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２５年５月２０日現在

機関番号：１７１０２
研究種目：基盤研究（Ｃ）
研究期間：2010～2013
課題番号：　22500093
研究課題名（和文）　ネットワーク不正侵入の効率的かつ高速な検知のためのヒストグラムデータベースの研究

研究課題名（英文）　Study on Histogram Database for Detecting Network Attacks

研究代表者
馮　尭楷（フォン　ヤオカイ）（Feng Yaokai）
九州大学・大学院システム情報科学研究院・助教
研究者番号：60363389

研究成果の概要（和文）：
ネットワークの不正侵入を効率的に検知するめに、刻々と観測されるパケットトラフィックの統計量を、通常時の統計量と比較し、統計量の時間的変化をみることで検知できることが明らかになった。具体的案としては、申請者は、既存の方法で検知が困難で、新しい攻撃技術としての低レート攻撃および次世代の攻撃とも呼ばれている分散型スキャン攻撃に関して、詳しく調査・分析の上で、新しい検知方法を提案した。セキュリティ分野の国際学会で発表の際、大好評を受けた。その拡張版は情報処理学会の英語論文誌 Journal of Informational Processing に採録され、2013 年 7 月に出版される予定である。ほかに、異なる次元数のデータの検索を対処できる索引構造も提案し、国際雑誌に採録された。

研究成果の概要（英文）：
By this study, it was made clear that the network attacks can be detected by checking the characteristic features of the packet traffics. As a concrete approach, we proposed a novel approach based on normal behavior mode for fast detection of distributed port scans in darknets. In this approach, the number of sources is counted in each time unit and a histogram is built for each of the monitored ports. Then, a normal behavior mode for each port can be extracted from the histogram of this port. At last, this normal behavior mode can be used to detect abnormal behaviors in the real network traffics. The related papers have been accepted by an internal conference and the Journal of Information Processing of IPJS.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２０１０年度	1,600,000	480,000	2,080,000
２０１１年度	900,000	270,000	1,170,000
２０１２年度	800,000	240,000	1,040,000
年度			
年度			
総　計	3,300,000	990,000	4,290,000

研究分野：情報学
科研費の分科・細目：　マルチメディア・データベース
キーワード：　データベースシステム

１．研究開始当初の背景

現在、インターネットの普及・拡大に伴い、インターネットに接続されたシステムに対する不正侵入の種類と頻度も増加している。重大な影響を与えるものが多い。ネットワークセキュリティシステムが必要であることは言うまでもない。

既存の異常検知システムには、１）導入作業が困難、２）多くの亜種・新種の攻撃の検知が困難、及び３）メンテナンスが煩雑という問題点がある。基本的な原因としては、現行システムでは、既存の不正侵入のパケットの既存パターンをシグネチャ辞書として整備し、それに一致するトラフィックを検知したら、脅威であると判断する方式が主流である。

２．研究の目的

攻撃を有効的に検知するために必要なヒストグラムの構成法、相応しい多次元インデックシング技術およびヒストグラムデータを利用してネットワーク攻撃の高速検知案の設計と評価。

３．研究の方法

第１段階では、既知の不正攻撃の特徴を詳しく分析する。そして、具体的なネットワークの個性を反映する通常時の統計量ヒストグラムデータベースを構築する。第２段階では、本システムに相応しい索引技術を導入して、異常検知を高速化させる。第３段階では、ネットワーク攻撃の検知案を構築して、性能を評価する。

４．研究成果

(1) ネットワークの不正侵入を効率的に検知するめに、刻々と観測されるパケットトラフィックの統計量を、通常時の統計量と比較し、統計量の時間的変化をみることで検知できることが明らかになった。

