

Міністерство освіти і науки України
Харківський національний автомобільно-дорожній університет



«КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ І МЕХАТРОНІКА»

(30 травня 2019 р.)

ЗБІРНИК НАУКОВИХ ПРАЦЬ
ЗА МАТЕРІАЛАМИ МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ
КОНФЕРЕНЦІЇ

Харків,

2019

УДК 004:629:656:658

Комп'ютерні технології і мехатроніка. Збірник наукових праць за матеріалами міжнародної науково-практичної конференції. – Харків, ХНАДУ, 2019. – 282 с.

Збірник містить результати теоретичних та практичних наукових досліджень та розробок, які були виконані науково-педагогічними працівниками вищої школи, науковими співробітниками, докторантами, аспірантами, магістрантами, студентами та фахівцями різних організацій і підприємств.

Для викладачів, наукових працівників, докторантів, аспірантів, магістрантів, студентів, фахівців.

Матеріали доповідей конференції відтворено з авторських оригіналів

Конференцію проведено згідно з планом проведення міжнародних, всеукраїнських науково-практичних і науково-методичних конференцій і семінарів Харківського національного автомобільно-дорожнього університету у 2019 р. (посвідчення УкрІНТЕІ № 666 від 20 грудня 2018 р.)

© ХНАДУ, 2019

УДК 004

**РОЗРОБКА ЗАСОБІВ ВИЗНАЧЕННЯ КОМП'ЮТЕРНИХ АТАК НА
ОСНОВІ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ****Черняк Т.О., асистент кафедри прикладної математики та інформатики,****ДонНТУ****Хоронько Д.С., магістрант, ДонНТУ**

Актуальність дослідження полягає в тому, що останнім часом поряд з удосконаленням корпоративних і відомчих мереж збільшується і ризик реалізації різних типів загроз їхній безпеці. У зв'язку з цим системи виявлення вторгнень (СВВ), крім миттєвого виявлення атак, повинні надавати всі можливі дані про хост, що атакується, і задовольняти цілому набору жорстких вимог. Сьогодні з'являється величезна кількість нових методів ініціювання атак, при цьому формуються нові вимоги до таких методів, тому потрібні більш ефективні підходи до розробки СВВ. Спостерігається широке розповсюдження інструментів в сучасних СВВ, що аналізують відомі сигнатури, в цілому демонструють високу продуктивність, але не здатні виявити невідому атаку.

Предметом дослідження є захист інформаційної системи від комп'ютерних атак з використанням нейронних мереж.

Об'єктом дослідження є принципи аналізу мережевого трафіку та побудови нейронної мережі, що аналізує трафік з метою виявлення мережевої атаки.

Наукова новизна роботи полягає в тому, що для виявлення комп'ютерних атак запропоноване використання багат шарового перцептронну, а також те, що експериментальні випробування здійснювалися на випробуваний базі даних KDD Cup1999 Data.

Метою роботи є розробка системи виявлення комп'ютерних атак на основі аналізу мережевого трафіку за допомогою нейронної мережі.

Комп'ютерні атаки – це реальна та зростаюча загроза, з якою стикаються компанії в усьому світі. Зазначені атаки реалізуються великою кількістю програмних агентів, розміщених на хостах, які зловмисник скомпрометував раніше. Реалізація цих атак може привести не тільки до виходу з ладу окремих хостів і служб, а й зупинити роботу корневих DNS-серверів і викликати часткове/повне припинення роботи мережі Інтернет. У зв'язку з критичністю та нетривіальністю даного класу атак, побудова ефективних засобів захисту від них являє собою складну науково-технічну проблему. Захист на рівні маршрутизаторів (наприклад, від DDoS-атак) вже досить успішно реалізували компанії Cisco Systems і Arbor Networks, але в цілому порушена проблема атак на сьогоднішній день, як і раніше, стоїть дуже гостро для більшості компаній.

