УДК 004.8

Н.П. Тимошик
Національний університет “Львівська політехніка”,
кафедра захисту інформації

ЗАСТОСУВАННЯ МЕТОДУ ГРУПОВОГО ВРАХУВАННЯ АРГУМЕНТІВ ДЛЯ СИСТЕМИ АВТОМАТИЧНОЇ ПОБУДОВИ МОДЕЛЕЙ МЕРЕЖЕВОГО ТРАФІКУ СИСТЕМ ВИЯВЛЕННЯ АТАК

Розглянуто застосування методу групового врахування аргументів для побудови системи класифікації мережевого трафіку та ідентифікації атак. Описано спосіб застосування комбінаторного алгоритму методу групового врахування аргументів (МГВА) при генерації моделей мережевого трафіку на основі вибірки KDD'99 системами виявлення атак проти атак класу “відмова в обслуговуванні”(DoS).

In the article the question is about application Group Method of Data Handling for the construction of the system of classification of network traffic and authentication of attacks. The method of application of Combi algorithm of Group Method of Data Handling (GMDH) is presented during the generation of models of network traffic on the basis of selection of KDD'99 by the systems of exposure of attacks against the attacks of class “deny of service”(DoS).

Постановка проблеми та мета роботи. Щоденно з'являються нові типи атак на комп'ютерні системи і мережі, з'являються нові віруси, які є інструментом і носієм мережевих атак. Збитки від атак деяких корпорацій сягають мільйонів доларів на день. Мережеві атаки стають плацдармом для руйнування мережевих інфраструктур та інструментом для викрадення конфіденційної інформації, для поширення вірусів, хробаків та спаму.

Відомі рішення із застосуванням адаптивних і самонавчальних систем захисту комп'ютерних мереж є малоефективними в реальній мережевій інфраструктурі через все більшу масштабність та неординарність атак, а також відсутність центрального джерела нових відомостей для донавчання. Крім цього, більшість рішень, які ґрунтуються на нейромережевих алгоритмах, неспроможні виявляти нові атаки в реальній мережі. Сучасні фільтри мережевого трафіку, системи виявлення та протидії втручанням стають щораз менш ефективними при роботі з великими об’ємами трафіку у високошвидкісних мережах і також малопридатні для розпізнавання нових типів і методів атак на комп’ютерні системи та мережі. Індуктивні методи забезпечують можливість отримання точної ідентифікації або прогнозу різних складних процесів у випадку коротких або зашумлених вхідних даних. Це актуально для розпізнавання мережевого трафіку на основі класифікації за протоколами, оскільки більшість нормального мережевого потоку відповідає стандартам RFC, встановленим розробниками, а аномалії найчастіше проявляються якраз у нестандартній поведінці та стані пакетів.

Відомі виробники мережевого обладнання – такі, як Cisco Systems, для систем виявлення та протидії втручанням (IDS/IPS) найчастіше користуються сигнатурними методами аналізу трафіку і частково рішеннями на основі нейронних мереж для виявлення аномальної активності в мережі. Перевагою сигнатурних методів є можливість виявляти відому атаку на основі відомих й описаних ознак та характеристик атаки, проте вони серйозно програють у високошвидкісних мережах передавання даних, оскільки потребують значних обчислювальних потужностей та часу на розбір та аналіз кожного пакета. Перевагою нейронних мереж є висока швидкість роботи, адаптивна логіка,

можливість самонавчання та донавчання. Недоліком є велика кількість часу і ресурсів, необхідна для навчання нейронної мережі. Саме ми пропонуємо використання алгоритмів МГВА для побудови спеціалізованих модулів систем виявлення втручань та аналізаторів віртуальних приманок.

Алгоритми МГВА мають значну перевагу, яка проявляється у можливості самоорганізації та самонавчання [1]. Також властивість короткострокового прогнозування МГВА на певних етапах атаки дає можливість зпрогнозувати та здійснити блокування або маршрутизацію підозрілого трафіку в систему-приманку.

