УДК 004.056.53:[004.85:004.77
DOI: 10.31673/2409-7292.2024.010005

Ветлицька О. С., Треньова К. О.

ВИЯВЛЕННЯ АТАК У МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ МЕТОДАМИ МАШИННОГО НАВЧАННЯ

Зростання обсягу цифрових даних, що генеруються, зокрема, розумними пристроями інтернету речей, зробило актуальними дослідження, пов'язані із застосуванням методів машинного навчання для виявлення аномалій мережевого трафіку - наявності мережевих атак. Для цього в статті запропоновано єдиний підхід до виявлення атак на різних рівнях архітектури мережі інтернету речей, заснований на методах машинного навчання. В статті досліджено, що на рівні бездротової сенсорної мережі виявлення атаки пов'язане з виявленням аномальної поведінки пристрою інтернету речей, за якого відхилення поведінки пристрою інтернету речей від його профілю може розцінюватися як компрометація пристрою. Побудова профілів розумних пристроїв інтернету речей здійснюється на основі статистичних характеристик, таких як інтенсивність і тривалість передавання пакетів, частка ретрансльованих пакетів тощо. Досліджено, що на рівні локальної або глобальної дротової мережі інтернету речей відбувається агрегування даних, аналіз яких також виконується методами машинного навчання. Навчені класифікатори можуть стати частиною системи виявлення мережевих атак, що ухвалюють рішення про компрометацію вузла "на льоту". Розглянуто експериментальним шляхом обрані моделі класифікаторів мережевих атак як на рівні бездротової сенсорної мережі, так і на рівні локальної або глобальної дротової мережі. Найкращі результати в сенсі оцінок повноти та точності продемонстровано методом випадкового лісу для дротової локальної і (або) глобальної мережі та всіма розглянутими методами для бездротової сенсорної мережі. Практичне значення: запропоновані моделі класифікаторів можуть знайти застосування при проектуванні систем виявлення атак у мережах інтернету речей.

Ключові слова: мережева атака, інтернет речей, система виявлення атак, ефективність моделі класифікатора, IoT-пристрої.

Вступ

Мережі інтернету речей (Internet of Things - IoT) гетерогенні, мобільні, характеризуються складною динамічною структурою [1]. Ці особливості сприяють розвитку мережевих атак, спрямованих на маршрутизацію, таких як "червоточина", "збірний пункт", "викид пакетів", Сівілли, зациклення, Rush. Наслідки від дій атак багатоаспектні - від компрометації вузлів і захоплення контролю над ними до розточення енергії вузлів, що призводить до швидкої деградації мережі IoT [2, 3]. Захист від атак у мережах IoT реалізується системою виявлення атак (СОА), яка під час своєї роботи незначно збільшує навантаження на малопотужні вузли мережі - сенсорні пристрої (СУ) [4, 5]. Система виявлення атак мережі IoT має ієрархічну структуру, як і сама мережа IoT, - три компонентні рівні (рис. 1) [2].

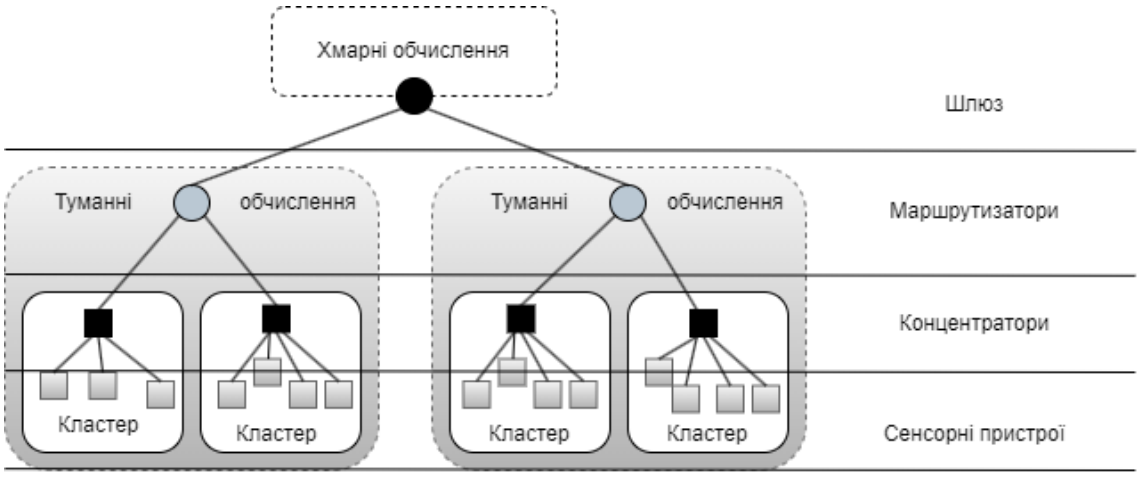

Рис. 1. Ієрархічна структура організації мереж IoT

На рівні сенсорних пристроїв розв'язують задачу виявлення аномальної поведінки, наприклад різкого збільшення інтенсивності та (або) тривалості передачі, необґрунтованого