Необхідно зазначити, що існує досить багато різних видів атак на відмову, кожна з яких використовує певну особливість побудови мережі або уразливості програмного забезпечення. Наприклад, атаки можуть здійснюватися шляхом безпосередньої пересилки великої кількості пакетів, використання проміжних вузлів, передачі занадто довгих, некоректних пакетів або великої кількості трудомістких запитів. З останніх тенденцій можна відзначити появу атак погіршення якості та низькочастотних атак і, безумовно, цей процес буде тривати, вимагаючи нових досліджень і розробки нових методів протидії.

Для успішного функціонування системи захисту від атак на відмову надзвичайно важливо виділити безліч припущень про систему, яка підлягає захисту. Очевидно, що захист систем різного типу повинен бути побудований на основі різних принципів, з урахуванням типових характеристик, класів атак, що спрямовані проти систем вказаного типу, вимог до функціонування систем захисту. Як правило, ці припущення стосуються нормальної роботи системи, що підлягає захисту. Виділення наведених емпіричних характеристик істотно полегшує процес виявлення атак за умови збереження їх відповідності реальному стану системи.

Слід відмітити також кілька базових припущень, що використовуються в усіх системах захисту. Перше з них полягає в тому, що атаки взаємопов'язані з незвичайним використанням системи, тому їхні дії істотно відрізняються від типової роботи.

Проаналізувавши вимоги, які пред'являються до систем виявлення мережових атак на підставі аналізу мережевого трафіку, були сформульовані вимоги до розроблюваної системи: система повинна вчитися на «хорошому» трафіку; враховувати IP-адресу, з якої йде запит; враховувати кількість запитів з однієї IP-адреси; враховувати країну-джерело запиту; враховувати метод запиту; враховувати адреси підмережі; визначати сторінку входу на сайт, тип браузера, тип операційної системи.

В межах даної роботи передбачений нейромережевий аналіз мережевого трафіку. У зв'язку з цим в роботі необхідно вирішити такі завдання: визначити тип нейронної мережі, яка буде найбільш ефективною для здійснення подальшого аналізу; визначити основні характеристики нейронної мережі – кількість нейронів вхідного шару, кількість прихованих шарів, кількість нейронів в прихованих шарах, кількість нейронів вихідного шару; визначити тип навчання; визначити вихідні дані для проведення аналізу; визначити середу побудови нейронної мережі; виконати побудову мережі та виконати процедуру її навчання; проаналізувати отриману вибірку.

Висновки. В подальшому, для виявлення мережових атак, планується використання засобів, що базуються на застосуванні методів штучного інтелекту – нейронних мереж. Нейронні мережі здатні до навчання та класифікації. Мережі, навчені на обмеженому обсязі даних, показують хороші результати виявлення різних типів мережових атак. Визначення мережових атак системи виконується шляхом аналізу мережевого трафіку та надалі приймається рішення про можливу наявну загрозу.

Література: 1. Дасгупта Д. Искусственные иммунные системы и их применение / Д. Дасгупта. – Москва : ФИЗМАТЛИТ, 2006. – 344 с. 2. Гаценко О.Ю. Защита информации. Основы организационного управления / О.Ю. Гаценко. – Санкт-Петербург : Сентябрь, 2001. – 228 с.