Опис набору вхідних даних. Для отримання моделей мережевого потоку ми використали дані, надані для досліджень інститутом MIT's Linkoln Lab, які були зібрані для конкурсу KDD'99 [2] на кращі алгоритми Data Mining систем виявлення втручань. Загалом вибірку вхідних даних можна подати за типами атак і класами, до яких вони належать:

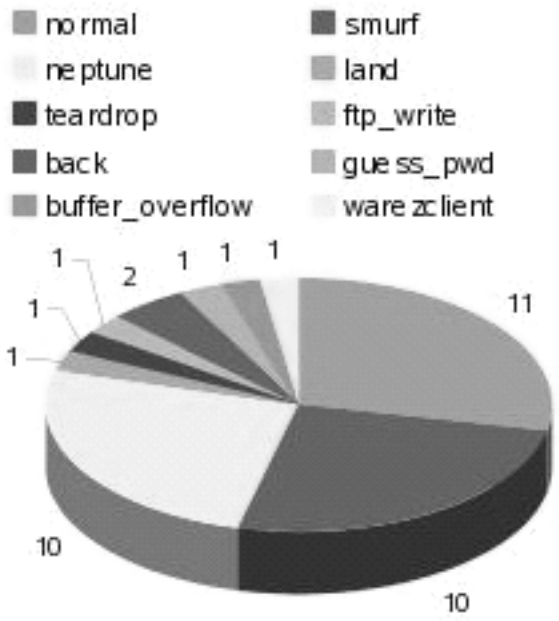

Рис. 1. Співвідношення даних про атаки різних типів у наборі даних KDD'99:
u2r (user2root) — клас атак з спробою підвищення локальних привілеїв;
dos (Denial of Service) — атаки на відмову в обслуговуванні;
r2l (remote to local) — віддалені атаки через мережу;
probe — різного роду сканування

Атаки в наборі з відповідним класом подають далі:

back dos
buffer_overflow u2r
ftp_write r2l
guess_passwd r2l
imap r2l
ipsweep probe
land dos
loadmodule u2r
satan probe
smurf dos
spy r2l
multihop r2l
neptune dos
nmap probe
perl u2r
phf r2l
pod dos
portsweep probe
rootkit u2r
teardrop dos
warezclient r2l
warezmaster r2l

Вибірка даних містить 24 відомі типи атак і 14 типів атак для перевірки.

Таблиця 1

Основні параметри окремого TCP з'єднання

Параметр	*Опис*	*Тип даних*
duration	тривалість (к-ть секунд) з'єднання	неперервні
protocol_type	Тип протоколу (tcp, udp, etc.)	дискретні
service	Атакований сервіс	дискретні
src_bytes	Кількість байтів від джерела до призначення	неперервні
dst_bytes	Кількість байтів відповіді клієнту	неперервні
flag	Прапорці з'єднання	дискретні
land	1 якщо з'єднання від/до того самого хоста/порта	дискретні
wrong_fragment	Кількість “хибних” фрагментів	неперервні
urgent	Кількість термінових пакетів	неперервні

Таблиця 2

Параметри пакетів в з'єднанні

Параметр	*Опис*	*Тип даних*
hot	Кількість ``гарячих" індикаторів	неперервні
num_failed_logins	Кількість невдалих спроб реєстрації	неперервні
logged_in	1, якщо успішний вхід в систему; 0 неуспішне	дискретні
num_compromised	Кількість ``компроментуючих" умов	неперервні
root_shell	1, якщо root shell отриманий; інакше 0	дискретні
su_attempted	1, якщо виконувалась``su root" ; інакше 0	дискретні
num_root	Кількість``root" доступів	неперервні
num_file_creations	Кількість операцій створення файлів	неперервні
num_shells	Кількість запитів на надання оболонки	неперервні
num_access_files	Кількість операцій на доступ до контролю файлів	неперервні
num_outbound_cmds	Кількість вихідних команд для FTP сесії	неперервні
is_hot_login	1, якщо логін належав до ``гарячого" списку;	дискретні
is_guest_login	1, якщо ``гостьовий" вхід;	дискретні