図１は分散型スキャン攻撃検知用のヒストグラムの例である。

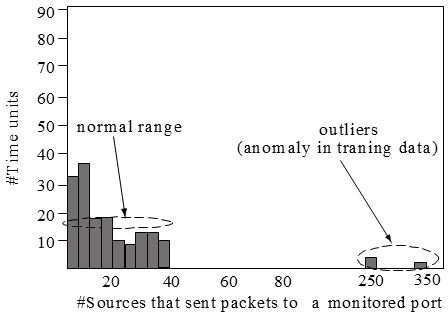

図 1. 分散型スキャン攻撃検知用のヒストグラムの例

(2) 具体的案としては、申請者は、既存の方法で検知が困難で、新しい攻撃技術としての低レート攻撃および次世代の攻撃とも呼ばれている分散型スキャン攻撃に関して、詳しく調査・分析の上で、新しい検知方法を提案した。セキュリティ分野の国際学会で発表の際、大好評を受けた。その拡張版は情報処理学会の英語論文誌 Journal of Informational Processing に採録され、2013年７月に出版される予定である。表１は提案の流れを、図２はデータ収集のプロセスを示す。図３は高速な学習と異常検知を実現するために本研究で提案したインデックス構造である。

表１．分散型スキャンの検知案

	Descriptions
学習	1. Collect and arrange the traffic Data
	2. Extract *source number vector* for each port.
	3. Create the *frequency distribution*
	4. Learn the *behavior mode* for each port
	5. Use an index for speeding up the learning
検知	Count and compare

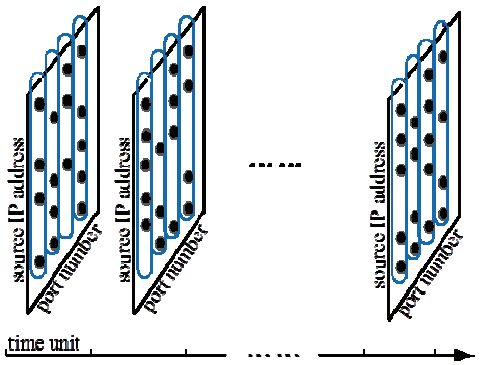

図 2. データ収集のプロセス

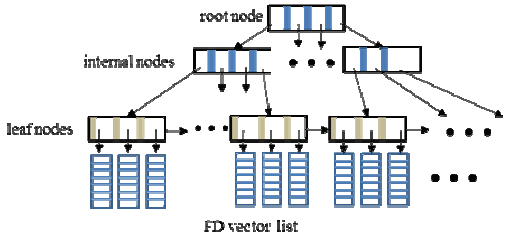

図 3. 学習と異常検知の高速化のために提案したインデックス

提案した学習アルゴリズムは表２で示す。このアルゴリズムの有効性は本研究で実証

した。

表 2．提案した学習段階のアルゴリズム

	Descriptions
1	• The bins are checked one by one starting from the rightmost bin in the frequency distribution (図 1). • The checked bins are placed in Ω. • Let d_n be the distance from the bin that was just checked, to the next bin. If there is no next bin, use the distance from the current bin to the y-axis as d_n.

2	Check the next bin if it exists.
	If (($d_n > \alpha$[1]) and (the area[2] in Ω is less than β%[3] of the total area)) then
	bins in Ω are regarded as outliers and are discarded
	go to step 1 // to find other outliers
	else
	put the current bin in Ω
	go to step 2 // this group is not finished

	1) Here α is a threshold. 2) The area denotes the number of time units. 3) β is another threshold, used to avoid the case where most of the bins are regarded as outliers.

