ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ «ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

МАРТОВИЦЬКОГО ВІТАЛІЯ ОЛЕКСАНДРОВИЧА

УДК 004.056.53

ДИСЕРТАЦІЯ
МОДЕЛІ ТА МЕТОД ВИЯВЛЕННЯ АНОМАЛІЙ ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ НА ОСНОВІ ТЕХНОЛОГІЇ МАШИННОГО НАВЧАННЯ

05.13.05 – комп'ютерні системи та компоненти
12 – Інформаційні технології
Подається на здобуття
наукового ступеня кандидата наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____В.О. Мартовицький

Науковий керівник
Рубан Ігор Вікторович, доктор технічних наук, професор

Харків –2019

АНОТАЦІЯ

Мартовицький В.О. Моделі та метод виявлення аномалій функціонування комп'ютерних систем на основі технології машинного навчання. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 «Комп'ютерні системи та компоненти». – Харківський національний університет радіоелектроніки, Міністерство освіти і науки України, Харків, 2019. У дисертаційній роботі вирішена актуальна наукова задача покращення показників виявлення аномалій функціонування РКС в умовах кібернетичних впливів зовнішнього та внутрішнього середовища шляхом побудови моделей і методів на основі технологій інтелектуального аналізу даних..

Об'єктом дослідження є процес моніторингу стану інформаційного та комунікаційного середовища розподілених комп'ютерних систем, предметом дослідження є методи і алгоритми моніторингу в розподілених комп'ютерних системах із застосуванням технологій інтелектуального аналізу даних.

Методи дослідження основані на використанні теорії множин – для розробки моделі функціонування розподілених комп'ютерних систем на основі клієнт-серверної архітектури, моделі мультиагентної підсистеми збору та зберігання даних, моделі моніторингу аномалій функціонування розподілених комп'ютерних систем; загальна теорія систем – для дослідження та розробки протоколу взаємодії агентів моніторингу в розподілених комп'ютерних системах.

Практична значимість отриманих теоретичних результатів дисертаційної роботи підтверджено ефективністю запропонованої моделі тільки для виявлення аномального поведінки мережного трафіку на основі множини параметрів мережних з'єднань , що реалізується шляхом аналізу

вхідного трафіку за допомогою ансамблю класифікаторів. Зокрема, практичне вирішення теоретичних досліджень полягає у наступному.

Запропонована методика моніторингу, яка визначає умови і порядок оцінки стану РКС за допомогою розробленої мультиагентної системи моніторингу.

Запропоновано архітектура системи моніторингу з використанням автономних програмних агентів. Архітектура передбачає динамічне формування ієрархічної структури, вузлом якої може виступати будь-яка сутність, що визначається джерелом даних або сенсором. Таким чином, стосовно моніторингу РКС можуть існувати метрики грід, кластерів, обчислювальних вузлів і завдань та інші.

Для взаємодії між усіма агентами пропонується використовувати групу інтелектуальних агентів запиту метою яких є координація агентів збору інформації, реструктуризація отриманої інформації і реалізація протоколів і механізмів передачі повідомлень між усіма агентами моделі.

Агенти моніторингу можна розділити на такі групи:

– агент комутатора і мережевий агент, які забезпечують збір даних з перших двох рівнів моделі OSI.

– агент сеансу, який забезпечує збір інформації про ім'я користувача, ім'я термінальної лінії, астрономічний час початку сеансу та інше.

– агент додатка, який відповідає за збір даних від різних додатків специфічних для тієї чи іншої інформаційно-обчислювальної системи.

– агенти запиту мета яких є обробка запитів на вибірку даних від користувачів системи збору, координація інших агентів для збору необхідної інформації, а також реструктуризація отриманої інформації для зберігання статистичний даних про систему в цілому.

Застосування таких агентів і програмна реалізація стандартизованих інтерфейсів взаємодії між ними дозволяють використовувати спільно на різних рівнях програмне забезпечення незалежних розробників. Наприклад, сенсорами можуть виступати файли даних. Але, всі сенсори формують єдину

структуру метрик, однаково доступну різним компонентам системи моніторингу.

