DOI 10.34185/1562-9945-6-137-2021-10
УДК 004.056:004.94

В.І. Корнієнко, О.В. Герасіна, Д.С. Тимофєєв, О.О. Сафаров, Ю.В. Ковальова

МОДЕЛІ МОНІТОРИНГУ САМОПОДІБНОГО ТРАФІКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ АТАК

Анотація. Розглянуті авторегресійні, фрактальні та мультифрактальні моделі мережевого самоподібного трафіку, які дозволяють формувати адекватну еталонну модель (шаблон) «нормального» трафіку і за нею виявляти аномалії трафіку в системах виявлення та запобігання атак. Шляхом моделювання визначено, що сигнали нейромережевого і нейровейвлетного адаптивних фільтрів-апроксиматорів, а також гібридної та бета мультивейвлетних моделей адекватні експериментальному сигналу трафіка та мають відповідні статистичні закономірності і характеристики.
Ключові слова: системи виявлення атак, самоподібний трафік, мультифрактальні вейвлет моделі, адаптивні фільтри-апроксиматори, авторегресійні моделі.

Постановка проблеми. Захист критичних об'єктів інфраструктури від кібератак є надзвичайно важливим. При цьому, наприклад, до основних загроз для промислових систем управління відносяться, зокрема: мережеві атаки через корпоративні мережі; атаки на стандартні мережеві компоненти; атаки типу «відмова в обслуговуванні» тощо [1].

Одним із рішень актуальної задачі захисту інформаційно-комунікаційних мереж (ІКМ) від кібератак є розробка та вдосконалення систем виявлення та запобігання атак (СВА) [1-3]. Головним завданням таких систем є саме виявлення мережевих атак, спроб несанкціонованого доступу та використання ресурсів мережі.

Аналіз останніх досліджень і публікацій. Основна задача СВА зводиться до оперативного виявлення вторгнень в ІКМ та ініціювання ефективного захисного сценарію щодо припинення факту порушення конфіденційності, доступності та цілісності інформаційних ресурсів, сервісів [4]. За способами виявлення атак в СВА розрізняють системи виявлення зловживань та системи виявлення аномалій [2-4].

Технологія виявлення атак на основі аномалій побудована на припущенні, що аномальна поведінка суб'єкта інформаційної діяльності (атака), зазвичай,

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

проявляється як відхилення від нормальної поведінки, що проявляється в мережевому трафіку. При цьому в процесі функціонування СВА виконується моніторинг мережевої активності ІКМ, на основі чого оцінюються показники, що характеризують штатне функціонування ІКМ, тобто визначається «нормальний» мережевий трафік. Опісля за статистичними правилами (критерієм) приймається рішення о стані ІКМ [2, 4-6].

Головною перевагою такого підходу в СВА є можливість в процесі моніторингу мережевого трафіку відрізняти «нормальну» мережеву активність від «аномальної».

Основний недолік такого підходу полягає у складнощах визначення шаблону «нормального» трафіку.

При цьому перспективним є використання моделей захисту на основі розпізнавання аномалій в ІКМ [7-10], оскільки поточний трафік є реалізацією випадкового процесу, а його адекватна модель – статистично стійка закономірність цього процесу.

Трафік в ІКМ є нелінійним стохастичним процесом з властивостями самоподоби та з хаотичною і фрактальною динамікою. Крім того, встановлено, що агрегований трафік від різних джерел на малих часових масштабах проявляє мультифрактальний характер [11, 12].

Оцінка характеристик мережевого трафіку необхідна для побудови його адекватної моделі, що дозволяє сформувати еталонну модель (шаблон) «нормального» трафіку і за нею виявляти аномалії трафіку в СВА.

Таким чином, невирішеною задачею є побудова адекватних моделей мережевого самоподібного трафіку, які б дозволяли їх використання в СВА для виявлення мережевих аномалій в реальному масштабі часу з достатньою ефективністю відносно похибок та достовірності.

Мета роботи – дослідження та обґрунтування моделей мережевого самоподібного трафіку для виявлення його аномалій при використанні в системах виявлення та запобігання атак.

Викладення основного матеріалу дослідження. Моделі мережевого самоподібного трафіку. Фрактальним (самоподібним) є стаціонарний випадковий процес X із постійним середнім і автокореляційною функцією (АКФ), яку можна записати як:

$$r(k) \sim L_1(t)k^{-\beta} \text{ при } k \to \infty \qquad (1)$$

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

де L_1 – поволі змінювана на нескінченності функція, тобто для $x > 0$ вона має $\lim_{t\to\infty} L_1(xt)/L_1(t) = 1$; $\beta = 2 - 2H$; $0 < \beta < 1$; H – показник Херста.

