

平成 17 年度科学研究費補助金実績報告書 (研究実績報告書)

1. 機関番号 1 4 6 0 3 2. 研究機関名 奈良先端科学技術大学院大学
3. 研究種目名 若手研究(B) 4. 研究期間 平成 16 年度 ~ 平成 17 年度
5. 課題番号 1 6 7 0 0 0 6 9
6. 研究課題名 独立成分分析によるインターネットトラフィック上の不正トラフィックの除去に関する研究

7. 研究代表者

研究者番号	研究代表者名	所属部局名	職名
1 0 3 3 5 4 9 0	フリガナ アダチナオトシ 安達 直世	情報科学研究科	助手

8. 研究分担者(所属研究機関名については、研究代表者の所属研究機関と異なる場合のみ記入すること。)

研究者番号	研究分担者名	所属研究機関名・部局名	職名
	フリガナ		
	フリガナ		
	フリガナ		
	フリガナ		
	フリガナ		

9. 研究実績の概要(国立情報学研究所でデータベース化するため、600字~800字で記入。図、グラフ等は記載しないこと。)

現在インターネットにおいては、ワーム感染によって発生する不正トラフィックの蔓延によるネットワークの利用効率の低下といった危険性に常にさらされている。新種のワームなどによる不正トラフィックは、その特性が未知であるため、対策は常に後手に回ることになりネットワークを介したセキュリティパッチの配布などにも支障を生じる可能性がある。これまでの研究および技術では、長期間に渡るトラフィックデータを観測し、不正トラフィックの発見の報告を元に、観測データを解析し特徴を捉え、以後の対策に利用する手法が一般的であった。しかし、このような手法では上でも述べたように、未知不正トラフィックに対しては即座に対応することができない。また観測データを蓄積するために、膨大なストレージを必要とする。

そこで本研究では観測結果から未知入力の変分が可能である独立成分分析の特徴を応用し、インターネット上の未知不正トラフィックの変分方法について研究を行った。観測データを通常の通信トラフィックと不正トラフィックが混合されたものであるとして注目し、混合過程のモデル化および不正トラフィックの推定・変分手法を提案した。提案手法の有効性を検証した結果、膨大な量のトラフィックデータを蓄積することなく、短期間における観測結果の統計情報だけを用いることによってパケットフィルタレベルで実装でき、提案手法により不正トラフィックの変分が可能であることがわかった。

これらに関する成果として、平成17年度において国内学会5件の発表を行い、さらに現在は学術雑誌への投稿を準備している。

成果の公表を見合わせる必要がある場合は、その理由及び差し控え期間等を記入した調書(A4 判縦長横書 1 枚)を添付すること。

10. キーワード

- (1) 独立成分分析 (2) 不正トラフィック推定 (3) 未知ウイルス対策
 (4) フィルタリング (5) ベイズ推定 (6)
 (7) (8)

(裏面に続く)

11. 研究発表(平成17年度の研究成果)

〔国内会議〕 計(5)件

著者名	論文標題			
安達直世, 笠原正治, 杉本謙二	BSS 問題における信号分離定式化表現にもとづいた不正トラヒック推定手法			
会議名	巻・号	発行年	ページ	
電子情報通信学会技術研究報告	NS2004-158	2004	21-24	

著者名	論文標題			
工藤正行, 安達直世, 佐藤淳, 笠原正治, 杉本謙二	無線アドホックネットワーク上における遠隔移動体制御システムの構築			
会議名	巻・号	発行年	ページ	
第49回システム制御情報学会研究発表講演会(SCI'05)		2005	401-402	

著者名	論文標題			
安達直世, 笠原正治, 杉本謙二, 新田益大	遠隔制御のためのフィードバック系を実現するネットワークアーキテクチャの提案			
会議名	巻・号	発行年	ページ	
電子情報通信学会技術研究報告	NS2005-35	2005	45-48	

著者名	論文標題			
工藤正行, 安達直世, 笠原正治, 杉本謙二	移動体遠隔操作に向けたセンサネットワークアーキテクチャ構成法			
会議名	巻・号	発行年	ページ	
計測自動制御学会第6回システムインテグレーション部門講演会(SI2005)	CD-ROM	2005	3K4-1	

著者名	論文標題			
安達直世, 工藤正行, 笠原正治, 杉本謙二	無線センサネットワークを利用した移動体遠隔制御			
雑誌名	巻・号	発行年	ページ	
計測自動制御学会関西支部平成17年度シンポジウム若手研究発表会		2005	55-58	

著者名	論文標題			
雑誌名	巻・号	発行年	ページ	

〔図書〕 計()件

著者名	出版社			
書名	発行年	総ページ数		

12. 研究成果による工業所有権の出願・取得状況

計()件

工業所有権の名称	発明者	権利者	工業所有権の種類、番号	出願年月日	取得年月日