зниження рівня залишкової енергії тощо. Аномальна поведінка може свідчити про наявність атаки на IoT-пристрій. Загальноприйнятого підходу до виявлення атак на рівні сенсорних пристроїв поки що не існує - вибір рішення залежить від багатьох причин: на яких пристроях побудована сенсорна мережа, чи є вони енергозалежними, до яких атак схильні, як довго поширюється атака тощо. Проте аналіз джерел показав окремі рішення, засновані на профілюванні IoT-пристроїв. Так, у роботі [3] продемонстровано побудову профілів розумних пристроїв інтернету речей на основі статистичних характеристик, таких як інтенсивність і тривалість передачі пакетів, частка ретрансльованих пакетів. При цьому треба враховувати, що профіль IoT-пристрою одного розробника не відповідає профілю IoT-пристрою з такими ж розумними функціями, але іншого розробника. Власне, у [3] ця обставина частково демонструється - автори опублікували у відкритому доступі навчальні вибірки для кількох розумних дверних дзвінків, кількох розумних камер (https://archive.ics.uci.edu/ml/machine-learning-databases/00442/). У роботі [4] створення профілю IoT-пристрою засноване на виявленні щільності функції розподілу обсягу переданих і прийнятих даних.

На рівні мереж - локальних (туманні обчислення) і глобальних (хмарні обчислення) - відбувається агрегування трафіку, згенерованого кількома сотнями або навіть мільйонами сенсорних пристроїв, що загалом являє собою звичайний мережевий трафік. Тому на рівні мереж завдання виявлення мережевих атак може вирішуватися відомими методами, заснованими на поведінковій моделі мережі. Принцип роботи таких методів ґрунтується на виявленні невідповідності між поточним режимом роботи мережі та штатним. Будь-яка невідповідність розглядається як атака [4, 5]. З іншого боку, поведінкова модель потребує часу для фіксації атаки - вузлові агенти спочатку збирають (накопичують) статистики поведінки і передають їх у модуль ухвалення рішення СОА. Оскільки розподілені атаки є атаками реального часу, то для їхнього розпізнавання та подальшого розвитку необхідні методи, що працюють "на льоту". У зв'язку з цим при побудові СОА в мережах інтернету речей популярності набувають методи машинного навчання.

Загалом обсяг і різнорідність даних, що генеруються інтернетом речей, наразі відносять до BigData. Аналіз BigData переважно виконують методами машинного навчання [6, 7]. За наявності навчених моделей класифікації на вході мережевого вузла рішення про нормальність/аномальність трафіку може прийматися "на льоту", на відміну, наприклад, від статистичних методів.

Мета і задачі дослідження.

Об'єктом дослідження є мережа інтернету речей, побудована за ієрархічним принципом - від бездротової сенсорної мережі до глобальної хмари.

Метою дослідження є пропозиція єдиного підходу до виявлення атак на всіх рівнях мережі IoT, заснованого на методах машинного навчання. Завданнями статті у зв’язку із визначеною метою є:

а) розглянути оцінки ефективності моделей класифікації, дослідити на основі чого приймається рішення про придатність або вибір того чи іншого методу класифікації, визначити, які критерії використовуються для оцінки ефективності алгоритмів навчання;

б) розглянути характеристику навчаючої вибірки, визначити від чого залежить ефективність класифікаторів, побудованих із застосуванням методів машинного навчання;

в) дослідити етапи запропонованого підходу до виявлення атак у мережах інтернету речей, визначити, які основні етапи включає в себе запропонований підхід для виявлення атак в мережах інтернету речей.

Результати дослідження.

Методи машинного навчання, які застосовувалися для побудови моделі детектування загроз на рівні сенсорної мережі та в агрегованому трафіку: дерево рішень; випадковий ліс; нейронна мережа прямого поширення; k-найближчих сусідів.

Основні параметри навчених класифікаторів наведено в табл. 1.

Таблиця 1

Основні параметри методів машинного навчання

Метод	Основні параметри
Дерево рішень	Відсікання гілок відбувається за показником достовірності - відношенню числа неправильно розпізнаних прикладів у листі до загального числа прикладів: $C_k = \frac{N_{nk}}{N_k}$ де N_{nk} – число нерозпізнаних прикладів k-го каса; N_k - загальна кількість прикладів k-го класу. Розщеплення відбувається за величиною найменшої інформаційної ентропії $H(x) = -\sum_{i=1}^{N} p(i) log_2 p(i)$, де x - випадкова подія з N можливими станами; p - ймовірність, що і-а ознака стане черговим вузлом дерева рішень Глибина дерева дорівнює 21
Випадковий ліс	Ансамбль складається з 10 дерев Глибина підсумкового класифікатора 15 Використані такі техніки побудови випадкового лісу: – bagging – випадкова вибірка навчальних прикладів за рівномірним законом із поверненням прикладів у вихідне навчальну множину, що дозволяє уникнути перенавчання - повного запам'ятовування всіх навчальних прикладів; – boosting – навчання слабких дерев рішень для складання їх у сильний класифікатор, при якому неправильно класифіковані приклади навчання отримують більшу вагу, а правильно класифіковані приклади втрачають вагу, що дозволяє при подальшому навчанні сфокусуватися на помилково класифікованих прикладах.
Нейронна мережа	Один прихований шар. Кількість прихованих шарів вибрано шляхом каскадного навчання при досягненні мінімального значення MSE Функція активації нейрона: $\phi(u_k + b_k) = \frac{1}{1+\exp(-\alpha(u_k+b_k}$ де α - параметр нахилу сигмоїди; u_k - зважена сума; b_k - поріг Ваги змінюються згідно локальному градієнту функції помилки
k-ближчих сусідів	*Число найближчих сусідів k = 3* Міра близькості – евклідова метрика Нормалізація параметрів методом мінімаксу: $x_i = \frac{x_i - x_{min}}{x_{max} - x_{min}}$

Оцінки ефективності моделей класифікації

Рішення про придатність або вибір того чи іншого методу класифікації приймається з урахуванням оцінки ефективності. Під час опису оцінок використовується матриця помилок (рис. 2).