以上の提案を利用して、あるダークネットの実際なトラフィックデータの異常検知の結果の例は図 4、5、6 で示す。

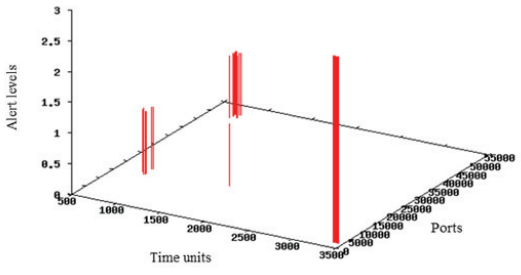

図 4．異常検知の例

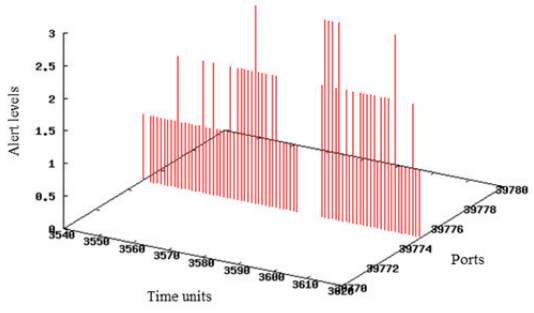

図 5．異常検知の結果例

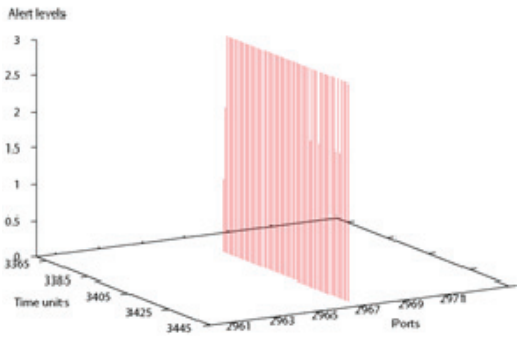

図 6．異常検知の結果例

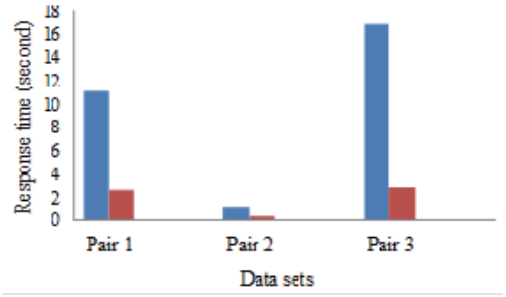

図 7．提案したインデックスの性能
Left bins: without index,
Right bins: using the index

提案した多次元インデックスの性能は図 7 で実証した。

(3) 異なる次元数のデータの検索を対処できる索引構造も提案し、国際雑誌に採録された。(4) セキュリティ分野で実際の研究・開発について深い知見と経験を得た。

研究期間では、国内研究会発表 1 回、国際学会（査読有）発表 2 回、国際雑誌（査読有）3 編、という業績が残ってある。詳しくは「主な発表論文等」を参照。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　3　件）

(1) **Yaokai Feng**, Yoshiaki Hori, Kouichi Sakurai, Jun'ichi Takeuchi,
A Behavior-Based Method for Detecting Distributed Scan Attacks in Darknets, Journal of Information Processing, Vol.21, No.3, Page 1-12, 2013.07. （査読有）

(2) **Yaokai FENG**, Kunihiko KANEKO, Akifumi MAKINOUCHI,
Efficient Evaluation of Partially-dimensional Range Queries in Large OLAP Datasets,

International Journal of Data Mining, Modelling and Management, Vol. 3, No. 2 , Page 150-171, 2011.06. （査読有）

(3) **Yaokai Feng**, Akifumi Makinouchi, Ag+-tree: an Index Structure for Range-aggregation Queries in Data Warehouse Environments, International Journal of Database Theory and Application, Vol. 4, No.2, Page 51-64, 2011.06. （査読有）

〔学会発表〕（計 3 件）

(1) **Yaokai Feng**, Yoshiaki Hori, Kouichi Sakurai, Jun'ichi Takeuchi, A Behavior-based Detection Method for Outbreaks of Low-rate Attacks, The 12th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT 2012), Page 267-272, 2012.07. （査読有）

(2) フォン ヤオカイ, 堀 良彰, 櫻井 幸一, 竹内 純一, 挙動に基づく同時多発低レート攻撃の検知案および実験検証, 第 17 回情報通信システムセキュリティ研究会（ICSS2012）, 2012.03.16. （査読無）

(3) **Yaokai Feng**, Seiichi Uchida, How to Design Kansei Retrieval Systems?, The 11th International Conference on Web-Age Information Management (WAIM2010), Lecture Note on Computer Science, LNCS 6184, Springer-Verlag, , Page 405-416, 2010.07. （査読有）

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
馮 尭楷（フォン ヤオカイ）
(Feng Yaokai)

九州大学大学院システム情報科学研究院
助教
研究者番号：60363389

(2)研究分担者
牧之内 顕文（Makinouchi Akifumi）
久留米工業大学工学部 教授
研究者番号：30221576

(3)連携研究者
（ ）

研究者番号：