Показник Херста H характеризує ступінь самоподоби процесу. Він свідчить про наявність тренда або про випадковість процесу, а також характеризує еволюцію системи (процесу). Якщо $0{,}5 < H < 1$, то процес характеризується довготривалою пам'яттю і є персистентним, для якого ймовірним є збереження тенденції еволюції системи в майбутньому. Якщо ж $0 < H < 0{,}5$, то це говорить про антиперсистентність процесу. Його часові реалізації мінливі і складаються з частих реверсів спад-підйом. Тобто для них збільшення (зменшення) значень в минулому означає ймовірне їх зменшення (збільшення) в майбутньому.

Для самоподібних процесів АКФ має довготривалу залежність, спектральна щільність підкорюється ступеневому закону, а розподіл має «важкий хвіст» [11].

Якщо дисперсія вибіркового середнього має повільніший спад, ніж величина, зворотна довжині вибірки, то даний процес є самоподібним.

Найчастіше для апроксимації гістограм експериментальних даних самоподібних процесів застосовуються функції субекспоненціальних законів розподілу, для перевірки адекватності яких використовуються критерії згоди Колмогорова і Пірсона.

Для перевірки нульової гіпотези про незалежність і тотожність розподілу значень часового ряду використовується BDS-тест, який дозволяє виявити нелінійність породжуючої системи, відрізнити випадкові системи від детермінованого хаосу або від нелінійних стохастичних систем.

Для визначення режиму породжуючого процесу оцінюють його ентропію Колмогорова K, яка характеризує швидкість втрати інформації про стан динамічної системи в часі. К-ентропія дорівнює нулю при регулярному русі, нескінченна для випадкових систем, позитивна і обмежена для хаотичних систем.

Значення кореляційної ентропії K_C є нижньою межею К-ентропії і дозволяє оцінити інтервал точної прогнозованості процесу T_C. За час, більший T_C, можливе тільки статистичне прогнозування.

Розмірність фазового простору d, починаючи з якої кореляційна розмірність D_C перестає змінюватися, є мінімальною розмірністю вкладення атрактора (найменшою цілою розмірністю фазового простору, що вміщує весь атрактор). Таким чином, розмірність d визначає порядок породжуючої системи (глибину її пам’яті).

Моделі фрактальних рухів. Фрактальний броунівський рух (ФБР) – це процес, що має приріст координати броунівської частинки для будь-якої пари моментів часу t і t_0 виду

$$x(t) - x(t_0) \sim \xi |t - t_0|^H, \ (t \geq t_0), \ 0 < H < 1, \tag{2}$$

де $x(t_0)$ – координата частинки в деякий початковий момент часу t_0; ξ – стандартний гаусовий випадковий процес з незалежними приростами; H – показник Херста. ФБР має нульове середнє, дисперсію приростів, яка збільшується з часом, а також нескінченно великий час кореляції.

Фрактальний гаусовий шум (ФГШ) – це строго самоподібний в широкому сенсі стохастичний процес з нульовим середнім та дисперсією виду

$$D[B_H(t) - B_H(t_0)] = D[\xi] \cdot |t - t_0|^{2H}, \tag{3}$$

де B_H – ФБР з показником Херста H і АКФ виду

$$r(k) = \left[|k+1|^{2H} - |2k|^{2H} + |k-1|^{2H} \right], \tag{4}$$

де $k \in N$, $0 < H < 1$.

Для побудови ФБР застосовують, наприклад, метод біортогональних вейвлетів, залежних від заданого базису і параметра Херста H. Основна ідея полягає у використанні дискретного вейвлет-перетворення (ДВП), деталізуючі коефіцієнти на кожному рівні якого є незалежними нормально розподіленими випадковими величинами, а апроксимуючі коефіцієнти – результат використання фрактальної авторегресійної інтегральної моделі з ковзним середнім (FARIMA) процесу:

$$B_H(t) = \sum_{k=-\infty}^{\infty} \Phi_H(t-k) S_k^{(H)} + \sum_{j=0}^{\infty} \sum_{k=-\infty}^{\infty} 2^{-jH} \Psi_H(2^j t - k) \varepsilon_{j,k} - b_0, \tag{5}$$

де Ψ_H, Φ_H – біортогональний вейвлет та відповідна їй скейлінг функції; $S_k^{(H)}$ – стаціонарний гаусовий процес FARIMA; $\varepsilon_{j,k}$ – незалежні гаусові випадкові величини; b_0 – константа, така що $B_H(0) = 0$.

Перевагами моделей ФБР і ФГШ є властивості самоподоби і довготривалої залежності, що відповідають властивостям експериментальних даних, а також можливість їх аналітичного трактування. Проте, їх недоліки полягають в обмеженнях опису мережевого трафіку і складнощах підбору значень параметрів для генерації трафіку, подібного до експериментальних даних. Крім цього, єдиного параметра, що характеризує кореляційну структуру (асимптотичне убування) ФБР і ФГШ, недостатньо для моделювання трафіку.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Фрактальний рух Леві є узагальненням ФБР, представником класу α-стійких процесів. Він має властивості самоподоби і нескінченний інтервал кореляції. Прирости даного процесу є самоподібними з $H = 1/\alpha 1$ і залежними один від одного, а також мають розподіли з «важкими хвостами». Відповідно, модель враховує два показники: Херста $H \in [1/2,1]$ і Леві $\alpha 1 \in [0,1]$. Позитивами даної моделі є можливість її математичного опису, а також здатність враховувати розподіл з «важким хвостом». Серед недоліків варто відзначити необхідність враховувати декілька параметрів, що визначають стан моделі (зокрема, для визначення показника $\alpha 1$ відсутній прямий метод оцінки).

