様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　３ 年　 ６ 月 ２０ 日現在

機関番号：１７１０２
研究種目：基盤研究(C)（一般）
研究期間：2018～2020
課題番号：１８Ｋ１１２９５

研究課題名（和文）多次元挙動パターンの高速自動抽出によるサイバー攻撃の検知に関する研究

研究課題名（英文）Study on Cyber-attack Detection based on Automatic Extraction of Multi-dimensional Behavior Modes

研究代表者

馮　尭楷（Feng, Yaokai）

九州大学・システム情報科学研究院・助教

研究者番号：６０３６３３８９

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：１）分散型攻撃の有効検知のための必要な特徴を検討した。２）機械学習に基づく軽量的な攻撃検知システムの実現・性能実証を行った。３）独特な特徴選択の方法を提案し、それを利用して、複数の検知器を並列的に用いる検知システムの提案および性能実証を行った；４）攻撃検知の複数の性能指標のバランスを保つことために、複数の分類器を利用する方法に関して、関連パラメーターの検知性能への影響を調べ有意義な知見を得た。５）多次元行動パターンからの攻撃検出のための閾値の自動抽出やその閾値の自動調整に関する研究を行い、意義がある結果を得た。本研究の研究成果により、学術雑誌論文7件および国内外学術会議論文8件を出版した。

研究成果の学術的意義や社会的意義
今回の研究で得られた様々な知見は、今後の研究や実際のサイバー攻撃検知システムの設計に役立つ。特には、1）新しい特徴選択方法を提案し、それを使用して複数の検出器を並列に使用する検出システムの提案； 2）攻撃検出システムにある複数の性能指標のバランスを保つのは難しい問題を解決するための調査と提案（複数の分類器を使用する順次検出システムのパラメーターの決定法）；3）多次元行動パターンから攻撃検出用閾値を自動抽出し、その自動抽出閾値を検出時に自動的に調整することにより実現した2段階検出方式は、検知システムの軽量化を実現したので、特に IoT 関連のシステムでは重要な知見と考えられている。

研究成果の概要（英文）：1) The necessary features for effective detection of distributed attacks were investigated. 2) Realization and performance verification of a lightweight attack detection system based on machine learning. 3) A new feature selection method was proposed,we proposed a detection system that uses multiple detectors in parallel and demonstrated its performance. 4) Regarding the method of using multiple classifiers in order to maintain the balance of multiple performance indicators for attack detection, the effects of related parameters on the detection performance were investigated and meaningful findings were obtained. 5) We conducted research on the automatic extraction of thresholds for attack detection from multidimensional behavior patterns and the automatic adjustment of the thresholds during detection, and obtained meaningful results.
Based on the research results of this research, seven academic journal papers and 8 domestic/international academic conference papers were published.

研究分野：情報セキュリティ

キーワード：攻撃パターン　パターンの自動抽出　検知時の閾値自動調整　サイバー攻撃　アンサンブル検知　シーケンシャル検知　2段階検知　特徴選択

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属します。

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

政府も企業も巨大な資金を投入し、多くの研究者が様々な防衛・検知案およびシステムを研究・構築してきたにも関わらず、サイバー攻撃による被害は甚大で急増している。その原因としては、攻撃技術の高度化・多様化によって攻撃の手法は頻繁に変わっているが、攻撃の検知手法は本質的に大きい変化がないことが挙げあれる。挙動に基づく方法は将来性があるとよく言われ、近年、マルウェアの分類でよく研究されている。しかし、残念なことに、相応しい挙動パターンの定義、高速抽出と高速マッチングは難しいので、挙動に基づく方法を利用するトラフィック監視による攻撃検知は実用できるシステムがまだ存在してない。

２．研究の目的

挙動に基づく手法は次世代のセキュリティ検知技術と言われ、近年、マルウェアの分類でよく研究されている。しかしながら、解決しなければならない問題があるので、挙動に基づく手法を利用したトラフィック監視による攻撃検知は実用できるシステムがまだ存在しない。本研究はそのようなシステムのコア技術を研究・提案することによって、実用可能な挙動に基づくネットワーク攻撃検知システムの提案・構築および性能検証を行う。

