のポートという関係も断絶されるため，各観測点特有の情報が失われる可能性もある．次節では提案手法が，一般的なダークネット観測システムと比較して，一般公開される情報にどの程度影響を及ぼすか検証する．

5 性能評価

性能評価は，MWS2015 で提供された nicter ダークネット (/20) による観測データセット [13] を利用したシミュレーションにて行った．本節では，提案手法を適用した場合に，一般公開できる観測結果にどの程度影響があるか検証する．

シミュレーションでは，2015 年 4 月，5 月，6 月を観測期間とし，観測ログは 24 時間毎に集約される設定とした．提案手法適用時は，観測ログを観測ポート毎に 256，512，1024 の観測点から集約した．評価指標は 2 種類定め，いずれも実際のダークネット観測システムの WEB インタフェースを参考にした．尚，評価環境の都合上，TCP・UDP パケットともに宛先ポート 0 番から 10000 番までを観測の対象とした．

5.1 宛先ポート番号の類似度による評価

実際のダークネット観測システムの多くは，観測結果として観測パケット数の上位 10 件程度の宛先ポート番号を公開している．そこで，観測結果の精度を評価する 1 つの指標として，全観測点を利用して得られた観測パケット数の上位の宛先ポート番号の集合と，提案手法による観測パケット数の上位の宛先ポート番号の集合の類似度を検証した．実験では，全観測点により得られた観測パケット数の上位 30 件の宛先ポート番号の集合 A と，提案手法による観測パケット数の上位 30 件の宛先ポート番号の集合 P との類似度を検証した．類似度算出には，シンプソン係数 $sim = \frac{|A \cap P|}{min(|A|,|P|)}$ を用いた．

評価結果を図 8，図 9 に示す．横軸が観測期間の 24 時間毎の観測ログの集約タイムスロットであり，縦軸が 2 つの集合の類似度 sim である．

TCP パケットの観測では，図 8 が示す通りに，いずれの場合も非常に高い類似度を示した．256 観測点 (全体の観測点の 1/16) から観測ログを集約するだけで 9 割以上の一致を示した．

一方，UDP パケットの観測では，図 9 が示す通りに，1024 観測点から観測ログを集約したとしても，高い類似度を示していない．これは上位 30 件の宛先ポート番号の中の下位のポート番号の入れ替わりが激しいためである．また，TCP パケットに比べ，全体的に UDP パケットの観測数が少ないことも原因である．そこで，上位 5 ポート程度に着目して分析したところ，TCP 同様に高い類似度が得られた．

5.2 観測パケット数のヒストグラムと時系列グラフによる評価

度々利用される観測結果の公開形式には，観測パケット数の時系列グラフがあることも知られる．そこで，2015 年 4 月に観測パケット数が特に多かった 23/tcp，観測パケット数 10 位から 20 位程度を継続的に維持した 445/tcp，UDP パ

ケットの例として 8888/udp ポートを挙げ，全観測点を利用して得られた観測パケット数の時間推移に，提案手法がどれだけ追従できるか検証した．

図 10 は，各宛先ポートに到着したパケット数をヒストグラムで表したものである．図 11 は，各宛先ポートへの到着パケット数の時系列グラフである．全観測点を利用した観測と提案手法による観測とでは，観測可能なパケット数の総量に違いがあるため，値は全て相互比較できるよう正規化している．

宛先ポートが 23/tcp，445/tcp の場合の観測結果では，ヒストグラムに若干の違いが見られるが，時系列で到着パケット数をプロットすると，提案手法による観測結果がオリジナルの観測結果にほぼ一致している．またこの傾向は，他の TCP パケットの観測数上位の宛先ポート番号にも当てはまることが確認された．

しかし，宛先ポートが 8888/udp の場合は，ヒストグラム，時系列グラフともに大きな違いが生じている．8888/udp での観測パケット数の時間推移 (図 11(c)) からオリジナルの観測結果と提案手法の観測結果が，同一傾向と判断することは困難と考えられる．UDP パケットの観測においては，上記のような結果を示すことが多々あるため，提案手法で UDP パケットの時系列グラフを公開する場合は注意が必要である．

6 おわりに

本稿では，攻撃者がダークネット観測システムの観測点を検出するため，1 つの観測点上の複数ポート間に秘匿シグナルの埋め込みを行うことを想定し，観測するポート毎に動的観測を行う新たな対策手法を提案した．提案手法を適用することによる，TCP パケットの観測への影響は軽微であった．UDP パケットの観測への影響はあったが，活動が顕著な攻撃は検知できており，運用上は問題ない可能性が高い．