True positive (справді позитивне рішення): результат класифікації аномального трафіку, передбачений моделлю, збігся з реальною міткою класу.

False Positive (хибнопозитивне рішення): помилка 1-го роду модель помилково класифікувала нормальний об'єкт, як аномальний.

False Negative (хибнонегативне рішення): помилка 2-го роду, модель помилково класифікувала аномальний об'єкт як нормальний.

True Negative (справді негативне рішення): модель класифікувала об'єкт як нормальний, яким він є насправді.

Помилки у чистому вигляді не використовуються, оскільки показники ефективності (якості) алгоритмів є імовірнісними - залежать від подій, що обробляються, і умов [9]. Тому для оцінки ефективності алгоритмів навчання використовуються інші критерії, наведені нижче [10].

Клас по алгоритму	Реальний клас	
	+	-
+	True Positive (TP)	False Positive (FP)
-	False Negative (FN)	True Negative (TN)

Рис. 2. Матриця похибок [11]

Достовірність алгоритму класифікації – accuracy:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Достовірність показує у відсотках частку правильної класифікації, у разі трафіку, що може характеризувати якість системи виявлення атак. За такої постановки accuracy 80 % означає, що з 100 записів мережного трафіку чітко детектуються 80.

Точність (precision) показує частку об'єктів, що дійсно належать даному класу щодо всіх об'єктів, які алгоритм зарахував до цього класу:

$$Precision = \frac{TP}{TP + FP}$$

Частка істинно позитивних рішень (TPR - True Positive Rate), називається також повнотою (recall), визначається як пропорція аномальних екземплярів, класифікованих коректно, у всій безлічі аномальних екземплярів, представлених у вибірці:

$$TPR = Recall = \frac{TP}{TP + FP}$$

При оцінці ефективності методів глибокого навчання для задач класифікації також застосовується побудова ROC-кривих (Receiver Operating Characteristic Curves). Абстрактно вони є залежністю істинно позитивних і хибнопозитивних рішень класифікатора щодо значень параметрів меж діапазону, саме їх зміни (рис. 3). Площа (area) під ROC-кривою є кількісна інтерпретація якості класифікатора.

F-величина (F-score) поєднує в собі оцінки точності та повноти, при цьому залишається чутливою до розподілу даних:

$$F\ score = \frac{2 \cdot recall \cdot precision}{recall + precision}$$

Характеристика навчаючої вибірки

Ефективність класифікаторів, побудованих із застосуванням методів машинного навчання, багато в чому залежить від наявності якісного у сенсі відсутності шуму та наявності збалансованості класів набору навчальних прикладів - dataset. Популярними наборами даних у галузі побудови класифікаторів мережевих атак для IoT-пристроїв є IoT-23, CTU-IoT-Malware-Capture, N_BaIoT та деякі інші. Всі ці навчальні приклади пожертвувані їх творцями у вигляді послуги спільноті дослідників методів машинного навчання та є у відкритому вигляді репозиторію UCI.

Навчання класифікаторів виявлення атак на сенсорні мережі виконано dataset N_BaIoT. Dataset містить реальні дані трафіку, зібрані з дев'яти комерційних IoT-пристроїв: дверного замка Danmini, термостата Ecobee, дверного замка Ennio, радіоняні Philips_B120N10, камери

відеоспостереження Provision PT737E, камери відеоспостереження Provision PT838, вебкамери Samsung SNH1011N, камери відеоспостереження SimpleHome XCS71002WHT, камери відеоспостереження XCS71003WHT. Усі пристрої достовірно заражені Mirai та Bashlite.