３．研究の方法

① 収集したトラフィックデータセットの前処理を行う；
② 多次元挙動パターンの構成を考案し、検知性能の確認を行う；
③ 学習データから通常時挙動パターンの自動抽出手法を提案し、実験を実施する；
④ 抽出された挙動パターンの後処理を行う；
⑤ 検知時の挙動パターンを高速に作成する手法を提案し、性能実証を行う；
⑥ 多次元挙動パターンの高速マッチング手法を検討する；

４．研究成果

① SDN の模擬環境（Mininet と Ryu)を作成し、その環境での攻撃データおよび通常データを D-ITG（分散型インターネットトラフィックジェネレーター）を利用して発生させ、検知システムの性能実証に必要なトラフィックデータを収集した。

② 歴史のトラフィックデータから行動パターンを自動的に抽出するための考案（下図）を更なる検討して改善方法を示した。

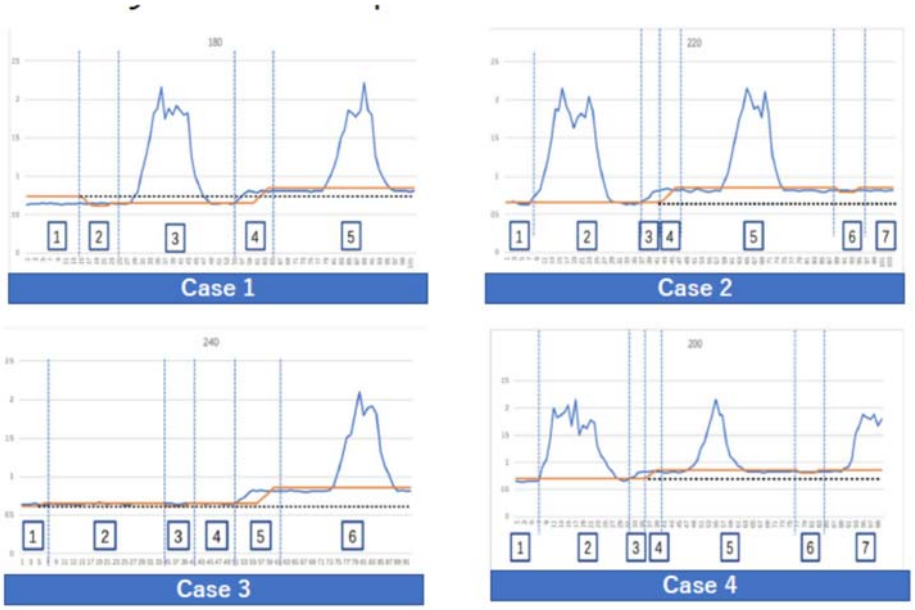
③ 特徴を評価するアルゴリズム（下図）を提案し、これを利用した軽量のサイバー攻撃検知システムの実装および性能実証を行った。

Algorithm 1 Correlated-Set Thresholding on Gain-Ratio (CST-GR)

Input: Feature Set (FI)
Output: Selected Feature Set (FS)

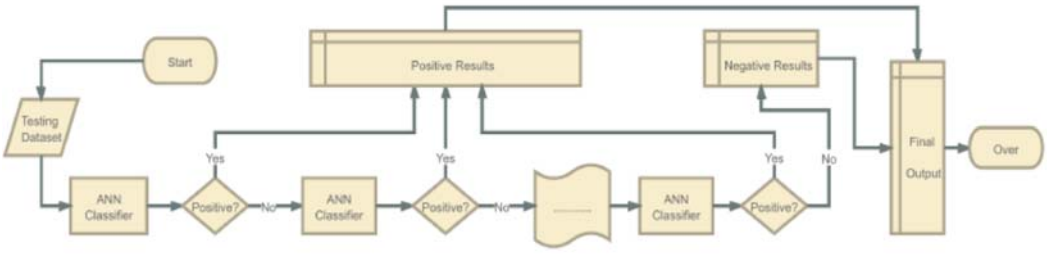
1. Read all the original features to the set FI.
   FI = $\{f_1, f_2, f_3, \ldots\ldots\ldots, f_n\}$, n = the number of the original features
2. Extract the feature set having the highest correlation based on the merit function: Equation (1), FC ⊂ FI
   FC = $\{f_1, f_2, \ldots, f_c\}$, c = the number of features in the subset having the best merit value
3. Calculate the minimum gain value of the features in FC, f_{min} (FC)
4. Use Equation (2) to calculate the gain-ratio value of each feature of FI
   GR = $\{\{f_1, v_1\}, \{f_2, v_2\}, \ldots, \{f_n, v_n\}\}$, where v_i is the gain-ratio value of f_i $(1 \le i \le n)$
5. From GR, select the features whose gain-ratio values are greater than or equal to f_{min} (FC), FS ⊂ FI
   FS = $\{r_1, r_2, r_3, \ldots\ldots\ldots, r_s\}$, s = the number of finally selected features
6. Output FS