Таблиця 3

Параметри трафіку в двосекундному вікні

Параметр	*Опис*	*Тип даних*
count	Кількість з'єднань на хост в поточній сесії така сама, як за останні 2 с	неперервні
serror_rate	% з'єднань що мали ``SYN" помилки	неперервні
rerror_rate	% з'єднань що мали ``REJ" помилки	неперервні
same_srv_rate	% з'єднань що мали однаковий сервіс	неперервні
diff_srv_rate	% з'єднань на різні сервіси	неперервні
srv_count	Кількість з'єднань на такий самий сервіс, як під час поточного з'єднання за останні 2 с	неперервні
srv_serror_rate	% з'єднання з помилкою в ``SYN" пакеті	неперервні
srv_rerror_rate	% з'єднання, що мають ``REJ" помилки	неперервні
srv_diff_host_rate	% з'єднання від інших хостів	неперервні

Дані проходять нормалізацію та оптимізацію для кожного типу трафіку. Запис про кожне з'єднання утворює послідовність пакетів відповідного протоколу з позначками початку та кінця з'єднання, під час якого відбувалось передавання даних між відправником та отримувачем через один з визначених вище протоколів. Кожне з'єднання марковане як нормальний трафік або атака.

Для підвищення швидкодії ми розділяємо загальний набір KDD на три класи: набір з DoS атаками, набір зі спробами сканування портів, і R2L/U2R набір. Отже, різні параметри сесії зв'язку можна аналізувати паралельно, що зменшує час затримки.

Загальна кількість відомостей про нормальний тип трафіку становить 972781 записів, а результати DoS атак – 3883106 записів, що з загального набору 4898431 записів становить 79.27 %.

Вибір алгоритму та генерація моделей методом групового врахування аргументів. За структурою алгоритми МГВА близькі до алгоритмів самонавчання багаторядних систем розпізнавання образів – до персептронів або нейромереж [6]. Істотна відмінність полягає в тому, що поліноміальні алгоритми МГВА оперують з неперервними змінними (саме таким є мережевий трафік). Дискретний характер вихідної змінної перцептрона, що вказує належність цього зображення до того чи іншого образу, унеможливлює тонше урахування неточності розпізнавання для вибору структури персептрону. Після дискретизації або кластеризації отримання нефізичних моделей неможливе. Тільки безперервні змінні дають змогу знайти мінімум зовнішнього критерію, що визначає оптимальну структуру нефізичних моделей.

Фізична модель відповідає поняттю математичного опису, прийнятого в математичній фізиці. Іноді фізичною моделлю об'єкта також називають її апроксимацію за допомогою полінома або мовою кластеризації. Фізична модель – єдина для кожного об'єкта й мови його опису.

Основний результат теорії МГВА полягає в тому, що при неточних зашумлених даних і коротких вибірках мінімум критерію вказує так звану нефізичну модель, точність якої вища і структура якої простіша від структури повної фізичної моделі [1]. Нефізичні моделі можна отримати лише за МГВА.

Структура нефізичної моделі тим простіша, чим більша дисперсія завад. Збільшення довжини вибірки рівнозначне зменшення перешкод. Структура нефізичної моделі при зростанні вибірки наближається до структури фізичної моделі. Отже, для об'єкта може існувати багато нефізичних моделей, що залежить від дисперсії перешкод та довжини вибірки. Нефізичні моделі отримують не тільки за допомогою виключення деяких членів фізичної моделі, але й випадково, так щоб отримати глибший мінімум зовнішнього критерію [6].

За точністю персептрони майже не поступаються поліноміальним алгоритмам МГВА за умови, що навчальна вибірка достатньо довга, дисперсія помилок — низька, а вибірка містить змінні, дискретизовані на невелику кількість рівнів, тобто у випадках, коли оптимальною є фізична модель [5]. Однак тільки неперервні змінні дають змогу знайти мінімум зовнішнього критерію, визначаючи оптимальну структуру нефізичних моделей [6]. Отже, МГВА найкраще підходить для отримання нефізичних моделей мережевого трафіку.

МГВА застосовується в різноманітних сферах для аналізу даних та знаходження знань та закономірностей, прогнозування і моделювання систем, оптимізації та розпізнавання образів. Індуктивні алгоритми МГВА дають унікальну можливість автоматично знаходити взаємозалежності у даних, вибрати оптимальну структуру моделі чи мережі, підвищувати точність наявних алгоритмів.