ЗМІСТ

Даниленко О.Ф., Скородєлов В.В., Черних О.П., Ягнюков С.Ю. Використання програмованих логічних інтегральних схем для реалізації протоколів передачі даних через Інтернет	3
Senouci S.M., Nikonov O.Ya., Shulyakov V.M., Nikonov D.O. Technologies d'information pour vehicules intelligents	5
Примаченко Г.О., Богомаз Д.М., Колісник Д.В. Впровадження сучасних інформаційно-комунікаційних технологій у логістичних системах	8
Грицук І. В, Погорлецький Д. С, Симоненко Р. В, Володарець М. В, Худяков І. В. Вимірювальний комплекс для дослідження роботи транспортного засобу з двигуном, обладнаним системою впорскування газового палива, в умовах експлуатації засобами ITS	11
Nikitina K.A. Partial differential equations model for modular conveyors controlling	15
Півнева О.А., Мнушка О.В. Проблема безпеки та аналіз типових загроз для інфраструктури Інтернету речей	18
Клец Д.М., Ніконов О.Я., Дроздик Є.В., Тимченко С.С. Розроблення інформаційної системи з технологією інтерактивної візуалізації засобами доповненої реальності	21
Ломотько Д. В. Проблеми нормативно-правового регулювання мультимодальних пасажирських перевезень за участю залізничного транспорту	24
Бєлов В. І., Дитятьєв О. В. Дуальна освіта, як форма інтеграції науки, освіти та виробництва	26
Шульдінер Ю.В., Зеленський Д.В., Шиян С.П., Угрін В.В. Впровадження GPS–систем спостереження при транспортуванні вантажів різними видами транспорту	29
Mnushka O.V., Savchenko V.M. Architecture models and patterns for safety and security for IOT applications	30
Грицук І.В., Волков В.П., Грицук Ю.В., Волков Ю.В. Використання інформаційних баз даних на автомобільному транспорті	34
Наглюк М.І., Ковтуненко В.В. Прилад для вимірювання електропровідності рідин, що застосовуються в автомобілях	37
Tkachenko M. STM32-based HMI solution for IOT application	39
Ломотько Д.В., Лаліменко М.А. Павленко І.А. Шляхи забезпечення інтероперабельності при створенні логістичних ланцюгів за участю залізниць	42
Кулик М.М., Ширін В.В. Проблеми та перспективи розвитку велосипедної інфраструктури в містах України	45

Мармут І.А. Структура і принцип роботи електронної моделі стенду при вимірюванні діагностичних параметрів гальмівної системи автомобіля	48
Khamza I.S., Mnushka O.V. Actual problems and perspectives of autonomous vehicles	51
Дитяцьєв О.В., Белов В.І. Про тестові впливи при діагностуванні підвіски автомобіля	54
Черняк Т.О., Хоронєко Д.С. Розробка засобів визначення комп'ютерних атак на основі аналізу мережевого трафіку	57
Ніконов О.Я., Іващенко М.О., Полосухіна Т.О., Железко Б.О. Розроблення інтелектуальної бортової інформаційної системи безпілотного транспортного засобу на основі фази-архітектури	60
Буцько Т.В., Ломотько Д.В., Арсененко Д. В. Управління процесом забезпечення залізничним рухомим складом при перевезенні зернових вантажів	63
Назаров О.І. Впровадження результатів передової світової практики викладання дисциплін у галузі ІТ-технологій	66
Шевченко В.О., Кудін А.І. Використання дистанційних курсів на базі moodle при викладанні дисциплін студентам денної форми навчання	69
Ломотько Д.В., Вовків А.Т. Удосконалення інформаційної взаємодії залізничних під'їзних колій шляхом впровадження логістичних технологій	73
Волков В.П., Грицук І.В., Волкова Т.В. Інформаційна система моніторингу технічного стану автомобіля в умовах ITS	77
Гулага Я.С., Мнушка О.В. Критерії оцінки якості в проектах, що використовують Agile	82
Фастовець В.І., Шуляков В.М., Мороз О.О. Використання генетичних алгоритмів для самовдосконалення елементів дизайну сайтів	85
Ткачук О.Ю. Розрахункові-логічні системи для управління КА	90
Мізяк І.О., Тімонін В.О. Система бездротової передачі даних між автомобілем та світлофором	92
Семченко Н.О., Решетніков Є.Б. Моделювання параметрів транспортних потоків у автоматизованих системах управління дорожнім рухом	95
Абрамова Л.С., Харченко Т.В., Безбородов Д.І. Підхід до визначення безпеки руху на транспортному вузлі міста	98
Ткачук О.Ю. Впровадження інформаційно-комунікаційних технологій на транспорті	102