Переваги моделей фрактальних рухів: концептуально прості; можуть описати складну динаміку багатьох реальних систем; відносно мале число параметрів і їх вибір наочний; дозволяють виявити стійкі стани системи.

Авторегресійні моделі припускають, що поточне значення процесу є сумою постійної, зваженої суми попередніх значень і похибки моделі. Прикладами таких моделей є: ARMA (авторегресійна модель ковзного середнього), ARIMA (авторегресійна інтегральна модель ковзного середнього) і FARIMA.

При оцінюванні та ідентифікації процесів для реалізації авторегресійних моделей використовують також адаптивні фільтри-апроксиматори (АФА), процес адаптації яких включає оцінювання шуканого виходу фільтра та корегування його параметрів в залежності від значення вихідної похибки.

Серед них можна виділити нейромережеві (НМ) та нейро-вейвлетні (НВ) АФА [11]. Нейромережеві (НМ) моделі представляють собою набір сполучених між собою нейронів, для яких перетворення вхідного вектора у вихідний задається значеннями вагів мережі. Вихідні значення нейронів залежать від вибору функції активації.

Серед НМ моделей найкращі результати показує гетерогенна мережа, що складається з прихованих шарів з нелінійною функцією активації нейронів і вихідного лінійного нейрона.

Рівняння АФА на основі НМ прямого розповсюдження з прихованим шаром представляється у вигляді рівняння згортки [11]:

$$\hat{x}[k+n] = \sum_{\tau \in P} F_{\hat{x}} \{ \sum_{l \in Q} v_l[\tau] \cdot F_l (\sum_{m \in Q} v_{l,m}[\tau] \cdot u_m[k-\tau]) \}, \quad (6)$$

де P – множина глибин пам'яті відповідних входів; $F_{\hat{x}}$ – активаційна функція вихідного шару НМ; Q – множина входів нейронів; l – порядковий номер входу вихідного шару НС; v_l – вагові коефіцієнти вихідного шару; F_l – активаційна

функція нейронів прихованого шару; m – порядковий номер входу НМ; $v_{l,m}$ – вагові коефіцієнти зв'язку m-го входу і l-го нейрона; u_m – вхід НМ.

Параметрами настройки цієї НМ є $\{v_l, v_{l,m}\} \subset a$, де a – вектор параметрів навчання мережі.

Зазвичай для настройки параметрів НМ прямого розповсюдження (6) використовують градієнтні алгоритми, наприклад, алгоритм зворотного поширення помилки в просторі параметрів a при заданій архітектурі НМ і структурних функціях F.

Перевагами НМ моделей є: автоматичне набуття знань; масштабованість; можливість навчання; нелінійність моделей; адаптивність; одноманітність аналізу і проектування. Серед недоліків варто відзначити: складний аналіз навченої мережі; процес їх навчання вимагає немало часу; труднощі вибору алгоритму навчання і архітектури мережі; жорсткі вимоги до навчальної вибірки.

Фільтри з частотним перетворенням мають переваги над фільтрами зі згорткою в часовій області, завдяки скороченню об'єму обчислень і покращенню властивості збіжності алгоритмів адаптації. При цьому, в наслідок здатності представляти нестаціонарні сигнали більш доцільним є використання дискретного час-частотного (вейвлет) перетворення, якому притаманні властивості ортонормованості, компактності, відновлення без втрат і малого об'єму обчислень.

Прикладом такого фільтру є нейронний вейвлет (НВ) АФА [11], в основу фільтрації якого покладена процедура прямого ДВП. Для зменшення впливу шуму у фільтрі здійснюють трешолдинг – порогове обмеження коефіцієнтів вейвлет розкладання. НМ використовується для прогнозування значень коефіцієнтів, по яким за допомогою зворотнього ДВП визначається прогнозований сигнал.

Рівняння НВ АФА має вигляд:

$$\hat{x}[k+1] = \sum_{p=1}^{P_L} \hat{a}_{L,p} \cdot \phi_{L,p}[k+1] + \sum_{l=1}^{L} \sum_{p=1}^{P_l} \hat{d}_{l,p} \cdot \psi_{l,p}[k+1]. \quad (7)$$

де ϕ, ψ – масштабуюча і відповідна їй вейвлет функції; L – кількість рівнів розкладання; P_l – кількість коефіцієнтів на рівні розкладання l; $\hat{a}_{L,p}$, $\hat{d}_{L,p}$ – коефіцієнти апроксимації і деталізації відповідно.