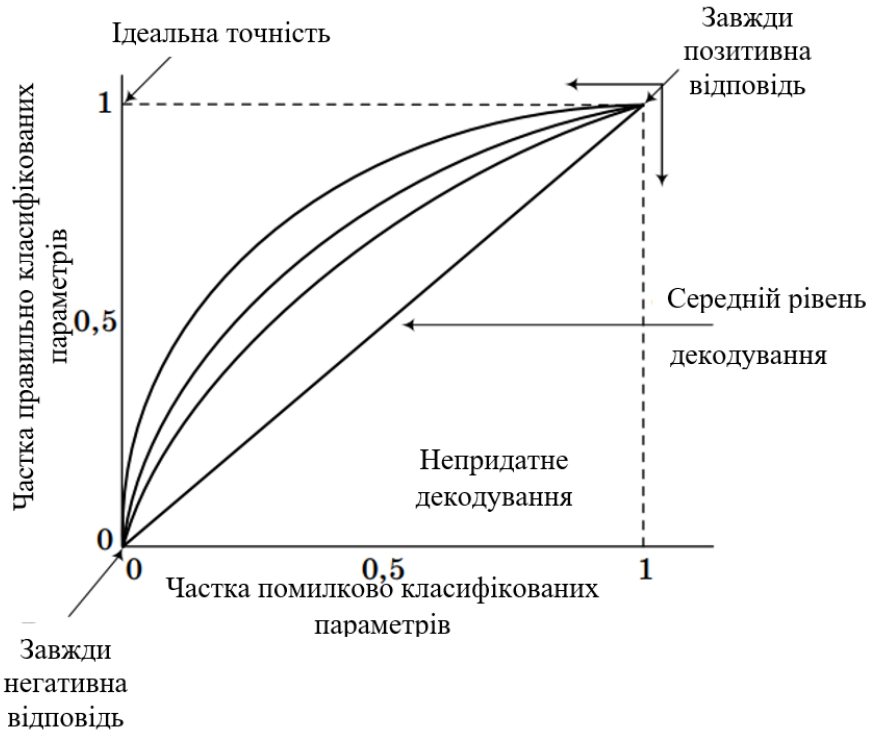

Рис. 3. Приклади ROC-кривих

Кожен запис набору даних представляє собою поведінковий знімок хостів та протоколів, за якими передавався пакет. Знімок отримує контекст пакету шляхом вилучення 115 ознак, опис яких наведено у роботі [3]. Найменування класів та кількість прикладів навчання dataset N_BaIoT наведено у табл. 2. Співвідношення навчальних та тестових прикладів становило 80 і 20% відповідно для кожного класу.

Таблиця 2

Dataset N_BaIoT

Назва класу	Мітка класу	Кількість прикладів
begin	0	98514
combo_bashlite	1	18339
junk_bashlite	2	9266
scan_bashlite	3	9052
tcp_bashlite	4	28494
udp_bashlite	5	33362
ack_mirai	6	13307
scan_mirai	7	22279
syn_mirai	8	14192
upplain_mirai	9	12341
udp_mirai	10	36393

Для провідних мереж популярні такі dataset.

KDDCup 1999 - dataset, що включає п'ять мільйонів записів. Запис представляє собою 42 зафіксованих параметра, що характеризують пакети, які передаються протоколами TCP, UDP та ICMP у певні проміжки часу, при цьому 41 параметр – це інформаційні ознаки, а 42-й параметр – мітка класу, що позначає найменування атаки або її відсутність. У роботі [11] наведено опис інформаційних ознак.

NSL-KDD 2009 - dataset, що є удосконаленням KDDCup 1999, зокрема, не містить записів, які дублюються. Dataset NSL-KDD містить 36 типів атак за чотирма категоріями:

1) Denial of Service (Dos) - атаки, що обмежують доступ верифікованим користувачам до конкретного сервісу через певний протокол (Back, Land, Neptune, Pod, Smurf, Teardrop, Apache2, Udpstorm, Processtable, Worm);

2) Remote to Local (R2L) - атаки, спрямовані на отримання доступу до локальної машини користувача із зовнішнього середовища (Guess_Password, Ftp_write, Imap, Phf, Multihop, Warezmaster, Warezclient, Spy, Xlock, Xsnoop, Snmpguess, Snmpgetattack, Httptunnel, Sendmail, Named);

3) User to Root (U2R) - атаки, спрямовані на отримання привілейованих прав доступу до машини жертви (Buffer_overflow, Loadmodule, Rootkit, Perl, Sqlattack, Xterm, Ps);

4) Probe - атаки, спрямовані на отримання відомостей про інфраструктуру користувача (Satan, Ipsweep, Nmap, Portsweep, Mscan, Saint) [11].

Загалом NSL-KDD містить 125 973 записи, призначені для навчання, і 22 544 записи для тестування.

Крім dataset KDDCup 1999 і його поліпшеної версії NSL-KDD 2009, у галузі інформаційної безпеки інфокомунікаційних мереж існує багато інших навчальних вибірок, наприклад: ECML-PKDD 2007 - включає контекст web-ресурсу, запиту і клас атаки; HTTPCSIC 2010 - включає кілька тисяч веб-запитів, які пропонуються для тестування систем захисту від веб-атак; ADFA2013 - містить трафікові траси системних викликів ОС Linux нормального режиму роботи і траси мережевих атак; UNSW-NB15 2015 - містить дані трафіку, записаного протягом однієї години, що налічує дев'ять типів атак, згенерованих спеціальним програмним забезпеченням, тощо.

З безлічі перерахованих навчальних прикладів для виявлення атак у дротових мережах тільки NSL-KDD очищений від шумів, що дає змогу використовувати його відразу без попередньої обробки, до того ж має найбільшу практику застосування. Щоправда, класи в NSL-KDD незбалансовані, що змушує відмовитися від від класів, представлених малими обсягами прикладів навчання. У табл. 3 наведено найменування класів і кількість навчальних прикладів класів, які використано в роботі. Співвідношення навчальних і тестових прикладів становило 80 і 20 % відповідно для кожного класу.

Таблиця 3

Dataset NSL-KDD після виключення класів малих обсягів

Назва класу	Мітка класу	Кількість прикладів	Назва класу	Мітка класу	Кількість прикладів
smurf	0	164 091	back	9	1098
normal	1	60 593	Mscan	10	1053
neptune	2	58 001	apache2	11	794
snmpgetattack	3	7741	Processtable	12	759
mailbomb	4	5000	Saint	13	736
guess_passwd	5	4367	Portsweep	14	354
snmpguess	6	2406	Ipsweep	15	306
satan	7	1633	Httptunnel	16	158
warezmaster	8	1602			

Експерименти та оцінка результатів

Значення оцінок достовірності методів машинного навчання з детектування атак у мережі IoT наведено у табл. 4.