④ 事前に自動抽出したパターンを利用した上で検知時に閾値の自動調整を導入する 2 段階検知システムを提案し、検知性能を実証した（下図)。

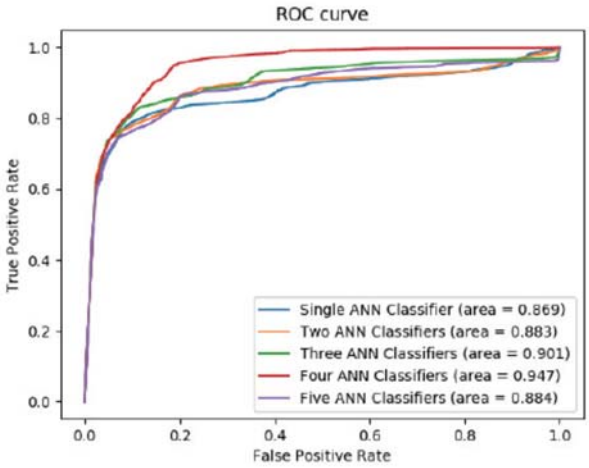


図： 提案した 2 段階検知法の性能実証。縦軸は検知時の閾値の動的調整（オレンジ色の線）；横軸は時間である。この結果から、時間のかかる本番検知アルゴリズムの呼び出し回数は明らかに減少していることが分かる

⑤ サイバー攻撃検知システムの偽陽性率と偽陰性率を同時に減らすために、ニューラルネットワークに基づくシーケンシャル検知システム（下図 a）を提案し、性能実証を行った（下図 b)。