До параметрів АФА, що навчаються (адаптуються), відносяться тип базисного вейвлета ψ, кількість рівнів розкладання L, а також параметри трешолдинга і НМ.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Мультифрактальні моделі ґрунтуються на використанні мультиплікативних каскадів, що застосовують ітеративну процедуру.

Спочатку одиничний інтервал ділиться на два рівні підінтервали, вагові коефіцієнти яких r_1 і $r_2 = 1 - r_1$ відповідно. Для кожного підінтервалу процедура повторюється. Вагові коефіцієнти є незалежними, випадковими і однаково розподіленими величинами $R \in [0,1]$ з функцією розподілу вірогідності $F_R(x)$, $M[R] = 1/2$. На k-ому кроці ітеративної процедури міра $\mu(\Delta t_k)$ підінтервалу довжини $\Delta t_k = 2 - k$ задовольняє співвідношенню масштабування:

$$M\left[\mu(\Delta t_k)^q\right] = \left(M\left[R^q\right]\right)^k = \Delta t_k^{-\log M\left[R^q\right]}, \tag{8}$$

яке визначає мультифрактальний процес з функцією масштабування:

$$\tau_0(q) = -\log_2 M\left[R^q\right]. \tag{9}$$

Завдання каскадного моделювання полягає в знаходженні розподілу вірогідності для множників R такого, щоб виконувалась рівність (9).

Не менш поширеними є мультифрактальні вейвлет моделі (МВМ) [12], що дозволяють моделювати позитивні часові ряди заданої довжини. В основі їх функціонування лежить метод вейвлет перетворення, а часовий має вигляд:

$$x(t) = \sum_k U_{J_0,k}\phi_{J_0,k}(t) + \sum_{i=J_0}^{\infty}\sum_k W_{j,k}\psi_{j,k}(t), \tag{10}$$

де $\psi_{j,k}(t) = 2^{j/2}\psi\left(2^j t - k\right), \phi_{j,k}(t) = 2^{j/2}\phi\left(2^j t - k\right)$ – вейвлет та відповідна йому масштабуюча функція; $W_{j,k} = \int x(t)\psi_{j,k}(t)dt$ – деталізуючі коефіцієнти; $U_{j,k} = \int x(t)\phi_{j,k}(t)dt$ – апроксимуючі (скейлінг) коефіцієнти; j – кількість рівнів вейвлет-розкладання; $j = J_0$ – найменша роздільна здатність; k показує просторове розташування аналізу.

Враховуючи, що на практиці часто розглядається дискретний сигнал $x^{(n)}(k)$ з кінцевою тривалістю, що апроксимує сигнал $x(t)$ з роздільною здатністю 2^{-n}, то напівнескінченну суму в (10) необхідно замінити на суму з кінцевим числом масштабів, тобто $0 \le j \le n$:

$$U_{j-1,k} = 2^{-1/2}\left(U_{j,2k} + U_{j,2k+1}\right), \tag{11}$$

$$W_{j-1,k} = 2^{-1/2}\left(U_{j,2k} - U_{j,2k+1}\right), \tag{12}$$

$$W_{j,k} = A_{j,k}U_{j,k}, \tag{13}$$

де $A_{j,k}$ – незалежні, випадкові, симетричні відносно нуля змінні $A_{j,k} \in [-1,1]$. Для простоти і гнучкості генерування множників $A_{j,k}$ використовується симетричні бета-розподіл та розподіл точкових мас.

Тоді отримаємо

$$U_{j,2k} = 2^{-1/2}\left(1 + A_{j+1,k}\right)U_{j-1,k}, \tag{14}$$

$$U_{j,2k+1} = 2^{-1/2}\left(1 - A_{j+1,k}\right)U_{j-1,k} \tag{15}$$

Скейлінг-коефіцієнти, обчислені при детальній роздільній здатності, є вихідними значеннями процесу, тобто

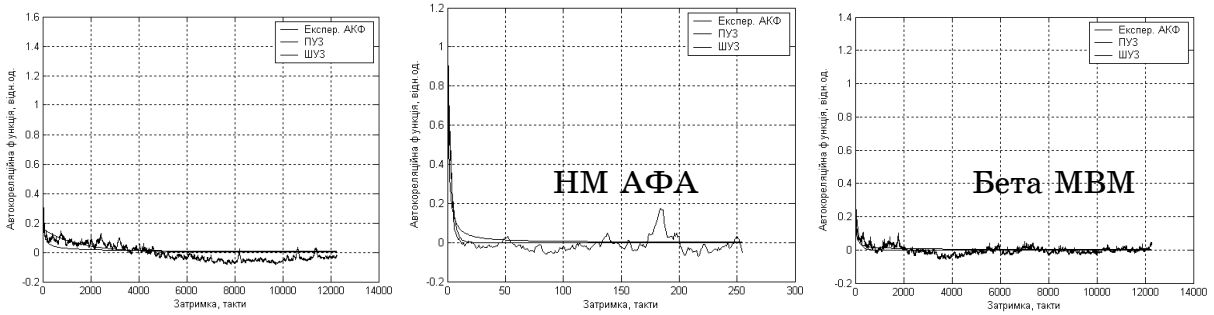
$$x^{(n)}[k] = 2^{-n/2}U_{n,k},\ k = 0,...,2^n - 1. \tag{16}$$

Мультифрактальні моделі забезпечують гнучкіший закон масштабної поведінки і вдало відтворюють трафік, агрегований від декількох джерел, що істотно відрізняються; аналітично прості. Проте вони оцінюють тільки верхню огинаючу мультифрактального спектру, що може призводити до помилкових результатів.