МГВА складається з ряду алгоритмів для вирішення широкого спектра завдань [5]. В нього входять як параметричні алгоритми, так і алгоритми кластеризації, комплексування аналогів, ребінаризації та ймовірнісні алгоритми. Цей підхід самоорганізації оснований на переборі моделей, що поступово ускладнюються та на виборі найкращого розв'язку згідно з мінімумом встановленого критерію [1].

Важливими особливостями алгоритмів МГВА порівняно з аналогічними підходами [6] для побудови ефективної системи виявлення атак (СВА) та системи аналізу приманок та атак (САПіА) віртуальних приманок є:

- можливість знаходження оптимальної складності структури моделі, адекватної до рівня завад у вибірці даних. (Для вирішення реальних проблем із зашумленими чи короткими даними спрощені прогнозуючі моделі виявляються точнішими);

- кількість шарів і нейронів у схованих шарах, структуру та інші оптимальні параметри нейромережі знаходять автоматично;
- гарантується знаходження найточнішої чи незміщеної моделі – метод не пропускає найкращого рішення під час перебору всіх варіантів (у заданому класі функцій);
- будь-які нелінійні функції чи ознаки, що можуть мати вплив на вихідну змінну, використовуються як вхідні аргументи;
- за допомогою МГВА автоматично знаходять інтерпретаційні взаємозв'язки у даних та вибирають ефективні вхідні змінні;
- критерії, розраховані на підставі нової незалежної інформації, можуть дати мінімум перебірної характеристики. Для цього вибірка ділиться на частини для побудови та оцінки моделей;
- всі алгоритми мають багаторядну структуру, завдяки чому можливе застосування паралельних обчислень для їхньої реалізації;
- у багаторядних алгоритмах МГВА з одного рівня на наступний має передаватися не один, а кілька кращих результатів для забезпечення “свободи вибору”;
- мережі МГВА можуть використовуватися для підвищення точності інших алгоритмів моделювання;
- метод використовує інформацію безпосередньо з вибірки даних і мінімізує вплив апріорних припущень автора про результати моделювання.

Отримання моделі для кожного класу трафіку ділиться на кілька етапів. Кожен із етапів починається формуванням ряду селекції, а закінчується визначенням групи найточніших моделей і переведенням цих моделей на вищий ряд селекції.

При формуванні ряду селекції повний опис об'єкта $Y= f(x_1, x_2, \ldots, x_n)$ замінюється кількома рядами окремих описів вигляду $y=f(x_1, x_2)$. В цей опис, попарно комбінуючись, входять всі параметри повного опису. Параметрами моделей, що формуються на цьому ряді селекції, слугують функції з попереднього ряду селекції, що переведені у вищий ряд за критерієм максимальної точності.

Параметри моделі на першому ряді селекції використовуються із матриці досліджень:

$$y_1=f(x_1,x_2),\ y_2=f(x_2,x_3),\ y_3= f(x_1,x_2),\ \ldots\ ,\ y_s=f(x_{n-1},x_n), \tag{1}$$

де $S = C_n^2$.

Кількість моделей визначається за формулою:

$$C_n^k = \frac{n!}{k!*(n-k)!}. \tag{2}$$

При створенні моделей другого ряду селекції за параметри функції “Z” приймаються моделі попереднього ряду, що переведені на вищий ряд селекції —“Y”

$$z_1=f(y_1,y_2),\ z_2=f(y_2,y_3),\ z_3= f(y_1,y_2),\ \ldots\ ,\ z_p=f(y_{n-1},y_n), \tag{3}$$

де кількість моделей p визначається за формулою:

$$p = C_n^2. \tag{4}$$

При створенні моделей третього ряду селекції за параметри функції “G” приймають моделі попереднього ряду, що переведені на вищий ряд селекції —“Z”.

$$g_1=f(z_1,z_2),\ g_2=f(z_2,z_3),\ g_3= f(z_1,z_2),\ \ldots\ ,\ g_h=f(z_{n-1},z_n), \tag{5}$$

де кількість моделей h визначається за формулою:

$$h = C_n^2. \tag{6}$$

Генерація рядів селекції зупиняється відповідно до правила зупинки селекції, що описане нижче.