図(a) 本研究で提案したシーケンシャル攻撃検知システム



図(b)提案したシステムの性能実証

（４つの分類器の場合は検知性能がベストであることが分かった）

５．主な発表論文等

〔雑誌論文〕　計10件（うち査読付論文　10件／うち国際共著　4件／うちオープンアクセス　5件）

１．著者名 Wang Tao, Yaokai Feng, Kouichi Sakurai	４．巻 2021
２．論文標題 Improving the Two-stage Detection of Cyberattacks in SDN Environment Using Dynamic Thresholding	５．発行年 2021年
３．雑誌名 Proc. 15th International Conference on Ubiquitous Information Management and Communication	６．最初と最後の頁 1-7
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/IMCOM51814.2021.9377395	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Yan Naung Soe, Yaokai Feng, Paulus Insap Santosa 2, Rudy Hartanto and Kouichi Sakurai	４．巻 9(1)
２．論文標題 Towards a Lightweight Detection System for Cyber Attacks in the IoT Environment Using Corresponding Features	５．発行年 2020年
３．雑誌名 Electronics	６．最初と最後の頁 1-19
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/electronics9010144	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Hao Zhao, Yaokai Feng, Hiroshi Koide, Kouichi Sakurai	４．巻 10
２．論文標題 A Sequential Detection Method for Intrusion Detection System Based on Artificial Neural Networks	５．発行年 2020年
３．雑誌名 International Journal of Networking and Computing	６．最初と最後の頁 213～226
掲載論文のDOI（デジタルオブジェクト識別子） 10.15803/ijnc.10.2_213	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Soe Yan Naung, Yaokai Feng, Santosa Paulus Insap, Hartanto Rudy, Kouichi Sakurai	４．巻 20(16)
２．論文標題 Machine Learning-Based IoT-Botnet Attack Detection with Sequential Architecture	５．発行年 2020年
３．雑誌名 Sensors	６．最初と最後の頁 1-15
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/s20164372	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Yan Naung Soe, Yaokai Feng, Paulus Insap Santosa, Rudy Hartanto, Kouichi Sakurai	4．巻 2019
2．論文標題 A Sequential Scheme for Detecting Cyber Attacks in IoT Environment	5．発行年 2019年
3．雑誌名 Proc. the 4th IEEE Cyber Science and Technology Congress	6．最初と最後の頁 238-244
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00051	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Hao Zhao, Yaokai Feng, Hiroshi Koide, Kouichi Sakurai	4．巻 2019
2．論文標題 An ANN Based Sequential Detection Method for Balancing Performance Indicators of IDS	5．発行年 2019年
3．雑誌名 Proc the 7th International Symposium on Computing and Networking	6．最初と最後の頁 239-244
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CANDAR.2019.00039	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Yan Naung Soe, Yaokai Feng, Paulus Insap Santosa, Rudy Hartanto, Kouichi Sakurai	4．巻 2019
2．論文標題 Rule Generation for Signature Based Detection Systems of Cyber Attacks for IoT Environments	5．発行年 2019年
3．雑誌名 MiniCandar2019	6．最初と最後の頁 1-6
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Soe Yan Naung, Yaokai Feng, Santosa Paulus Insap, Hartanto Rudy, Kouichi Sakurai	4．巻 2019
2．論文標題 Implementing Lightweight IoT-IDS on Raspberry Pi Using Correlation-Based Feature Selection and Its Performance Evaluation	5．発行年 2019年
3．雑誌名 Proc. the 33rd International Conference on Advanced Information Networking and Applications	6．最初と最後の頁 458～469
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-15032-7_39	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Ryousuke Komiya, Yaokai Feng, Kouichi Sakurai	4．巻 2018
2．論文標題 Detecting Distributed Cyber Attacks in SDN Based on Automatic Thresholding	5．発行年 2018年
3．雑誌名 Proc. the 6th International Symposium on Computing and Networking	6．最初と最後の頁 417-423
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CANDARW.2018.00083	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Yaokai Feng, Hitoshi Akiyama, Liang Lu, Kouichi Sakurai	4．巻 2018
2．論文標題 Feature Selection for Machine Learning-Based Early Detection of Distributed Cyber Attacks	5．発行年 2018年
3．雑誌名 Proc. the 4th IEEE Cyber Science and Technology Conference	6．最初と最後の頁 173-180
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00040	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計5件（うち招待講演　0件／うち国際学会　0件）

1．発表者名 XiaoJuan Cai, Yaokai Feng, Kouichi Sakurai
2．発表標題 Performance Investigation of An Intrusion Detection System Based on Sequential Artificial Neural Network Classifiers
3．学会等名 Information Processing Society of Japan
4．発表年 2021年

1．発表者名 Yan Naung Soe, Yaokai Feng, Paulus Insap Santosa, Rudy Hartanto, Kouichi Sakurai
2．発表標題 Rule Generation for Signature Based Detection Systems of Cyber Attacks for IoT Environments
3．学会等名 The 9th International Workshop on Networking, Computing, Systems, and Software (NCSS-9)
4．発表年 2019年

１．発表者名
秋山仁志、Yaokai Feng、櫻井幸一

２．発表標題
異なる機械学習アルゴリズムと4つの特徴選択法によるDDoS攻撃検出のパフォーマンス比較

３．学会等名
火の国シンポジウム2020

４．発表年
2020年

１．発表者名
Hao Zhao、小出 洋、Yaokai Feng、櫻井 幸一

２．発表標題
U2RおよびR2L攻撃の効率的な検出に向けて

３．学会等名
火の国情報シンポジウム2019

４．発表年
2019年

１．発表者名
Longjian Ye、小出 洋、Yaokai Feng、櫻井 幸一

２．発表標題
分散XML処理をための複数経路を用いたルーティングアルゴリズムの提案と評価

３．学会等名
火の国情報シンポジウム2019

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	櫻井　幸一 (Sakurai Kouichi) (60264066)	九州大学・システム情報科学研究院・教授 (17102)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関			
インドネシア	Universitas Gadjah Mada			