Як видно з отриманих результатів навчання:

для бездротової сенсорної мережі IoT всі методи машинного навчання показали високу точність класифікації. Це свідчить про якісний dataset;

для дротової мережі IoT випадковий ліс показує кожному класу високі результати, близькі до 100 % точності. В інших методах є «провали» у розпізнаванні певних класів атак, наприклад, для дерева рішень snmpgetattack з 65,27% точності, для нейронної мережі - portsweep з 61,70% точності, для k-найближчих сусідів - satan з 36,91% і saint - з 13,12%.

Результати ефективності методів машинного навчання стосовно задачі класифікації мережевих атак представлені на рис. 4–7.

Результати порівняння методів машинного навчання за оцінками precision, recall та F-score ідентичні у відсотковому співвідношенні оцінки precision, наведеної на рис. 4.

Таблиця 4

Значення accuracy методів машинного навчання

Мітка класу	Дерево рішень	Випадковий ліс	Нейронна мережа	k-найближчих сусідів
Бездротова сенсорна мережа IoT				
benign	100	100	99,98	100
combo_ bashlite	99,98	99,74	100	99,99
junk_bashlite	99,88	99,81	99,92	99,96
scan_bashlite	99,96	100	99,92	99,98
tcp_bashlite	99,97	99,97	99,97	99,99
udp_bashlite	99,98	100	99,96	99,99
ack_mirai	99,97	99,97	99,97	99,99
scan_mirai	100	100	100	100
syn_mirai	100	100	100	100
udpplain_ mirai	100	100	100	100
Проводова обчислювальна мережа IoT				
smurf	100	100	99,5	100
normal	94,64	94,75	92	93,52
neptune	99,99	100	99,9	99,76
snmpgetattack	65,27	100	99,9	70,18
mailbomb	99,93	95,19	94,9	100
guess_passwd	99,51	99,93	97	99,22
snmpguess	99,71	100	97,9	100
satan	97,53	97,11	81,8	36,91
warezmaster	99,36	98,73	98,1	99,36
back	99,71	100	97,7	99,14
mscan	99,08	100	98,1	99,39
apache2	100	100	99,7	96,94
processtable	100	100	98,4	100
saint	91,4	92,76	100	13,12
portsweep	100	100	61,7	96,19
ipsweep	100	100	79,3	97,78
httptunnel	100	100	100	92,73

Результати ROC-кривих для інших класифікаторів, навчених методами випадкового лісу, нейронна мережа та *k*-найближчих сусідів для бездротової сенсорної мережі IoT, ідентичні ROC-кривій, наведеній на рис. 6.

ROC-криві для класифікаторів COA на рівні провідної локальної чи глобальної мережі представлені на рис. 7, *а-г*.

© Ветлицька, О. С., & Треньова, К. О. (2024). Виявлення атак у мережах Інтернету речей методами машинного навчання. Сучасний захист інформації, 1(57), 39–49. https://doi.org/10.31673/2409-7292.2024.010005.

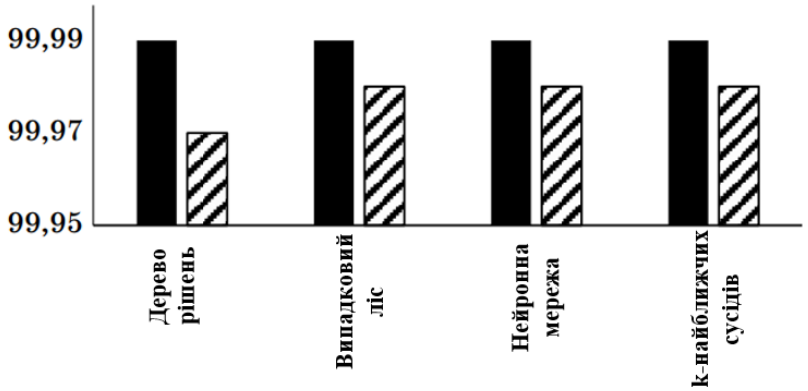

Рис. 4. Результати оцінки precision методів машинного навчання під час класифікації мережевих атак сенсорної мережі