今後は，複数ポート間に秘匿シグナルを埋め込む観測点検出攻撃を実装し，提案手法の防御性能を評価する予定である．

謝辞

貴重なデータセットを提供して下さった MWS 組織委員会，nicter 運営関係者に感謝する．本研究は一部科研費 (基盤研究 (C)26330159) の助成を受けたものである．

参考文献

[1] J. Xia, S. Vangala, J. Wu, L. Gao, and K. Kwiat, “Effective Worm Detection for Various Scan Technique,” *Journal of Computer Security*, vol.14, no.4, pp.359–387, 2006.

[2] 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, 2009.

[3] M. Narita, K. Ogura, B.B. Bista, and T. Takata, “Evaluating a Dynamic Internet Threat Monitoring Method for Preventing PN Code-Based Localization Attack,” *Proc. 17th International Conference on Network-Based Information Systems (NBiS 2014)*, 2014.

[4] W. Yu, S. Wei, G. Ma, X. Fu, and N. Zhang, “On Effective Localization Attacks Against Internet Threat Monitors,” *Proc. 2013 IEEE International Conference on Communications (ICC)*, pp.2011–2015, 2013.

[5] UCSD Network Telescope. `https://www.caida.org/projects/network_telescope/`

[6] DShield. `http://www.dshield.org/`

[7] 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*, pp.37–45, 2011.

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

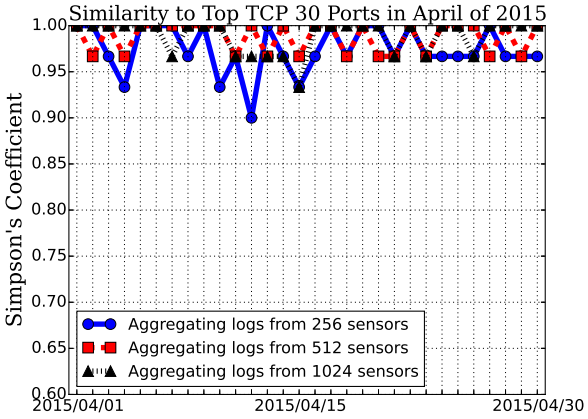
[9] J. Bethencourt, J. Franklin, and M. Vernon, “Mapping Internet Sensors with Probe Response Attacks,” *Proc. 14th USENIX Security Symposium*, pp.193–208, 2005.

[10] S. Wei, D. Shen, L. Ge, W. Yu, E.P. Blasch, K.D. Pham, and G. Chen, “Secured Network Sensor-Based Defense System,” *Proc. SPIE 9469, Sensors and Systems for Space Applications VIII*, 2015.

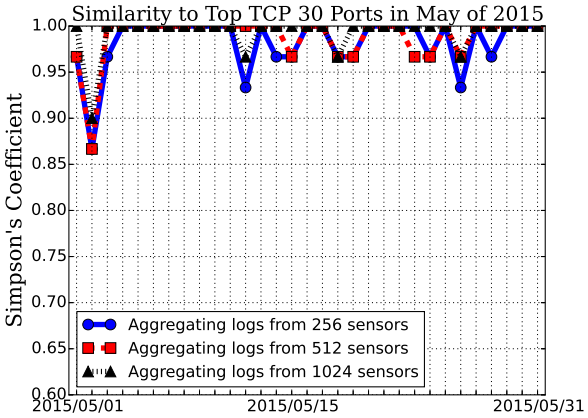
[11] W. Yu, N. Zhang, X. Fu, R. Bettati, and W. Zhao, “Localization Attacks to Internet Threat Monitors: Modeling and Countermeasures,” *IEEE Trans. Computers*, vol.59, no.12, pp.1655–1668, 2010.

[12] ENISA, “Proactive Detection of Network Security Incidents, Report,” `https://www.enisa.europa.eu/`, 2011.

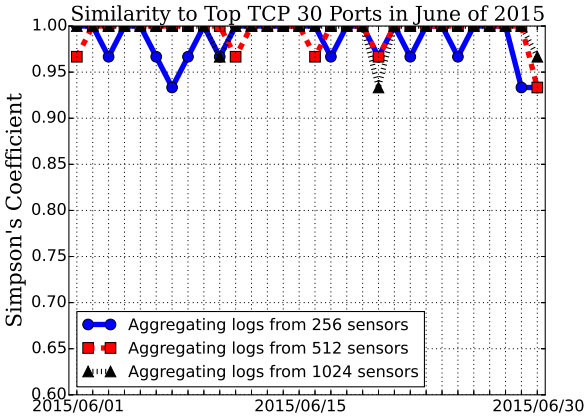
[13] 神薗雅紀, 他, “マルウェア対策のための研究用データセット〜MWS Datasets 2015〜,” MWS2015, 2015.