Аналіз та моделювання мережевого трафіку. Використовувався експериментальний сигнал трафіку, що передавався через мережу Інтернет і який являє собою залежність розміру Ethernet кадрів в байтах від часу [13]. Для того, щоб привести початкові дані до еквідистантної шкали по часовій осі була проведена процедура агрегації з кроком в 5 с.

Результати аналізу та моделювання наведені на рис. 1-3 та в табл. 1.

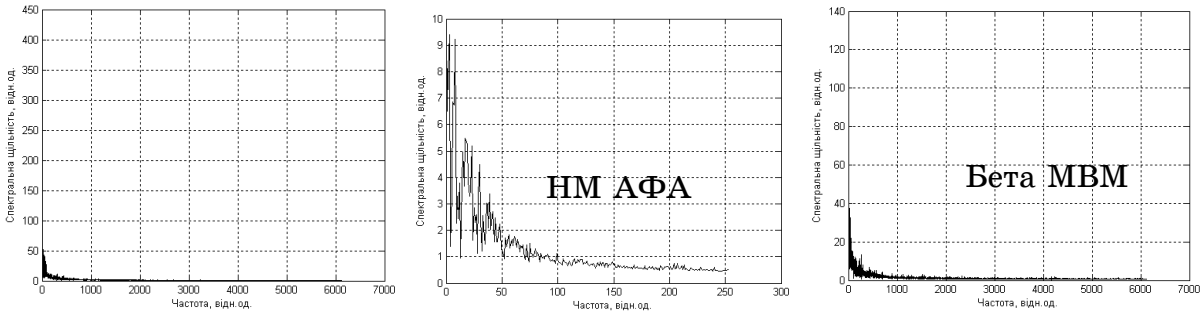
Породжуючий процес експериментального сигналу має властивості, притаманні самоподібним процесам: гіперболічне убування АКФ із зростанням часової затримки (рис. 1,а), ступеневий закон графіка його спектральної щільності (рис. 2,а) та поволі убуваючу дисперсію (рис. 3,а). На графіках АКФ також наведені їх апроксимації у вигляді поволі (ПУЗ) та швидко (ШУЗ) убуваючих залежностей.



а б в

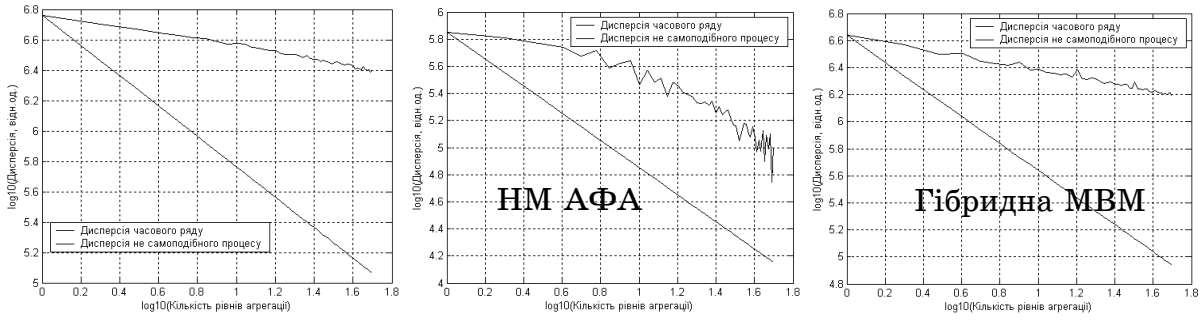
Рисунок 1 - АКФ експериментального (а) та модельних:
НВ АФА (б), Бета МВМ (в) сигналів

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)



а б в

Рисунок 2 - Спектри експериментального (а) та модельних:
НВ АФА (б), Бета МВМ (в) сигналів



а б в

Рисунок 3 - Дисперсії експериментального (а) та модельних:
НВ АФА (б), гібридна МВМ (в) сигналів

Сигнал трафіку має (табл. 1) розподіл з «важким хвостом» (показник «важкості хвоста» становить α =1,4), гістограма експериментального розподілу згідно з критеріями згоди Колмогорова і Пірсона відповідає розподілу Парето, скейлетон вейвлет-перетворення сигналу має деревоподібну структуру, а показник Херста має діапазон значень [0,888; 0,980]. Процес також є нелінійним відповідно до результатів BDS-тесту. Гіпотези про тотожність розподілу значень сигналу приймались з вірогідністю 95 %.