У першому ряді реалізується квадратична регресія, у другому – регресія 4-го ступеня, у третьому – регресія 8-го ступеня і т.д. Кожний конкретний опис є функцією двох аргументів, тому коефіцієнти частинних описів можна легко визначити за даними навчальної послідовності за малою кількістю вузлів інтерполяції (перша операція). Виключаючи проміжні змінні (друга операція), ми

можемо отримати аналог повного опису. В результаті можливо визначити числові значення найскладнішого повного опису за малої кількості вузлів інтерполяції. Наприклад, за 10 вузлами інтерполяції можливо отримати оцінки коефіцієнтів полінома 7-го ступеня і т.д.

При здійсненні селекції, з ряду в ряд за допомогою порогових відборів пропускається тільки деяка кількість найрегулярніших або незміщених змінних. Ступінь регуляризації оцінюють за величиною середньоквадратичної похибки (середня для всіх f, які вибирають для всіх змінних у кожному поколінні, або однієї найточнішої змінної на окремій перевірочній послідовності). Ступінь незміщеності оцінюється за спеціальним критерієм. Повний опис знаходять за допомогою виключення проміжних змінних із ряду частинних описів (якщо вони лінійні) [7].

Ряди селекції нарощуються доти, доки критерій незміщеності рішень зменшується. Нульове значення оцінки незміщеності досягається тільки за відсутності завад у початкових даних і під час розв'язання задачі відкриття законів та ідентифікацій. Це свідчить про те, що отриманий результат є шуканим фізичним законом [8].

Як тільки досягнутий мінімум похибки або незміщеності, селекцію необхідно зупинити. Практично рекомендується зупинити селекцію навіть дещо раніше від досягнення повного мінімуму – як тільки похибка почне зменшуватись занадто повільно. Тоді отримують простіші вірогідні рішення.

Для отримання найрегулярнішого математичного опису як критерій селекції при використанні критерію регулярності [8] використовують середньоквадратичну похибку, виміряну на окремій перевірочній послідовності

$$\Delta^2_{пр} = \frac{1}{N_{пр}} \sum_{i=1}^{N_{пр}} \left(\varphi_i - \varphi_i^*\right)^2 ; \quad \delta^2{}_{(1)} = \frac{\sum_{i=1}^{N_{пр}} \left(\varphi_i - \varphi_i^*\right)^2}{\sum_{i=1}^{N_{пр}} \varphi_i^2} * 100\% . \tag{7}$$

Перше рівняння описує абсолютну похибку на перевіряючій послідовності, а друге – середньоквадратичну похибку.

Для розрахунку критерію незміщеності [8] всі експериментальні точки ранжуються, тобто розміщуються в ряд за величиною дисперсії

$$D^2 = \frac{1}{N} \sum_{i=1}^{N} \left[\left(\varphi_i - \bar{\varphi}_i\right)^2 / \bar{\varphi}_i \right]^2 , \tag{8}$$

і діляться на дві частини: точки з парними номерами утворюють послідовність R1, а точки з непарними – послідовність R2. За алгоритмом МГВА після кожного ряду селекції вибирається за F рівнянь регресії виду:

1 ряд: y=f(xi,xj); R1=Nн; R2=Nпер.; y*r=f(xi,xj);

2 ряд: z=f(yi,yj); R1=Nпер; R2=Nн.; y**r=f(xi,xj); де 1<r<F

3 ряд: v=f(zi,zj);

4 ряд: v=f(vivj); і т.д.

На особливу увагу заслуговує комбінаторний алгоритм МГВА (COMBI), який ми спробуємо застосувати для побудови системи класифікації мережевого трафіку та ідентифікації атак.

