様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年　５月３１日現在

機関番号：１７１０２
研究種目：基盤研究（Ｃ）
研究期間：2009～2011
課題番号：21500078
研究課題名（和文）　ネットワークトラヒックを用いたネットワークサービスの構造発見と解析手法の確立
研究課題名（英文）　Structure discovery of Network Services by Using Network Traffic
研究代表者
堀　良彰（HORI YOSHIAKI）
九州大学・システム情報科学研究院・准教授
研究者番号：90264126

研究成果の概要（和文）：
ネットワークトラヒック観測により，ネットワークサービスの挙動を把握するため，その背後に潜む構造を発見し解明するための研究を実施した．通信を行う２者間で伝送されるパケット情報から機械学習を用いて，アプリケーション決定するための手法を考案した．ＩＲＣ通信を利用するトラヒック伝送間隔分布を解析することによって，ボットを検知する手法を考案した．さらに，ドメイン情報とその属性の関係構造をグラフ化することによる悪性ドメイン検出手法を考案した．

研究成果の概要（英文）：
We carry out research for discovering the structure of network services by using network traffic analysis. We propose a flow traffic classification scheme with machine learning by using payload length. We also propose bot detection scheme based on inter-arrival-time analysis on messages between an IRC client and an IRC server. Furthermore, we propose malicious domain evaluation scheme based on analysis of graph structure of domain information and its attributes.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００９年度	1,400,000	420,000	1,820,000
２０１０年度	1,100,000	330,000	1,430,000
２０１１年度	900,000	270,000	1,170,000
総　計	3,400,000	1,020,000	4,420,000

研究分野：
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：トラヒック観測，ネットワークセキュリティ，ネットワーク管理運用，構造発見，異常発見

１．研究開始当初の背景

ネットワーク化された情報システム環境の複雑性は，ユーザ数の増加，様々なプロトコルの利用，アプリケーションの複雑化，OS ならびにネットワークに接続されるデバイスの多様化等を要因として，さらに増加傾向にある．その結果，LAN のような最も小規模なネットワークにおいてさえ，ネットワークの挙動を把握することは挑戦すべき課題であり，障害対策，ネットワーク管理，セキュリティ対策のために特に重要さが増している．ネットワークの挙動把握のためには，複数のアプリケーションプロセスがどのように連携して，どのようなサービスを行っているかを把握する必要があるが，ネットワークトラヒックの観測で直接に得られる情報は

パケットやフローがネットワーク中を伝送されているという事実のみである．したがって，ネットワークの挙動把握のためには，パケットやフローの観測によって得られた情報を基にして，知的処理を行うことで，構造を発見し解析することで複数のアプリケーションプロセスとそれがもたらすサービスの状況を明らかにする必要がある．

従来行われている基本的解析手法として，パケットヘッダを参照して得られる IP アドレス，利用プロトコル，TCP/UDP のポート番号, TCP フラグ等の情報に基づきパケットを分類し解析する手法があるが，そのような手法は，ネットワークトラヒックの全体構造を理解する際には不十分である．また，パケットのペイロードを参照し，シグニチャベースのパターンマッチングを適用することで攻撃を検出する手法は，NIDS（Network Intrusion Detection System)において広く用いられているが，ペイロード参照のためのオーバヘッド，暗号化ペイロードへの対応困難，シグニチャの準備を必要という問題がある．

２．研究の目的

トラヒック観測によりネットワークの挙動を明らかにするために，パケットヘッダ情報に対する事前のルール設定を行わずネットワークトラヒックの背後に潜む構造を発見しそれを解明するための手法を確立することを目的とする．ここでの構造とは，ひとつのアプリケーションプロセスの振る舞いにとどまらず，関連する複数のプロセスの振る舞いに相当するものとする．このような構造を機械的に発見しそれを解析することは，ネットワーク管理運用，ネットワーク化された情報システムにおける異常発見，攻撃の検出と防御等の自動化をもたらし，複雑度を増す情報システムの管理コストを低減させ，ユビキタス社会を支えるネットワーク基盤の信頼性安全性確保に貢献できる．

３．研究の方法

事前のルール設定行わずネットワークトラヒックの背後にある構造を発見しそれを解明する手法を確立するために，次に掲げる３つの副課題を設定し総合的観点から研究を実施する．これらの副課題によって得られた知見は，他の副課題にフィードバックさせ有機的連携の下に並行して各課題を実施する．

［副課題１］視覚化によるネットワークトラヒックの背後にある構造の発見とその分析: ネットワークトラヒックの視覚化は，ネットワークトラヒック情報がもたらすいくつかの属性を，複数の軸や平面上に描画することで，パターンとして観測者に知覚させ，その構造を明らかにすることができる．本研究では，構造発見ならびにその解明を容易にするための視覚化手法による解析を行う．