Колеснікова Н.В. Використання комп'ютера для побудови графіків на заняттях з математики	105
Лебединський А.В., Янушкевич С.Д. Оцінка точності апроксимації нестационарних сигналів емпіричними модами Гільберта-Хуанга	109
Кривошапов С.І. Бортова система реєстрації витрати палива та умов експлуатації автомобіля	112
Коваль О. А., Коваль А. О., Петрукович Д. Є. Підвищення точності та достовірності вимірювання відстані автомобіля до перешкод	115
Нижников А., Маций О. Б. Применение технологии WEBGL для разработки интерактивного веб-приложения	118
Оксанич І. Г. Розвиток методу верифікації оціночних показників для їх використання у якості критерію оптимізації	122
Котенко Б.О., Мнушка О.В. Об'єктно-орієнтований підхід до дизайну навчаючих програм	125
Ніконов О.Я., Полосухіна Т.О., Семергей А.М. Технічні аспекти автоматичного керування наземними безпілотними транспортними засобами	127
Тимонин В.А., Пономарев А.Е. Алгоритм функционирования системы предупреждения столкновений на участках дорог с ограниченной видимостью.	130
Пронин С.В. Инструменты для разработки искусственных агентов в сфере транспортной логистики	133
Сільченко В.Р. Автоматизована система діагностування зернових культур за допомогою автономного літального апарата	139
Петренко Ю.А., Михайлова А.І. Комп'ютерна технологія моніторингу якості води на технічному водоймищі автотранспортного підприємства	142
Тимонин В.А. Использование технологии A-GPS для определения местоположения движущихся объектов	145
Тиричева О.А., Репін І.О. Дослідження впливу масштабування на ефективність роботи локальної мережі	149
Шапошнікова О.П. Прием та обробка інформації про місце знаходження транспорту для мобільного додатку «Мій транспорт»	153
Поперешняк С.В. Оцінка якості послідовностей псевдовипадкових чисел	157
Маций О. Б., Наумов В.С. Паросполучення в моделях транспортної логістики	160
Тимонин В.А., Калинин А.А. Обзор технологий передачи данных в системах коммуникации автомобилей	163
Пономарьов В.В., Ширін В.В. Аналіз досвіду оцінки транспортної	169

доступності інфраструктури сучасних міст

Левченко О.С., Холодова О.О., Потапенко А.І. Необхідність вибору оптимальних технічних периферійних засобів автоматизованих систем керування дорожнім рухом	172
Matsiy M. E., Alekseyev O. P., Jörg P. Interactive monitoring, as effective management of the state of transport communications	175
Борзенко О.П. ІТ-технології як важіль підвищення ефективності процесу викладання іноземної мови	178
Венгер А. С., Степанов О. В., Волобуєва Т. В., Міжнародний досвід використання інтелектуальних транспортних систем	181
Пімонов І.Г., Рукавішніков Ю.В. Створення логістичного підходу при конструюванні та експлуатації будівельно-дорожніх машин	184
Зибцев Ю.В. Перевірка тягово-швидкісних властивостей колісних машин у дорожніх умовах	186
Oleynyk Y.S. Discrete event model of the movement of a batch of subjects of labour on technological route	189
Тимонин В.А., Луговой А.Б. Обзор методов и алгоритмов определения скорости транспортных средств по данным видеоаналитики	193
Пронин С.В., Жученко О.О. Огляд бібліотек комп'ютерного зору	197
Sholominska L. S., Storchak M. O. Software engineering education at university	201
Пронин С.В., Луговой А.А., Есмагамбетов Б.-Б.С. Использование мультиагентных систем в транспортной логистике	203
Книщенко А.О. Мехатронна система керування гідроприводом мобільного підйомника	206
Аль-Дара Є.Н., Мойсеєв В.Ю. Автоматизована система моніторингу стану хворого на прикладі моніторингу пульсу	209
Костікова М. В., Скрипіна І. В. Аналіз досвіду використання платформи Futurelearn для інтеграції масових відкритих онлайн-курсів в систему навчання	212
Біньковська А.Б., Нефьодов Л.І. Інформаційна технологія синтезу територіально-просторово-розподіленої комп'ютерної мережі офісів транспортних систем	214
Yefimenko O.V., Pluhin D.A. Designing the structure of intelligent control system in construction and road machines	217
Шевченко В.О., Онишко І.В. Особливості використання Microsoft Excel для обробки великих масивів даних	220
Байдун В.В., Мнушка О.В. Засоби забезпечення безпеки даних в Інтернеті речей	223