Вхідна вибірка даних являє собою таблицю, яка містить N рівнів (точок) спостережень множини з M змінних. Вибірка поділяється на дві частини. Приблизно дві третини точок належать до навчальної підвибірки N_A, а одна третина точок, що залишилися (отже, кожна третя точка), з такою самою варіацією, формують перевірочну підвибірку N_b. Перед розбиттям точки ранжуються за значенням варіації. Навчальна вибірка використовується для одержання оцінок коефіцієнтів полінома, а перевірочна вибірка використовується для вибору структури оптимальної моделі, для якої зовнішній критерій регулярності AR(s) набуває найменших значень

$$AR(s) = \frac{1}{N_B} \sum_{i=1}^{N} (y_i - \hat{y}_i(B))^2 \to \min . \tag{9}$$

Другим варіантом може бути застосовування критерію перехресного контролю [8](cross-validation) PRR(s) (цей варіант бере до уваги всю інформацію з вибірки даних і може бути підрахований без перерахування матриці для кожної перевірочної точки):

$$PRR(s) = \frac{1}{N}\sum_{1}^{N}\left[y_i - y_i(B)\right]^2 \to \min, \quad N_A = N - 1; \quad N_B = 1. \tag{10}$$

Для тестування моделі на відповідність за критерієм балансу [7] вхідна вибірка даних поділяється на дві частини. Критерій вимагає вибору моделі, яка буде найбільш однаковою в обох підвибірках. Критерій балансу буде знаходити єдину оптимальну фізичну модель, тільки якщо вхідна вибірка зашумлена. Для отримання плавної перебірної кривої, яка дає змогу визначити правило зупинки перебірної процедури, повний пошук ведеться на групах моделей однакової складності. Наприклад, перший рівень може використовувати інформацію з кожної одної колонки вибірки даних так, що повний пошук ведеться серед всіх можливих моделей виду:

$$y = a_0 + a_1 x_i, \qquad i = 1,2,...,M\ . \tag{11}$$

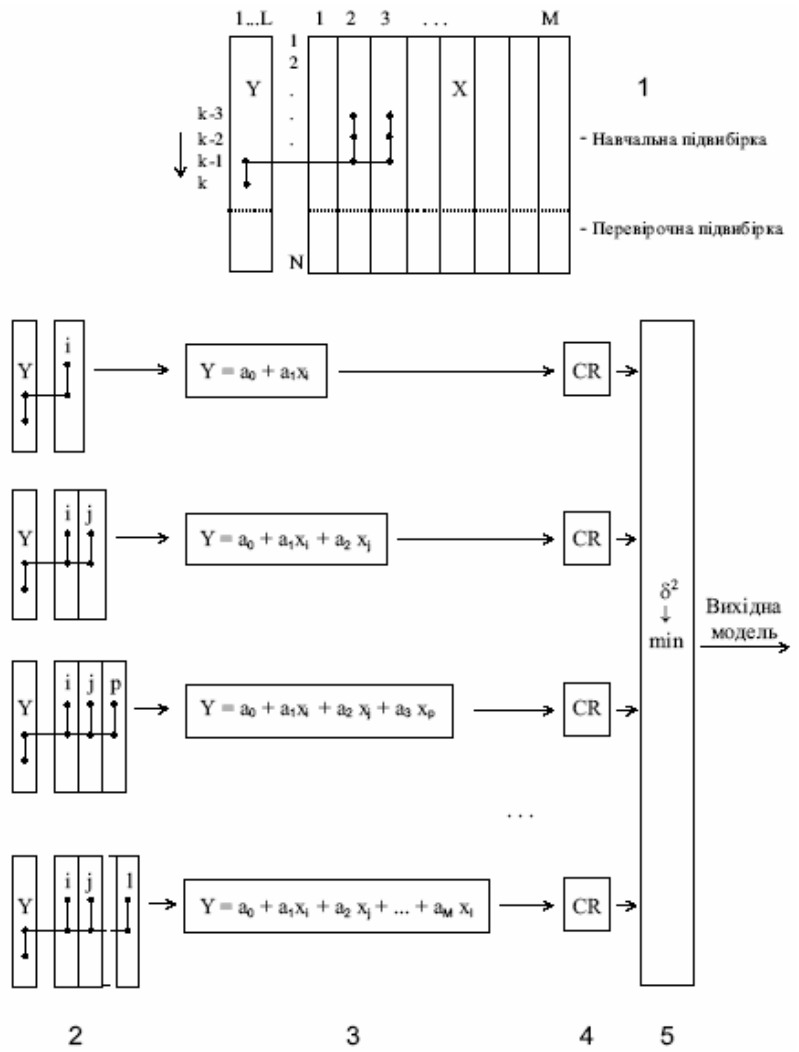

Рис. 2. Комбінаторний алгоритм МГВА:
1 – вибірка даних; 2 – ряди ускладнення часткових описів;
3 – форми часткових описів; 4 – вибір оптимальних моделей;
5 – додаткове визначеній моделі за дискримінаційним критерієм