［副課題２］クラスタリングによるネットワークトラヒックの背後にある構造の発見とその分析:ネットワークトラヒックはそれが有する多数の属性に関して，適切なクラスタリングを行うことにより，その構造を発見することができるようになる．本副課題では，攻撃トラヒック等いくつかの現実的なシナリオにおいて，その構造を発見し分析するための手法を考案する．

［副課題３］グラフマイニングによるネットワークトラヒックの背後にある構造の発見とその分析: 複数の通信者が連携してネットワークサービスや攻撃を実施する場合，単一の通信者のトラヒックの観測だけでは，その全体構造を明らかにすることはできない．そこで，本研究では，通信において用いられる情報の構造をグラフを用いて解析することで，その背後にある構造と特性を明らかにする．それにより，多数の通信者が関連するネットワークサービスにおける構造の発見と分析を行う手法を考案する．

４．研究成果

トラヒック観測によりネットワークの挙動を明らかにするために，ネットワークトラヒックの背後に潜む構造を発見しそれを解明するため，次の研究を行った．

トラヒック観測によりネットワークアプリケーションの挙動を明らかにする方策として，通信を行う２者間でやり取りされるパケット情報からアプリケーション決定手法を考案するための調査を行った．特に，ペイロード長によるアプリケーションの決定手法に着目した．アプリケーション開始時から１０パケット程度のパケット観測により，い

くつかのアプリケーションについては，それを推定できることを明らかにした．

ネットワークトラヒックが有する多数の属性に関して，適切なクラスタリングを行うことにより，その構造を抽出する手法について検討した．特に，ＩＲＣ環境におけるボットトラヒックの応用に焦点をあて，ボットが生成するパケット送出間隔情報にクラスタリング手法を適用することによって，その分布の特徴からボットを検出する手法を考案した．さらに，トラヒック送出間隔のばらつきを評価する指標としてクラスタリングよりも高速処理できるエントロピーに着目した手法を用いてボット検知システムを設計した．

ウェブサイトが有するドメイン名ならびに属性間の関連性に着目した信頼性評価の研究を行った．IP アドレスおよびドメイン名の割当機関，所属する AS 等の関係からグラフを構築しグラフの形状を評価することによる特徴抽出を行った．ネットワークサービスを実施する上では，ドメイン名や IP アドレスを行った情報をネットワークトラヒックとして送出する問い合わせにより順に解決していくため，これらを観測することによりウェブサイトの評価を行うことができる手法を考案した．悪意を持って構築されるウェブサイトのデータセットを評価したところ，ドメイン名登録者，IP アドレス，IP アドレスブロックへの集中がある構造を明らかにした．また，その構造を基にしたブラックリスト生成手法を考案した．

情報の漏洩問題に直面する機会が増えてきている．特に近年多くのネットワークアプリケーションの構築基盤として普及している HTTP によるネットワークを介した情報漏洩に関しては対策が不十分である．そこで HTTP リクエストが有する近似情報量を算出し，これによる異常検出に基づいた情報漏洩検知システムについて提案した．特に，HTTP リクエストの送出履歴に基づき近似情報量の精度を上げる手法を提案・評価した．さらに情報漏洩の恐れがある際にアラートを挙げるシステムの提案を行った．

HTTP リクエストの送信間隔分布によるウェブサーバへのアクセス挙動をモデル化する手法を考案した．さらに，確率分布の同一性を検定するコルモゴロフ・スミルノフ検定を用いその比較により異常検知を行う手法を提案した．実環境における１ヶ月分のウェブサーバのアクセスログを日毎に分割し，すべての組み合わせに対して検定を行った．これにより送信間隔分布に定常性が見られることを確認した．次に定常性の確認できたデータと，2 種類の模擬サービス妨害攻撃を行った際のアクセスログのデータとを検定した．定常データとそれぞれの模擬攻撃データの送信間隔分布に相違点が生じたことから異常挙動の検出を確認した．

これらの研究を実施することにより，トラヒック情報の解析に高度な数理的技法を適用することで，これまでの単純なパケットヘッダ情報へのパターンマッチングでは解析できなかったアプリケーショントラヒック挙動の解析手法について研究を行った．

５．主な発表論文等

〔雑誌論文〕（計４件）

Masayoshi Kohara, Yoshiaki Hori, Kouichi Sakurai, Heejo Lee, Jae-Cheol Ryou, ″Flow Traffic Classification with Support Vector Machine by Using Payload Length,″ Proceedings of the 2nd International Conference on Computer Science and its Applications (CSA2009), Vol. 2, pp.703-707, December 2009〈査読有〉

Seiichiro Mizoguchi, Yuji Kugisaki, Yoshiaki Kasahara, Yoshiaki Hori, Kouichi Sakurai, ″Implementation and Evaluation of Bot Detection Scheme based on Data Transmission Interval,″ Proceedings of the 6th Workshop on Secure Network Protocols (NPsec2010), pp.73-78, October 2010〈査読有〉