Таким чином, побудована за даною архітектурою система моніторингу може працювати паралельно з уже розгорнутими засобами моніторингу, заміщаючи їх на деяких рівнях, що дозволяє змінювати і розширювати набір доступних функцій цих систем.

Результати дисертаційної роботи впроваджено у державному підприємстві «Центральне конструкторське бюро «ПРОТОН»», м. Харків (акт від 30.05.18) та Харківському національному університеті радіоелектроніки, кафедра електронних обчислювальних машин, м. Харків в процесі проведення лекційних занять і лабораторних робіт з курсу «Технології виявлення загроз в комп'ютерних мережах».

Матеріали дисертації достатньо повно викладені у 13 роботах: з них 6 статей у виданнях, які зазначені в переліку фахових видань України з технічних наук [1-6] (всі праці входять до науково-метричних баз, 2 – до бази Scopus) та 7 тез доповідей міжнародних конференцій [7-13] (1 – до бази Scopus).

Ключові слова: розподілені комп'ютерні системи, моніторинг, аномалії, машинне навчання, методи виявлення аномалій, мультиагентні системи.

Список публікацій здобувача:

1. Мартовицький В. О. Класифікація методів виявлення аномалій в інформаційних системах / В. О. Мартовицький, І. В. Рубан, С. О. Партика. // Системи озброєння і військова техніка. – 2016. – №3. – С. 100–105.

2. Martovytskyi V. Designing a monitoring model for cluster super-computer / V. Martovytskyi, I. Ruban, N. Lukova-Chuiko. // Eastern-European Journal of Enterprise Technologies. - 2016. - №84. - Pp. 32-37.

3. Martovytskyi V. Approach to Classifying the State of a Network Based on Statistical Parameters for Detecting Anomalies in the Information Structure of a Computing System / V. Martovytskyi, I. Ruban, N. Lukova-Chuiko. // Cybernetics and Systems Analysis. - 2018. - №54. - Pp. 302-309.

4. Мартовицкий В. Модель мультиагентной системы сбора и хранения информации / В. Мартовицкий, И. Рубан. // Системы управления, навигации и связи. - 2017. - №6. - С. 150-153.

5. Відбір параметрів моніторингу мережної інфраструктури для класифікації стану мережі / В. О.Мартовицький, І. В. Рубан, О. В. Сєвєрінов, О. В. Бологова. // Сучасні інформаційні системи. – 2018. – №4. – С. 5–10.

6. Мартовицький В. О. Створення крос-платформної системи захисту Web-сервісів і додатків на основі XML-файлів для технології ASP. NET / В. О. Мартовицький, Л. Л. Колодочкин. // Системи озброєння і військова техніка. – 2015. – №2. – С. 122–123.

7. Мартовицкий В. А. Анализ современных сканеров уязвимостей / В. А. Мартовицкий, И. О. Тимофеев. // Міжнародна наукова інтернет-конференція" Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення. – 2017. – №23 – С. 28–30.

8. Мартовицкий В.А. Критерии обнаружения угроз безопасности по цели сетевого воздействия // II Міжнародна науково-практична конференція "Інформаційна безпека та комп’ютерні технології", 20-22 квітня 2017 року. – Кропивницький: ЦНТУ, 2017– С. 60–61.

9. Мартовицький В.О. Модель мультиагентної системи збору і зберігання інформації / В.О. Мартовицький, Я.В. Дух // Проблеми інформатизації тези доповідей п’ятої міжнародної науково-технічної конференції, 13 – 15 листопада 2017 року– С. 48.

10. Мартовицький В.О. Модифікація алгоритму узагальненого стекінгу / В.О. Мартовицький, Н.О. Запорожець // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління матеріали шостої міжнародної науково-технічної конференції, 26 – 27 квітня 2018 року

11. Мартовицький В.О. Модель системи моніторингу мережної інфраструктури / В.О. Мартовицький, І. В. Рубан // Друга міжнародна науково-технічна конференція «Комп’ютерні та інформаційні системи і технології». Збірка наукових праць. Харків: ХНУРЕ. 2018– С. 18–20.

12. Мартовицький В.О. Виявлення шкідливого програмного коду з використанням методів машинного навчання/ В.О. Мартовицький, В.О. Шандула, Є.Ю. Кортяк // Проблеми інформатизації тези доповідей шостої міжнародної науково-технічної конференції, 14 – 16 листопада 2018 року– С. 14.