Нелінійні члени можуть бути враховані як нові вхідні змінні у вибірці даних. Вихідна змінна визначається наперед експериментатором. На наступному рівні перебираються всі моделі виду:

$$y = a_0 + a_1 x_i + a_2 x_j,\ j = 1,2,...,M\ . \tag{12}$$

Моделі оцінюються на відповідність за критеріям, доки значення критерію зменшується.

Для обмеження часу обчислень пропонується під час повного перебору моделей ранжувати змінні відповідно до значень критерію після деякого часу обчислень або кількох рівнів ітерації. Потім процедура повного перебору продовжується до вибраної множини кращих змінних, поки мінімальне значення зовнішнього критерію не буде знайдене. Це дає можливість задавати значно більшу кількість змінних на вході та зберегти ефективні змінні між рівнями для знаходження оптимальної моделі.

Опис схеми системи виявлення втручань з використанням сенсорів, згенерованих МГВА. Мережевий сенсор на базі відповідних моделей, які будуть отримані за допомогою МГВА для нормального та аномального трафіку, складається із декількох шарів, кожен з яких має певні параметри та орієнтований на відповідні протоколи. Кожен шар сенсора навчається окремо на базі нормального трафіку та трафіку, що містить атаки. Шари мають лінійну або ієрархічну структуру залежно від завдань кожного сенсора (виявлення атак/аномалій/нормального трафіку). Якщо пакет від користувача проходить всі шари сенсора, то він передається на сервер. В іншому випадку пакет передається на доопрацювання або до системи-приманки. Кожна система-приманка є клоном сервера, для якого був призначений підозрілий мережевий потік. Завдяки даним, отриманим від системи-приманки, стає можливим створення нових сигнатур про досі невідомі методи зламу. Водночас промислова система залишається в робочому стані.

Схему ієрархії аналізу для кожного типу протоколу подано на рис. 3.