Значення кореляційних ентропії і розмірності атрактору, а також інтервал точної передбачуваності (глибина точного прогнозу) експериментального сигналу наведені в табл. 1.

При моделюванні у якості моделей трафіку використовувались НМ і НВ АФА, а також мультифрактальні вейвлет моделі двох типів: МВМ з бета-розподілом та гібридна МВМ, в якій бета розподіл використовується на грубих масштабах, а розподіл точкових мас – на точних масштабах.

Таблиця 1

Характеристики експериментального та модельних сигналів

	Експери-ментальний	**Бета МВМ**	**Гібридна МВМ**	**НМ АФА**	**НМ АФА**
АКФ	ПУЗ			ШУЗ	
Спектр	Ступеневий закон				
Вейвлет-перетворення	Деревоподібна структура скейлетона				
Дисперсія	Поволі убуваюча				
Закон розподілу за критерієм: - Колмогорова - Пірсона	Парето Парето		Парето Логнорм	Логнорм Логнорм	Парето Експоненц
Показник «важкості хвоста»	~1,4	~1,5	~1,2	~1,2	~1,5
BDS-тест	Хаотичний нелінійний процес				
Показник Херста: - періодограмний метод - метод агрегованої дисперсії - R/S аналіз	0,980 0,888 0,913	0,940 0,843 0858	0,884 0,869 0,877	0,936 0,687 0,788	0,974 1,454 0,764
Кореляційна розмірність	2,956	2,978	2,864	3,992	3,483
Кореляційна ентропія	0,640	0,742	0,857	0,826	0,643
Інтервал прогнозованості	2,525	2,178	1,886	3,063	2,987
Розмірність фазового простору	3	3	3	4	4

В результаті адаптації та навчання моделей, АКФ (див рис. 1,б,в), спектри (див. рис. 2,б,в) та дисперсії (див. рис. 3,б,в) модельних сигналів якісно відповідають графікам експериментального сигналу. Крім того, якісні та числові зна-

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

чення характеристик модельних сигналів в цілому відповідають характеристикам експериментального сигналу (див. табл. 1).

При цьому бета МВМ мають меншу похибку визначення характеристик, ніж гібридні МВМ, а відносна середньоквадратична похибка апроксимації експериментального сигналу за допомогою НМ АФА не перевищує 0,046.

Статистична перевірка за непараметричним критерієм знаків дозволила встановити адекватність експериментального і модельних сигналів з рівнем значущості 0,01.

Висновки

Розглянуті авторегресійні, фрактальні та мультифрактальні моделі мережевого самоподібного трафіку, які дозволяють формувати адекватну еталонну модель (шаблон) «нормального» трафіку і за нею виявляти аномалії трафіку в СВА.

Визначено, що сигнали нейромережевого і нейровейвлетного адаптивних фільтрів-апроксиматорів, а також гібридної та бета мультивейвлетних моделей адекватні експериментальному сигналу трафіка та мають відповідні статистичні закономірності і характеристики.

Подальші дослідження мають бути спрямовані на розробку та використання прогнозуючих моделей самоподібного трафіку в СВА, що дозволить підвищити оперативність виявлення атак.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Проблеми захисту критично важливих об’єктів інфраструктури / Н. Лукова-Чуйко, В. Наконечний, С. Толюпа, Р. Зюбіна // Безпека інформаційних систем і технологій. – 2020. – № 1(2). – С. 31-39.

2. Браницкий А.А. Анализ и классификация методов обнаружения сетевых атак / А.А. Браницкий, И.В. Котенко // Труды СПИИРАН. – 2016. – № 2(45). – С. 207-244. [Електронний ресурс] – Режим доступу: www.proceedings.spiiras.nw.ru.

3. Носенко К.М. Огляд систем виявлення атак в мережевому трафіку / К.М. Носенко, О.І. Півторак, Т.А. Ліхоузова // Міжвідомчий науково-технічний збірник «Адаптивні системи автоматичного управління». – 2014. – № 1(24). – С. 67-75.

4. Довбешко С.В. Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак / С.В. Довбешко, С.В. Толюпа, Я.В. Шестак // Сучасний захист інформації. – 2019. – №1(37). – С. 6-15.

5. Смирнов А. Имитационная модель NIPDS для обнаружения и предотвращения вторжений в телекоммуникационных системах и сетях / А. Смирнов, Ю. Дрейс, Д. Даниленко // Ukrainian Scientific Journal of Information Security. – 2014. – Vol. 20, issue 1. – P. 29-35.