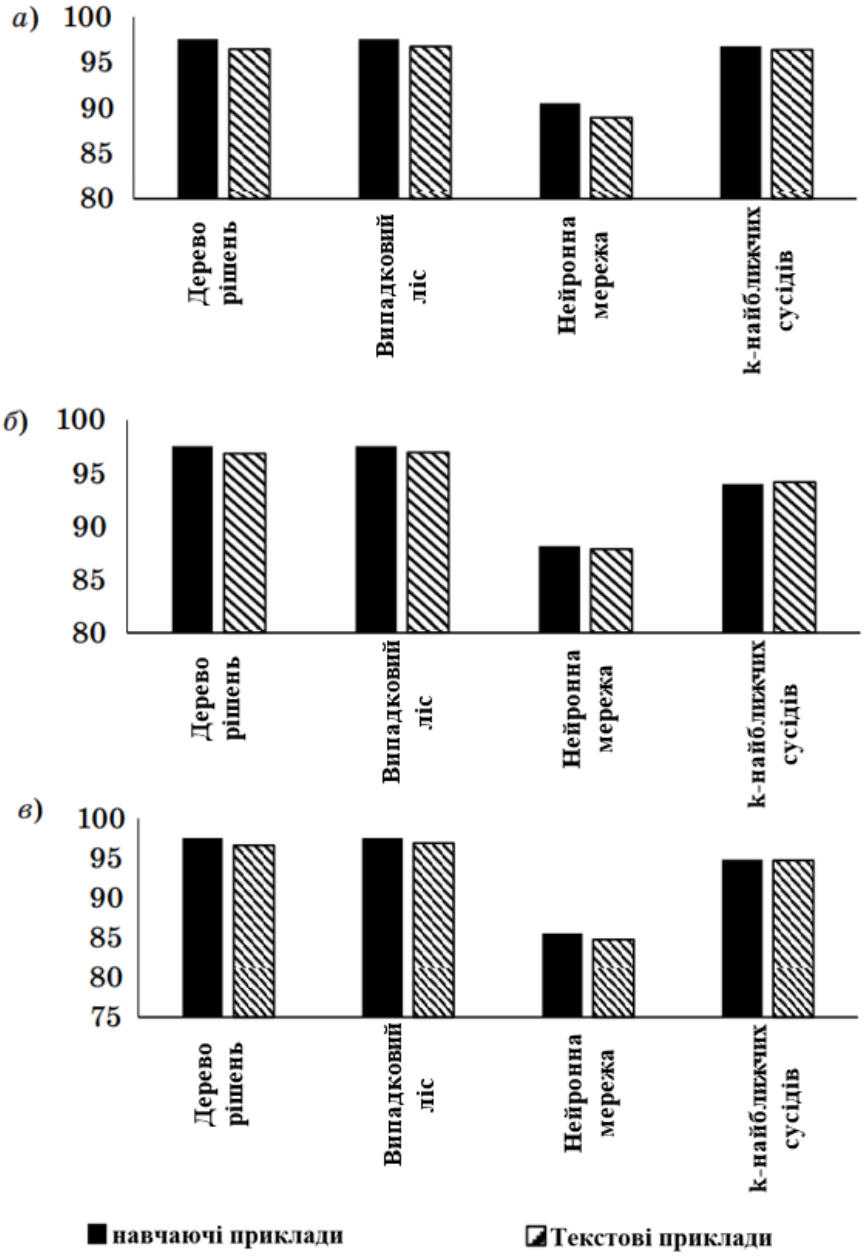

Рис. 5. Результати оцінки ефективності методів машинного навчання при класифікації мережевих атак у провідній мережі: *а* - precision; *б* - recall; *в* - F-score

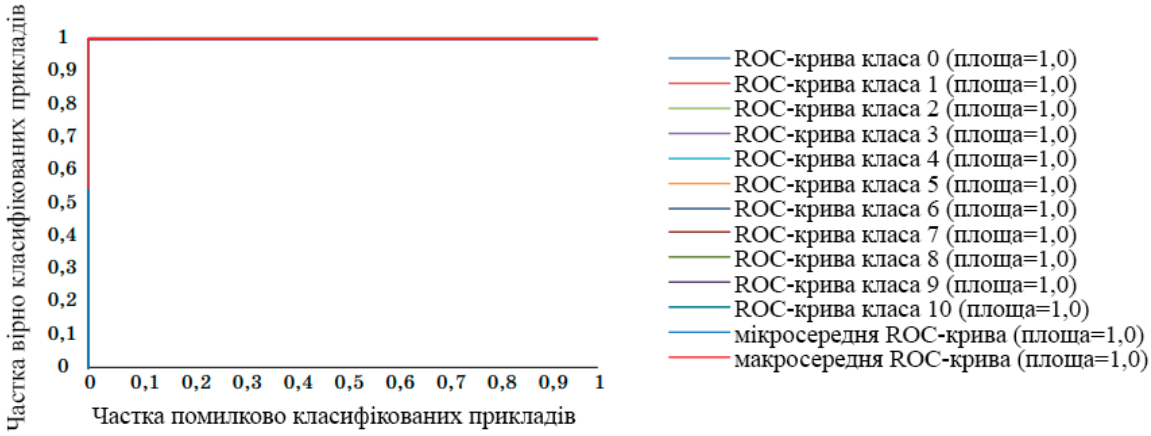

Рис. 6. ROC-криві, отримані методом дерево рішень для бездротової сенсорної мережі