(a) 2015 年 4 月観測のデータを使用した場合

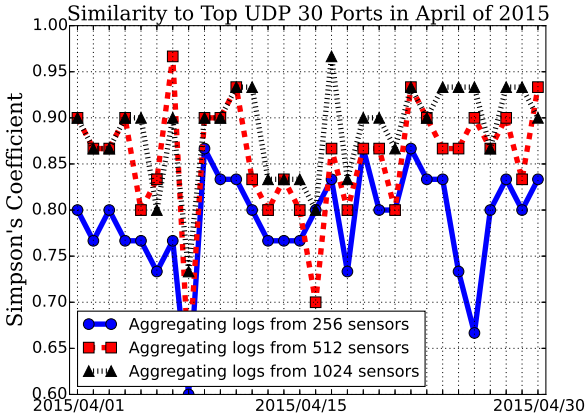


(b) 2015 年 5 月観測のデータを使用した場合

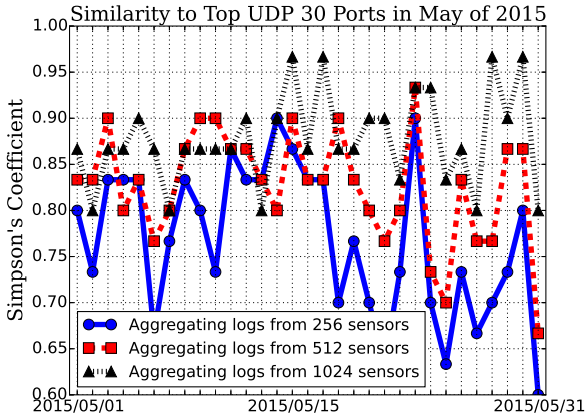


(c) 2015 年 6 月観測のデータを使用した場合

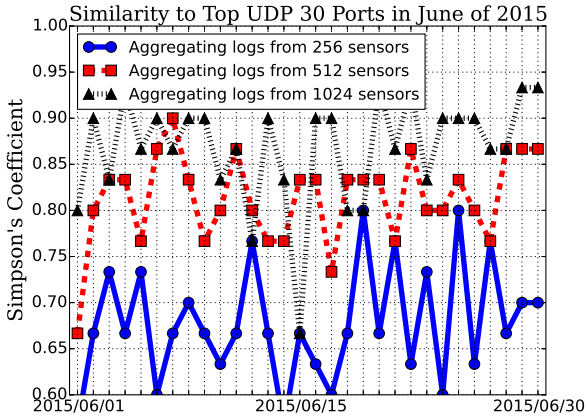
図 8: 2015 年 4 月，5 月，6 月に nicter で観測されたパケットデータに提案手法を適用した場合のアクセス数上位 30 ポート (TCP) との一致結果