6. Лазаренко С.В. Особливості функціонування систем виявлення атак на автоматизовані системи / С.В. Лазаренко // Сучасний захист інформації. – 2015. – № 1. – С. 33-40.
7. Гулак Г.М. Модель системи виявлення вторгнень з використанням двоступеневого критерію виявлення мережевих аномалій / Г.М. Гулак, В.В. Семко, П.М. Складанний // Сучасний захист інформації. – 2015. – №4. – С. 81-85.
8. Разработка модели интеллектуального распознавания аномалій и кибератак с использованием логических процедур, базирующихся на покрытиях матриц признаков / Г. Бекетова, Б. Ахметов, А. Корченко, В. Лахно // Ukrainian Scientific Journal of Information Security. – 2016. – Vol. 22, issue 3. – P. 242-254.
9. Петров О. Метод та модель інтелектуального розпізнавання загроз інформаційно-комунікаційному середовищу транспорту / О. Петров, О. Корченко, В. Лахно // Ukrainian Scientific Journal of Information Security. – 2015. – Vol. 21, issue 1. – P. 26-34.
10. Карачанская Е.В. Метод выявления аномалий сетевого трафика, основанный на его самоподобной структуре / Е.В. Карачанская, Н.И. Соседова // Безопасность информационных технологий. – 2019. – С. 98-110. [Електронний ресурс] – Режим доступу: https://bit.mephi.ru/index.php/bit/article/view/1185.
11. Корнієнко В.І. Інтелектуальне моделювання нелінійних динамічних процесів в системах керування, кібербезпеки, телекомунікацій: підручник / В.І. Корнієнко, О.Ю. Гусєв, О.В. Герасіна; за заг. ред. В.І. Корнієнка ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро : НТУ «ДП», 2020. – 536 с.
12. A multifractal wavelet model with application to network traffic / R.H. Riedi, M.S. Crouse, V. Ribeiro, R.G. Baraniuk // IEEE Transactions on Information Theory. – 1999. – V. 45. – P. 992-1018.
13. Архів трафіку [Електронний ресурс] – Режим доступу: http://ita.ee.lbl.gov.

REFERENCES

1. Problemy zakhystu krytychno vazhlyvykh obiektiv infrastruktury / N. Lukova-Chuiko, V. Nakonechnyi, S. Toliupa, R. Ziubina // Bezpeka informatsiinykh system i tekhnolohii. – 2020. – № 1(2). – P. 31-39.
2. Branytskyi A.A. Analiz i klassifikaciya metodov obnaruzheniya setevykh atak / A.A. Branytskyi, I.V. Kotenko // Trudy SPIIRAN. – 2016. – № 2(45). – P. 207-244. [Electronic resource] – Access mode: www.proceedings.spiiras.nw.ru.
3. Nosenko K.M. Ohliad system vyiavlennia atak v merezhevomu trafiku / K.M. Nosenko, O.I. Pivtorak, T.A. Likhouzova // Mizhvidomchyi naukovo-tekhnichnyi zbirnyk «Adaptyvni systemy avtomatychnoho upravlinnia». – 2014. – № 1(24). – P. 67-75.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

4. Dovbeshko S.V. Zastosuvannia metodiv intelektualnoho analizu danykh dlia pobudovy system vyiavlennia atak / S.V. Dovbeshko, S.V. Toliupa, Ya.V. Shestak // Suchasnyi zakhyst informatsii. – 2019. – № 1(37). – P. 6-15.
5. Smirnov A. Imitacionnaya model' NIPDS dlya obnaruzheniya i predotvrashcheniya vtorzhenij v telekommunikacionnykh sistemakh i setyakh / A. Smirnov, Yu. Drejs, D. Danilenko // Ukrainian Scientific Journal of Information Security. – 2014. – Vol. 20, issue 1. – P. 29-35.
6. Lazarenko S.V. Osoblyvosti funktsionuvannia system vyiavlennia atak na avtomatyzovani systemy / S.V. Lazarenko // Suchasnyi zakhyst informatsii. – 2015. – № 1. – P. 33-40.
7. Hulak H.M. Model systemy vyiavlennia vtorhnen z vykorystanniam dvostupenevoho kryteriiu vyiavlennia merezhevykh anomalii / H.M. Hulak, V.V. Semko, P.M. Skladannyi // Suchasnyi zakhyst informatsii. – 2015. – №4. – P. 81-85.
8. Razrabotka modeli intellektual'nogo raspoznavaniya anomalij i kiberatak s ispol'zovaniem logicheskikh procedur, baziruyushchikhsya na pokrytiyakh matric priznakov / G. Beketova, B. Akhmetov, A. Korchenko, V. Lakhno // Ukrainian Scientific Journal of Information Security. – 2016. – Vol. 22, issue 3. – P. 242-254.
9. Petrov O. Metod ta model intelektualnoho rozpiznavannia zahroz informatsiinokomunikatsiinomu seredovyshchu transportu / O. Petrov, O. Korchenko, V. Lakhno // Ukrainian Scientific Journal of Information Security. – 2015. – Vol. 21, issue 1. – P. 26-34.
10. Karachanskaya E.V. Metod vyyavleniya anomalij setevogo trafika, osnovannyj na ego samopodobnoj strukture / E.V. Karachanskaya, N.I. Sosedova // Bezopasnost' informacionnykh tekhnologij. – 2019. – C. 98-110. [Electronic resource] – Access mode: https://bit.mephi.ru/index.php/bit/article/view/1185.
11. Korniienko V.I. Intelektualne modeliuvannia neliniinykh dynamichnykh protsesiv v systemakh keruvannia, kiberbezpeky, telekomunikatsii: pidruchnyk / V.I. Korniienko, O.Yu. Husiev, O.V. Herasina; za zah. red. V.I. Korniienka; M-vo osvity i nauky Ukrainy, Nats. tekhn. un-t «Dniprovska politekhnika». – Dnipro : NTU «DP», 2020. – 536 p.
12. A multifractal wavelet model with application to network traffic / R.H. Riedi, M.S. Crouse, V. Ribeiro, R.G. Baraniuk // IEEE Transactions on Information Theory. – 1999. – V. 45. – P. 992-1018.
13. Arkhiv trafiku [Electronic resource] – Access mode: http://ita.ee.lbl.gov.