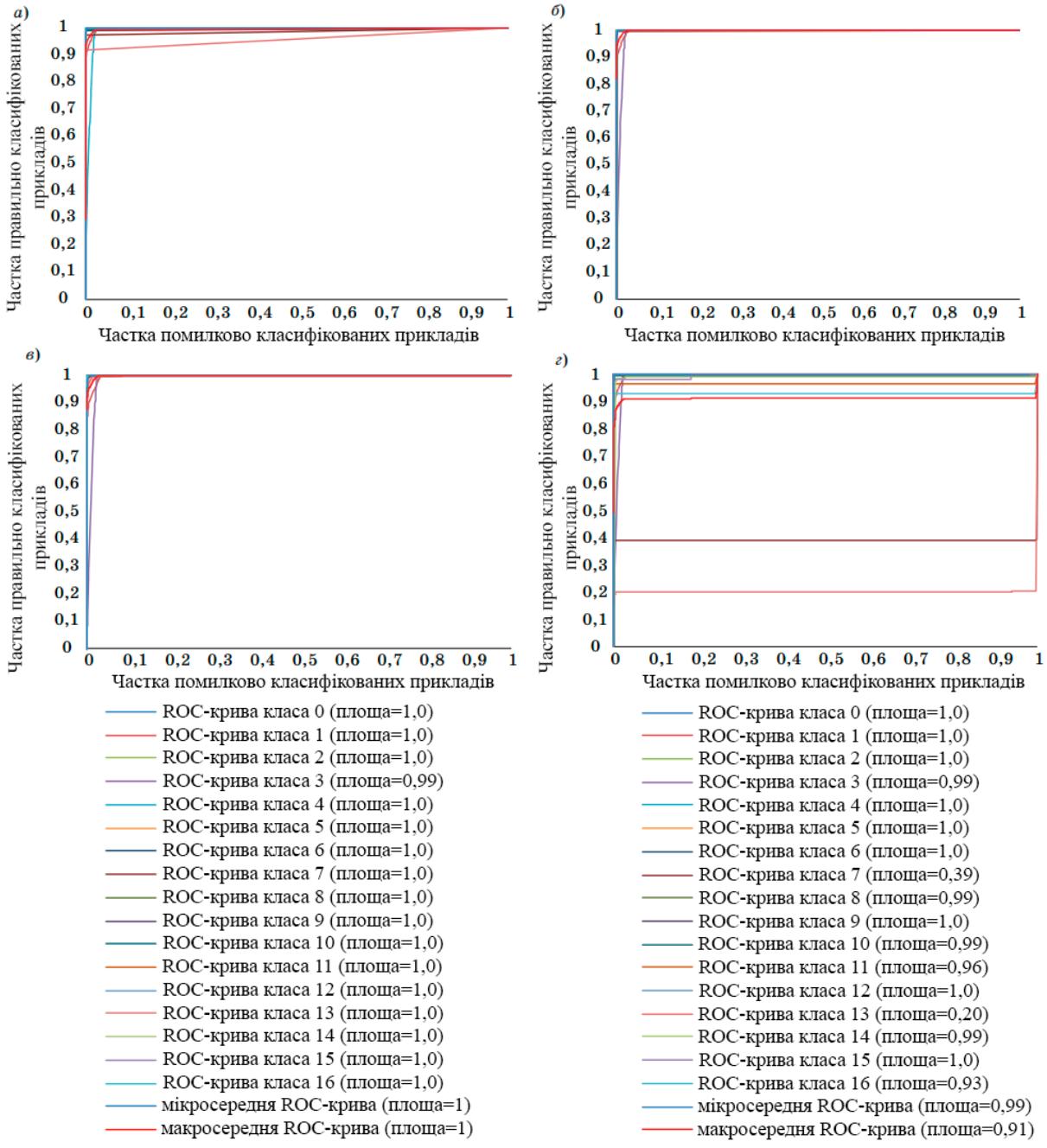

Рис. 7. ROC-криві, отримані методами дерево рішень (*а*); випадковий ліс (*б*); нейронна мережа (*в*); *k*-найближчих сусідів (*г*) для проводової мережі IoT

© Ветлицька, О. С., & Треньова, К. О. (2024). Виявлення атак у мережах Інтернету речей методами машинного навчання. Сучасний захист інформації, 1(57), 39–49. https://doi.org/10.31673/2409-7292.2024.010005.

Наведені на рис. 7, *а-г* ROC-криві показують високу ефективність навчених класифікаторів. Так, для методів дерево рішень, випадковий ліс та нейронна мережа значення відносин істинно позитивних та хибнопозитивних рішень класифікаторів близькі до одиниці. Для методу *k*-найближчих сусідів не можуть бути достовірно виявлені атаки satan та saint.

Зміст етапів пропонованого підходу до виявлення атак у мережах інтернету речей

Пропонований підхід до виявлення атак в мережах інтернету речей включає такі основні етапи:

1) збір статистики про переданій трафік;

2) витяг ознак із зібраної статистики;

3) класифікація трафіку;

4) безперервний моніторинг мережі IoT.

На етапі збирання даних здійснюється знімання статистик з:

головних вузлів кластерів бездротової сенсорної мережі, що приймають дані від IoT пристроїв;

маршрутизаторів і шлюзів дротової локальної та глобальної мережі;

протоколів передачі даних.

Вузлові та мережеві агенти доставляють зібрані статистики в СОА.

На другому етапі із зібраних статистик витягують ознаки окремо для класифікатора бездротової сенсорної мережі та для дротової локальної і (або) глобальної мережі. Ознаки ті ж самі, що застосовувалися для навчання класифікаторів.

На третьому етапі витягнуті ознаки подаються на входи відповідних класифікаторів. Виявлені аномалії в трафіку, що передається від IoT-пристроїв, можуть вказувати на те, що пристрій скомпрометовано. Ознаки, що вказують на аномальну поведінку будь-якого сенсорного пристрою, передаються в блок прийняття рішень СОА, де відбувається аналіз ознак і приймається рішення про реагування на ситуацію, що склалася. Атаки, виявлені на рівні дротової локальної або глобальної мережі, також передаються в блок прийняття рішень СОА для вибору варіантів реагування на виявлену атаку або клас атак.