13. Martovytskyi V. Investigation of network infrastructure control parameters for effective intellectual analysis / V. Martovytskyi, K. Smelyakov, D. Pribylnov, A. Chupryna // IEEE 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 20-24 Feb. 2018. – P. 983-986. DOI: 10.1109/TCSET.2018.8336359

ABSTRACT

Martovytskyy VA Models and method for detecting computer system anomalies based on machine learning technology. - Qualified scientific work on the rights of the manuscript. Thesis for a Candidate Degree in Engineering, specialty 05.13.05 “Computer Systems and Components”. - Kharkiv National University of Radio Electronics, Ministry of Education and Science of Ukraine, Kharkiv, 2019. The dissertation deals with the actual scientific task of improving the detection of anomalies of functioning of RKS in the conditions of cybernetic influences of external and internal environment by constructing models and methods based on the analysis of data technologies.

The object of the study is the process of monitoring the state of information and communication environment of distributed computer systems, the subject of research is the methods and algorithms of monitoring in distributed computer systems using data mining technologies.

Research methods are based on the use of set theory - to develop a model of functioning of distributed computer systems based on client-server architecture, model of multiagent subsystem of collecting and storage of data, models of monitoring anomalies of functioning of distributed computer systems; general systems theory - for research and development of the protocol of interaction of monitoring agents in distributed computer systems.

The practical significance of the obtained theoretical results of the dissertation is confirmed by the effectiveness of the proposed model only for the detection of anomalous behavior of network traffic based on a set of network connection parameters, which is realized by analyzing the inbound traffic using an ensemble of classifiers. In particular, the practical solution to theoretical studies is as follows.

A monitoring technique is proposed that defines the conditions and procedure for assessing the status of RCCs using the developed multi-agent monitoring system.

The architecture of the monitoring system using autonomous software agents is proposed. Architecture involves the dynamic formation of a hierarchical structure, the node of which can be any entity defined by the data source or sensor. Thus, metrics of grids, clusters, computing nodes and tasks, and others, may exist with respect to RCC monitoring.

For the interaction between all agents, it is proposed to use a group of intelligent inquiry agents to coordinate information collection agents, restructure the information received, and implement protocols and message mechanisms between all agents of the model.

Monitoring agents can be divided into the following groups:

– is a switch agent and network agent that collects data from the first two levels of the OSI model.

– is a session agent that collects information about a user name, terminal name, astronomical start time, and more.

– is an application agent responsible for collecting data from various applications specific to a particular computer system.

– - query agents whose purpose is to process queries for data collection from users of the collection system, coordinate other agents to collect the necessary information, as well as restructure the information obtained to store statistics about the system as a whole.

The use of such agents and the software implementation of standardized interfaces between them allow the use of third-party software at different levels. For example, sensors can act as data files. However, all sensors form a single metric structure that is equally accessible to different components of the monitoring system.

Thus, a monitoring system built on this architecture can work in parallel with already deployed monitoring tools, replacing them at some levels, which allows to change and extend the range of available functions of these systems.

The results of the dissertation were implemented at the State Enterprise "Central Design Bureau" PROTON ", Kharkiv (act dated 30.05.18) and Kharkiv

National University of Radio Electronics, Department of Electronic Computing Machines, Kharkiv in the course of conducting lectures and laboratory work on the course "Threat detection technologies in computer networks".

The materials of the dissertation are quite sufficiently presented in 13 papers: 6 of them are articles in the editions that are listed in the list of professional editions of Ukraine in technical sciences [1-6] (all works are included in scientific-metric bases, 2 - in Scopus base) and 7 theses international conference reports [7-13] (1 to Scopus database).

Keywords: distributed computer systems, monitoring, anomalies, machine learning, anomaly detection methods, multi-agent systems.

List of references*:*

1. Martovytskyi V. O. Klasyfikatsiia metodiv vyiavlennia anomalii v informatsiinykh systemakh / V. O. Martovytskyi, I. V. Ruban, S. O. Partyka. // Systemy ozbroiennia i viiskova tekhnika. – 2016. – №3. – S. 100–105.