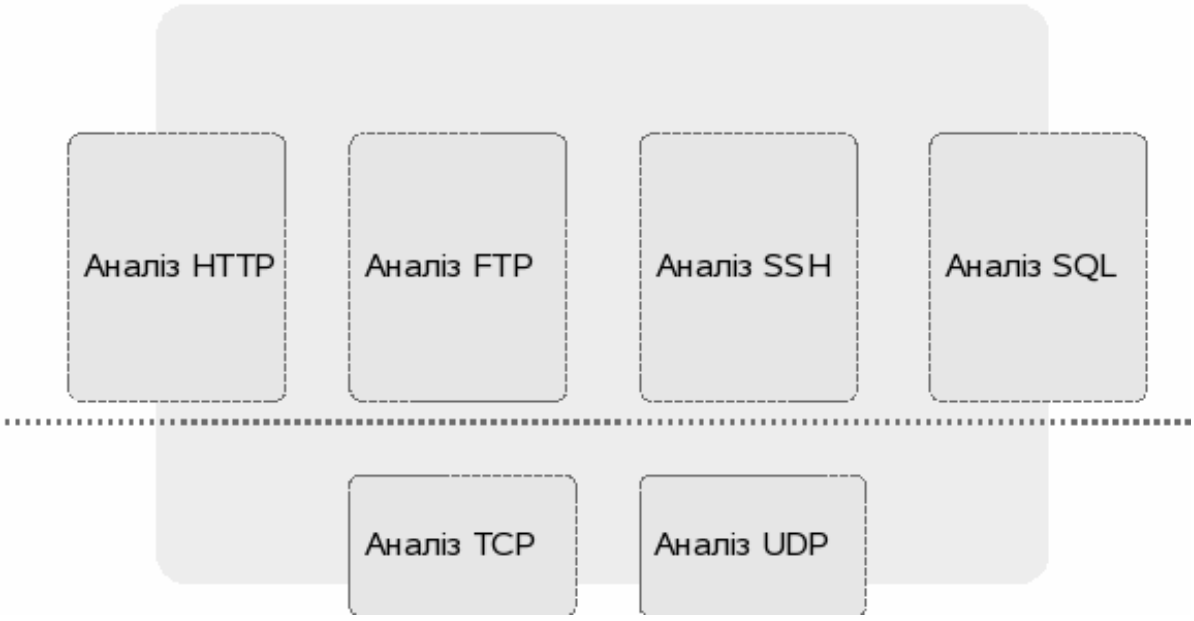

Рис. 3. Загальна структура сенсора

Генерація моделей для кожного протоколу складається з таких етапів:

1) Вибір важливих параметрів з'єднання для базового протоколу/сервісу, мінімізація кількості параметрів для підвищення швидкодії генерації моделей.

2) Генерація моделей оптимальної складності основі відібраних параметрів з основної вибірки. Процес генерації залежить від кількості параметрів у вибірці. Оскільки зазвичай кількість параметрів навіть після мінімізації залишається достатньо великою, обчислення виконують паралельно в обчислювальному кластері з використанням механізмів MPI [mpich].

3) Тестування ефективності отриманої моделі на основі тестової вибірки та роботи з не маркованими даними.

4) Тестування роботи готової моделі для реальної мережі.

5) Отримана модель при тестуваннях повинна сповістити про аномалію. Такий трафік ми будемо маршрутизувати в систему-приманку.

Результатом моделювання буде модель оптимальної складності, яка для цього типу трафіку може ідентифікувати певний сегмент з'єднання як нормальний або аномальний. Якщо частота появи аномального трафіку перетинає певний поріг, всі подальші сесії від цього джерела, а також такі, в яких є подібні запити та параметри з'єднання, маршрутизуються в приманку для запобігання виявленню розбіжностей у відповідях автентичного сервера та приманки.

Висновки. У статті описано застосування комбінаторного алгоритму методу групового врахування аргументів при генерації моделей мережевого трафіку. В результаті аналізу показано, що МГВА найпридатніший для отримання нефізичних моделей мережевого трафіку і для оперування з неперервними змінними, чим власне і є мережевий трафік. Індуктивні методи дають можливість отримання точної ідентифікації або прогнозу різних складних процесів у разі коротких або зашумлених вхідних даних, що вигідно вирізняє їх з-поміж інших багаторядних систем розпізнавання образів.

Особливістю запропонованої системи є використання нестандартних методів аналізу та фільтрації мережевого трафіку з використанням адаптивної фільтрації та алгоритмів багаторядної селекції.

Розроблений мережевий сенсор на базі відповідних моделей, які будуть отримані за допомогою МГВА для нормального та аномального трафіку, який складається із декількох шарів, кожен з яких має певні параметри та орієнтований на відповідні протоколи.

Метою подальших досліджень буде числове моделювання на базі розробленої системи, яке дає змогу ефективно порівняти її з відомими в світі системами подібного виду, враховуючи параметри точності та швидкодії.

Отже, запропонована система дасть змогу заощадити кошти завдяки самодостатності, використанню алгоритмів самонавчання, самоорганізації, саморегулюванню, а також підвищити ефективність використання систем-приманок.

1. Group Method of Data Handling http://www.gmdh.net/. 2. KDD Cup 1999 Data, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. 3. Ивахненко А.Г., Ивахненко Г.А. Обзор задач, решаемых по алгоритмам метода группового учета аргументов (МГУА). 4. Івахненко О.Г., Івахненко Г.О. Індуктивні методи прогнозування та аналізу складних економічних систем. 5. Ивахненко А.Г., Коппа Ю.В., Степашко В.С., Справочник по типовым программам моделирования. – К.: Техніка, 1980. – 184 с. 6. Ивахненко А.Г., Савченко Е.А., Ивахненко Г.А., Надирадзе А.Б., Рогов А.О. Обнаружение закономерностей взаимодействия ионов с поверхностью материалов по комбинаторному алгоритму МГУА.