Received 28.09.2021.
Accepted 01.10.2021.

Модели мониторинга самоподобного трафика информационно-коммуникационных сетей для систем обнаружения атак

Рассмотрены авторегрессионные, фрактальные и мультифрактальные модели сетевого самоподобного трафика, которые позволяют формировать адекватную эталонную модель (шаблон) «нормального» трафика и по ней выявлять аномалии трафика в системах обнаружения и предотвращения атак. Путем моделирования определено, что сигналы нейросетевого и нейровейвлетного адаптивных фильтров-аппроксиматоров, а также гибридной и бета мультивейвлетних моделей адекватны экспериментальному сигналу трафика и имеют соответствующие статистические закономерности и характеристики.

Models of monitoring of self-like traffic of information and communication networks for attack detection systems

Autoregressive, fractal and multifractal models of network self-similar traffic are considered, which allow to form an adequate reference model (template) of "normal" traffic and to detect traffic anomalies in attack detection and prevention systems. Models of fractal Brownian motion and fractal Gaussian noise were considered as models of fractal motions, because they have self-similarity and long-term dependence properties that correspond to the properties of experimental data, as well as the possibility of their analytical interpretation. When evaluating and identifying processes for the implementation of autoregressive models use adaptive filters-approximators, among which there are neural network and neuro-wavelet. The following were used as multifractal models: a multifractal wavelet model with a beta distribution and a hybrid multifractal wavelet model in which the beta distribution is used on a coarse scale and the distribution of point masses on an accurate scale By modeling as a result of adaptation and learning of models, autocorrelation functions, spectra and variances of model signals qualitatively correspond to the graphs of the experimental signal. In addition, the qualitative and numerical values of the characteristics of the model signals generally correspond to the characteristics of the experimental signal. In this case, beta multifractal wavelet models have a smaller error of determination of characteristics than hybrid multifractal wavelet models, and the relative root mean square error of approximation of the experimental signal using a neural network adaptive filter approximator does not exceed 0.046. Statistical verification by non-parametric criterion of signs allowed to establish the adequacy of experimental and model signals with a significance level of 0.01. Further research should be aimed at developing and using predictive models of self-similar traffic in attack detection and prevention systems, which will increase the efficiency of attack detection.

Корнієнко Валерій Іванович – завідувач кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», д.т.н., професор.

Герасіна Олександра Володимирівна – доцент кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», к.т.н., доцент;

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Тимофєєв Дмитро Сергійович – старший викладач кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка»;
Сафаров Олександр Олександрович – доцент кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», к.т.н.;
Ковальова Юлія Вікторівна – асистент кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», к.т.н.

Корниенко Валерий Иванович – заведующий кафедры безопасности информации и телекоммуникаций, Национальный технический университет «Днепровская политехника», д.т.н., профессор.
Герасина Александра Владимировна – доцент кафедры безопасности информации и телекоммуникаций, Национальный технический университет «Днепровская политехника», к.т.н., доцент;
Тимофеев Дмитрий Сергеевич – старший преподаватель кафедры безопасности информации и телекоммуникаций, Национальный технический университет «Днепровская политехника»;
Сафаров Александр Александрович – доцент кафедры безопасности информации и телекоммуникаций, Национальный технический университет «Днепровская политехника», к.т.н.;
Ковалева Юлия Викторовна – ассистент кафедры безопасности информации и телекоммуникаций, Национальный технический университет «Днепровская политехника», к.т.н.

Korniienko Valerii – Head of Department of Information Security and Telecommunications, Dnipro University of Technology, Doctor of Technical Sciences, Professor;
Gerasina Oleksandra – Associate Professor of Department of Information Security and Telecommunications, Dnipro University of Technology, Candidate of Technical Sciences, Associate Professor;
Dmytro Tymofieiev – Senior Instructor of Department of Information Security and Telecommunications, Dnipro University of Technology;
Safarov Oleksandr – Associate Professor of Department of Information Security and Telecommunications, Dnipro University of Technology, Candidate of Technical Sciences;
Kovalova Yuliia – Assistant Lecturer of Department of Information Security and Telecommunications, Dnipro University of Technology, Candidate of Technical Sciences.