2. Martovytskyi V. Designing a monitoring model for cluster super-computer / V. Martovytskyi, I. Ruban, N. Lukova-Chuiko. // Eastern-European Journal of Enterprise Technologies. - 2016. - №84. - Pp. 32-37.

3. Martovytskyi V. Approach to Classifying the State of a Network Based on Statistical Parameters for Detecting Anomalies in the Information Structure of a Computing System / V. Martovytskyi, I. Ruban, N. Lukova-Chuiko. // Cybernetics and Systems Analysis. - 2018. - №54. - Pp. 302-309.

4. Martovytskyi V. Model multyahentnoi systemi sbora y khranenyia ynformatsyy / V. Martovytskyi, Y. Ruban. // Systemi upravlenyia, navyhatsyy y sviazy. - 2017. - №6. - S. 150-153.

5. Vidbir parametriv monitorynhu merezhnoi infrastruktury dlia klasyfikatsii stanu merezhi / V. O.Martovytskyi, I. V. Ruban, O. V. Sievierinov, O. V. Bolohova. // Suchasni informatsiini systemy. – 2018. – №4. – S. 5–10.

6. Martovytskyi V. O. Stvorennia kros-platformnoi systemy zakhystu Web-servisiv i dodatkiv na osnovi XML-failiv dlia tekhnolohii ASP. NET / V. O.

Martovytskyi, L. L. Kolodochkyn. // Systemy ozbroiennia i viiskova tekhnika. – 2015. – №2. – S. 122–123.

7. Martovitskiy V. A. Analiz sovremennyih skanerov uyazvimostey / V. A. Martovitskiy, I. O. Timofeev. // MIzhnarodna naukova Internet-konferentsIya" InformatsIyne suspIlstvo: tehnologIchnI, ekonomIchnI ta tehnIchnI aspekti stanovlennya. – 2017. – №23.

8. Martovitskiy V.A. Kriterii obnaruzheniya ugroz bezopasnosti po tseli setevogo vozdeystviya // II MIzhnarodna naukovo-praktichna konferentsIya "InformatsIyna bezpeka ta komp'yuternI tehnologIYi", 20-22 kvItnya 2017 roku. – Kropivnitskiy: TsNTU, 2017.

9. Martovitskiy V.O. Model multiagentnoYi sistemi zboru I zberIgannya InformatsIYi / V.O. Martovitskiy, Ya.V. Duh // Problemi InformatizatsIYi tezi dopovIdey p'yatoYi mIzhnarodnoYi naukovo-tehnIchnoYi konferentsIYi, 13 – 15 listopada 2017 roku

10. Martovitskiy V.O. ModifIkatsIya algoritmu uzagalnenogo stekIngu / V.O. Martovitskiy, N.O. Zaporozhets // SuchasnI napryami rozvitku InformatsIyno-komunIkatsIynih tehnologIy ta zasobIv upravlInnya materIali shostoYi mIzhnarodnoYi naukovo-tehnIchnoYi konferentsIYi, 26 – 27 kvItnya 2018 roku

11. Martovitskiy V.O. Model sistemi monItoringu merezhnoYi Infrastrukturi / V.O. Martovitskiy, I. V. Ruban // Druga mIzhnarodna naukovo-tehnIchna konferentsIya «Komp'yuternI ta InformatsIynI sistemi I tehnologIYi». ZbIrka naukovih prats. HarkIv: HNURE. 2018.

12. Martovitskiy V.O. Viyavlennya shkIdlivogo programnogo kodu z vikoristannyam metodIv mashinnogo navchannya/ V.O. Martovitskiy, V.O. Shandula, E.Yu. Kortyak // Problemi InformatizatsIYi tezi dopovIdey shostoYi mIzhnarodnoYi naukovo-tehnIchnoYi konferentsIYi, 14 – 16 listopada 2017 roku

13. Martovytskyi V. Investigation of network infrastructure control parameters for effective intellectual analysis / V. Martovytskyi, K. Smelyakov, D. Pribylnov, A. Chupryna // IEEE 14th International Conference on Advanced

Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 20-24 Feb. 2018. – P. 983-986. DOI: 10.1109/TCSET.2018.8336359

ЗМІСТ