Плугіна Т.В., Мураховський В.К. Інтенсифікація систем обробки інформації робочих параметрів будівельно-дорожніх машин	226
Плугіна Т.В., Мірошник В.А. Інтелектуальна система управління конвеєром	229
Плугіна Т.В., Колесніков В.С., Дудко Д.В. Управління приводом робочого органу машини як кіберфізичною системою	232
Плугіна Т.В., Кириченко Ю.В. Модель мехатронної системи управління виконавчими пристроями вантажно-розвантажувальної машини з GPS-інтенсифікатором	234
Горбик Ю.В. Аналіз направлений для підвищення екологічної безпеки автомобілей	237
Подолька О.А., Подолька А.Н., Новак І.В. Оптимізація транспортних перевозок в умовах ризику	241
Лабенко Д.П. ГІС як інструмент розв'язання транспортних задач	244
Скворчевський О.Є. Нове покоління гідравлічних приводів для мобільних машин на основі принципу e-LOAD SENSING (e-LS)	247
Подолька О.А., Подолька А.Н., Панов Е.В. Нормалізація критеріїв многокритеріальних задач транспортного типу на основі блочної сортировки	249
Чорний Б.С., Кононіхін О.С. Автоматизація процесу підбору персоналу	252
Ільге І.Г., Вагін Д.О. Модель вибору САУ асфальтоукладача	254
Кудін А. І., Жульєв Д.Н. Розвиток інформаційних технологій та їх вплив на майбутнє людства	257
Вітер Д.О., Кононіхін О.С. Вибір засобів комунікації співробітників розподіленого офісу	260
Чепусенко Є.О., Сахацький В.Д. Випромінювач комп'ютеризованої системи визначення координат проколюючої головки при безтраншейній прокладці трас підземних комунікацій	263
Згонник О.Є., Кононіхін О.С. Вибір апаратно-програмного забезпечення інформаційної системи контролю руху транспорту	266
Ільге І.Г., Мереха Р.Ю. Модель вибору елементної бази САУ робочими органами бульдозера	268
Шмойлов А.Ю., Кононіхін О.С. Впровадження системи супутникового моніторингу в дорожньо-будівельній організації	270
Рябушенко О.В., Краснов Ю.О. Дослідження впливу геометрії перехрестя на величину потоку насичення	272

НАУКОВЕ ВИДАННЯ

**ЗБІРНИК НАУКОВИХ ПРАЦЬ ЗА МАТЕРІАЛАМИ МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ «КОМП'ЮТЕРНІ
ТЕХНОЛОГІЇ І МЕХАТРОНІКА»**

Конференцію проведено згідно з планом проведення міжнародних, всеукраїнських науково-практичних і науково-методичних конференцій і семінарів Харківського національного автомобільно-дорожнього університету у 2019 р. (посвідчення УкрІНТЕІ № 666 від 20 грудня 2018 р.)

Відповідальний за випуск д.т.н., проф. Ніконов О.Я.

Науковий редактор д.т.н., проф. Ніконов О.Я.

Технічний редактор Мнушка О.В.