Seiichiro Mizoguchi, Yoshiro Fukushima, Yoshiaki Kasahara, Yoshiaki Hori, Kouichi Sakurai, ″Darknet Monitoring on Real-Operated Networks,″ Proceedings of the 5th International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA2010) pp. 278-285, November 2010〈査読有〉

Yoshiro Fukushima, Yoshiaki Hori, Kouichi Sakurai, ″Proactive Blacklisting for

Malicious Web Sites by Reputation Evaluation Based on Domain and IP Address Registration," Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-11), pp.352-361, November 2011〈査読有〉

〔学会発表〕(計１２件)

溝口誠一郎, 釘崎裕司, 笠原義晃, 堀良彰, 櫻井幸一, "データ送信間隔に基づくボット検知手法の実装ならびに評価," マルチメディア, 分散, 協調とモバイルシンポジウム(DICOMO2010), 岐阜県下呂市, 2010 年 7 月 7 日〈査読無〉

福島祥郎, 堀良彰, 櫻井幸一, "低レート攻撃トラフィック検出に関する検討", マルチメディア, 分散, 協調とモバイルシンポジウム (DICOMO2010), 岐阜県下呂市, 2010 年 7 月 7 日〈査読無〉

千葉一輝, 西出隆志, 堀良彰, 櫻井幸一, "情報量を用いた HTTP リクエストにおける情報漏洩検知システム", 2011 年火の国情報シンポジウム, 福岡市, 2011 年 3 月 9 日〈査読無〉

福島祥郎, 堀良彰, 櫻井幸一, "悪性 Web サイト間の関連性に着目した信頼性評価によるブラックリスト方式の検討", 情報処理学会第 146 回マルチメディア通信と分散処理・第 52 回コンピュータセキュリティ合同研究発表会, 大阪府吹田市, 2011 年 3 月 11 日

Seiichiro Mizoguchi, Yoshiaki Hori, Kouichi Sakurai, "Entropy based Network Behavior Characterization and Bot Detection," The 6th International Workshop on Security (IWSEC 2011), ポスター, 東京都, 2011 年 11 月 9 日〈査読無〉

Kazuki Chiba, Yoshiaki Hori, Kouichi Sakurai, "Reviewing the Way to Quantifying Information Leaks on HTTP Requests and Proposing the Detection System," 5th Workshop among Asian Information Security Labs (WAIS 2012), Pohang, South Korea, 2012 年 1 月 13 日〈査読無〉

千葉一輝, 堀良彰, 櫻井幸一, "履歴情報に基づく HTTP リクエストにおける情報漏洩量の数値化手法の検討," 2011 年電気関係学会九州支部連合大会 (第 64 回連合大会), 佐賀市, 2011 年 9 月 27 日〈査読無〉

溝口誠一郎, 堀良彰, 櫻井幸一, "エントロピーを用いた機械的特徴のスコアリングとボット検知への応用", 2011 年電気関係学会九州支部連合大会 (第 64 回連合大会), 佐賀市, 2011 年 9 月 27 日〈査読無〉

千葉一輝, 堀良彰, 櫻井幸一, "履歴情報に基づく HTTP リクエストにおける情報量の数値化手法の検討と検知システムの考案", 2011 年コンピュータセキュリティシンポジウム(CSS2011), 新潟市, 2011 年 10 月 19 日〈査読無〉

溝口誠一郎, 堀良彰, 櫻井幸一, "データ送信間隔のエントロピーに着目した挙動の数値化手法," 2012 年暗号と情報セキュリティシンポジウム (SCIS2012), 金沢市, 2012 年 1 月 31 日〈査読無〉

落水壱歩, 堀良彰, 櫻井幸一, "ウェブサーバのログ解析による異常検知", 火の国情報シンポジウム 2012, 福岡県飯塚市, 2012 年 3 月 15 日〈査読無〉

千葉一輝, 堀良彰, 櫻井幸一, "HTTP リクエストにおける情報量の外れ値検出を用いた漏洩検知", 2012 年電子情報通信学会総合大会, 岡山市, 2012 年 3 月 23 日〈査読無〉

〔その他〕

ホームページ等

http://itslab.inf.kyushu-u.ac.jp/index-j.html

６．研究組織

(1)研究代表者

堀　良彰 (HORI YOSHIAKI)

九州大学・大学院システム情報科学研究院・准教授

研究者番号：90264126

(2)研究分担者

櫻井　幸一 (SAKURAI KOUICHI)

九州大学・大学院システム情報科学研究院・教授

研究者番号：60264066

竹内　純一 (TAKEUCHI JUN-ICHI)

九州大学・大学院システム情報科学研究院・教授

研究者番号：80432871