Безперервний моніторинг передбачає виконання етапів 1-3 з періодичністю, яка може збігатися, наприклад, із тривалістю раундів, під час яких сенсорні пристрої передають дані на головний вузол свого кластера бездротової сенсорної мережі.

Під час реєстрації нового IoT-пристрою трафік, що генерується ним, має бути зібраний відразу після підключення IoT-пристрою до мережі, щоб гарантувати, що дані є незараженими. Таким чином формується база даних профілів нормальної поведінки кожного IoT-пристрою. При появі нового виду або класу мережевих атак розглянутий підхід передбачає організацію збору статистик зараженого трафіку з метою подальшого навчання класифікатора на виявлення цих атак. Витягнуті ознаки являють собою профіль конкретного виду або класу атаки.

Таким чином, на головних вузлах кластерів бездротової сенсорної мережі функціонує модуль виявлення аномальної поведінки IoT-пристроїв, що являє собою навчений класифікатор; на маршрутизаторах і шлюзах функціонує модуль виявлення мережевих атак, що також являє собою навчений класифікатор.

Висновки

Зі зростанням обсягів цифрових даних у методах виявлення атак стали актуальними дослідження, пов'язані із застосуванням методів машинного навчання для виявлення аномалій мережевого трафіку - наявності мережевих атак. Це повною мірою стосується і мереж інтернету речей, а постійне підключення сенсорних пристроїв до інтернету робить їх зручним інструментом для організації кібератак. На рівні бездротової сенсорної мережі виявлення аномальної поведінки IoT-пристроїв реалізується оцінкою відхилення поведінки IoT-пристроїв від відповідних їм профілів поведінки. Побудова профілів розумних пристроїв здійснюється на основі статистичних характеристик, що знімаються з вузлів мережі інтернету

© Ветлицька, О. С., & Треньова, К. О. (2024). Виявлення атак у мережах Інтернету речей методами машинного навчання. Сучасний захист інформації, 1(57), 39–49. https://doi.org/10.31673/2409-7292.2024.010005.

речей і протоколів, за якими передаються пакети даних. На рівні локальної або глобальної дротової мережі інтернету речей відбувається агрегування даних, аналіз яких також виконується методами машинного навчання.

Навчені моделі класифікації можуть стати частиною системи виявлення мережевих атак, які ухвалюють рішення про компрометацію вузла "на льоту". Експериментальним шляхом обрано модель класифікатора мережевих атак на рівні бездротової сенсорної мережі та локальної або глобальної дротової мережі. Найкращі результати в сенсі оцінок повноти й точності продемонстровано методом випадкового лісу для дротової локальної або глобальної мережі та всіма розглянутими методами для бездротової сенсорної мережі.

На якість класифікаторів істотно впливає наявність збалансованого і підготовленого набору даних. Надалі планується систематизувати інформаційні параметри, які можуть мати найбільшу важливість під час навчання класифікаторів. А також виконати порівняння двох підходів до побудови СОА: заснованих на методах машинного навчання і методах оцінки довіри вузла до своїх сусідів.

Перелік посилань

1. Baddar, S. A.-H., Merlo, A., Megiliardi, M. Anomaly detection in computer networks: A state-of-the-art review. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2014, vol. 5, no. 4, pp. 29–64.
2. Lee, P. Internet of Things for Architects. Birmingham – Mumbai, Packt Publ., 2018. 524 p.
3. Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Breitenbacher, D., Shabtai, A., and Elovici, Y. N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Computing, Special Issue – Securing the IoT, 2018, vol. 17(3), pp. 12–22.
4. Kumar, S., Spafford, E. H. A pattern matching model for misuse intrusion detection. Proceedings of the 17th National Computer Security Conference, 1994, pp. 11–21.
5. Thatte, G., Mitra, U., Heidemann, J. Parametric methods for anomaly detection in aggregate traffic. IEEE/ ACM Transaction on Networking, 2011, vol. 19(2), pp. 512–525.
6. Wu, S. X., Banzhaf, W. The use of computational intelligence in intrusion detection systems: A review. Applied Soft Computing, 2010, vol. 10(1), pp. 1–35.
7. Ingre, B., Yadav, A., Soni, A. K. Decision tree based intrusion detection system for NSL-KDD dataset. Proceedings of the International Conference on Information and Communication Technology for Intelligent Systems (ICTIS), Ahmedabad, India, March 25–26, 2017, Cham, Springer, 2017, vol. 2, pp. 207–218. doi:10.1007/978-3-319-63645-0_23.
8. Fatihand, E., Aydin, G. Data classification with deep learning using tensorflow. International Conference on Computer Science and Engineering, 2017, pp. 755–758.
9. Gyanchandani, M., Rana, J. L., Yadav, R. N. Taxonomy of anomal based intrusion detection system: A review. International Journal of Scientific and Research Publications, 2012, vol. 2(12), pp. 1–13.
10. Jyothsna, V., Prasad V. V. R. A Review of anomaly вased intrusion detection systems. International Journal of Computer Applications, 2011, vol. 28, no. 7, pp. 26–35.
11. A Deeper Dive into the NSL-KDD Data Set – Towards Data Science. https://towardsdatascience.com/adeeper-dive-into-the-nsl-kdd-data-set-15c753364657.

Надійшла 13.01.2024