(a) 2015 年 4 月観測のデータを使用した場合

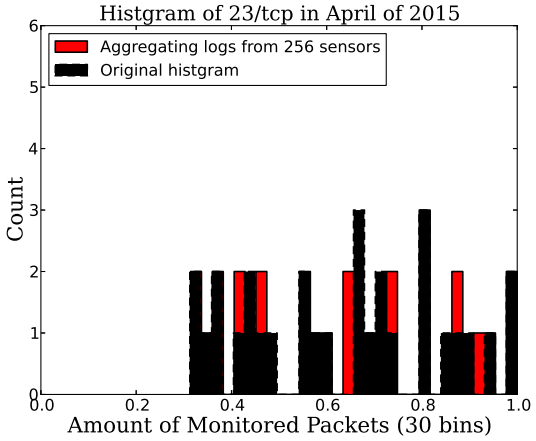


(b) 2015 年 5 月観測のデータを使用した場合

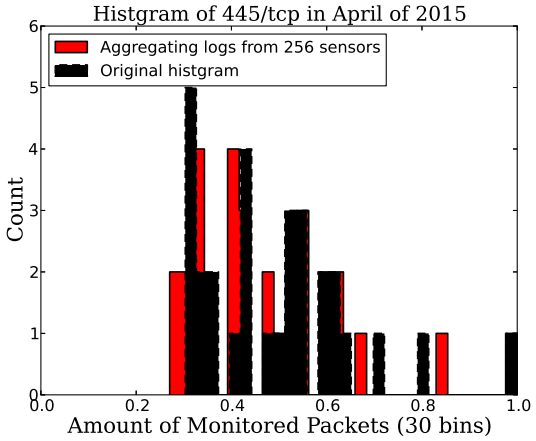


(c) 2015 年 6 月観測のデータを使用した場合

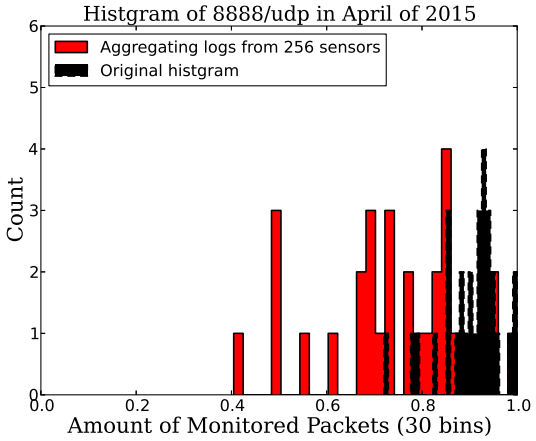
図 9: 2015 年 4 月，5 月，6 月に nicter で観測されたパケットデータに提案手法を適用した場合のアクセス数上位 30 ポート (UDP) との一致結果



(a) 23/tcp ポートでの比較

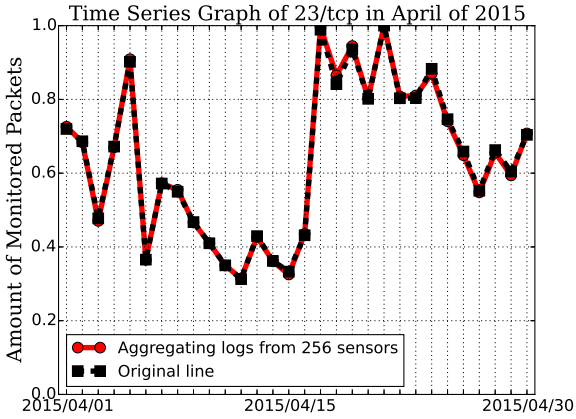


(b) 445/tcp ポートでの比較

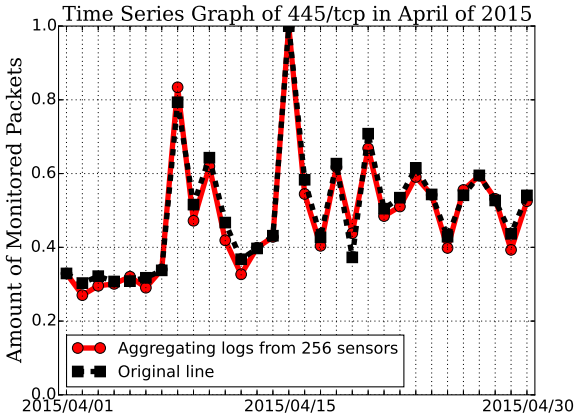


(c) 8888/udp ポートでの比較

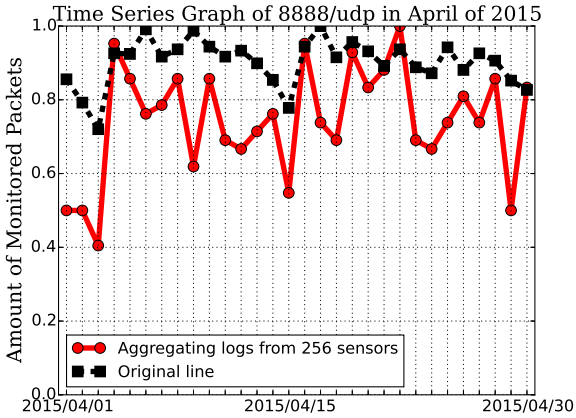
図 10: 2015 年 4 月に nicter ダークネットの 3 種類のポート番号で観測されたパケットのヒストグラムと，提案手法により 256 の観測点で得られた観測パケットのヒストグラムとの比較



(a) 23/tcp ポートでの比較



(b) 445/tcp ポートでの比較



(c) 8888/udp ポートでの比較

図 11: 2015 年 4 月に nicter ダークネットの 3 種類のポート番号での観測パケット数の時間推移と，提案手法により 256 の観測点で得られた観測パケット数の時間推移との比較