УДК 681.14

ПРОГНОЗУВАННЯ РІВНЯ ЗАГРОЗ З ВИКОРИСТАННЯМ МЕРЕЖ БАЙЄСА

Міщенко М.В., Гребенник А.Г., Трунова О.В.
Чернігівський національний технологічний університет

У сучасному світі питання кібербезпеки набуло досить великої актуальності, адже питома вага інформації, що знаходиться у електронному вигляді зростає з кожним днем, гостро ставлячи питання про її захист. З відокремленням розподілених інформаційних систем у окремі корпоративні комп'ютерні мережі, інформація стала більш ізольованою від зовнішніх впливів, проте нелінійність та складність протікання процесів в таких мережах, а також ряд загроз, що несе в собі не тільки зовнішній, а й внутрішній мережевий трафік, дає підстави до посилення контролю та аналізу мережевих потоків.

На даний момент існує ряд інформаційних систем, метою яких є виявлення та запобігання мережевим атакам та аномаліям трафіку, проте більшість з них працює в реальному часі з множиною вже відомих загроз, надає інформацію або вживає необхідних дій за фактом настання цієї загрози. Такі системи переважно побудовані на сигнатурному методі виявлення і не враховують шкідливих утручань нового типу та особливостей конкретної комп'ютерної мережі.

Із розвитком та широким розповсюдженням методів штучного інтелекту, активно почали розвиватися системи, які побудовані на адаптивних методах виявлення та прогнозування загроз ПЗ. Зокрема, у 2014 році, Агентством передових оборонних дослідницьких проектів США, було ініційовано створення класу інформаційних систем, побудованих на основі штучного інтелекту, призначених для знаходження, перевірки та виявлення кіберзагроз [1]. Цей клас систем отримав назву Cyber Reasoning Systems (англ. – системи кіберрозсудження) та активно розвивається у сфері кіберзмагань, зокрема Cyber Grand Challenge. Дані системи, працюючи у реальному часі, орієнтовані на висунення гіпотези про існуючі загрози для досліджуваного ПЗ, перевірки цієї гіпотези та її підтвердження або відхилення. Проте на даний момент, системи такого класу є досить енергомісткими та не розраховані на виявлення та прогнозування рівня загроз для корпоративної комп'ютерної мережі [2].

Вирішення проблеми прогнозування загроз для корпоративної комп'ютерної мережі надало б можливість спеціалісту з кібербезпеки завчасно вживати заходів до їх дослідження та усунення. Також, в залежності від обраних методів прогнозування, це допомогло б, з певною точністю, завчасно ідентифікувати наміри атакувальника, зокрема послідовність його дій та джерела можливих загроз.

Одним з найбільш гнучких та точних методів прогнозування рівня загроз є прогнозування рівня загроз за допомогою ймовірнісних мереж

Байєса. Метод прогнозування загроз за допомогою Баєсових мереж досить тісно пов'язаний з підходами, заснованими на графах атаки. Байєсова мережа, як правило, побудована на основі графа атак. Відмінна риса Байєсових мереж – це умовні змінні та ймовірності, які відображені в моделі.

Байєсова мережа – це імовірнісна графова модель, яка складається зі змінних та зв'язків між ними. Дана мережа представляє собою спрямований ациклічний граф з вузлами, представленими дискретними або неперервними змінними, та ребрами, що відображають зв'язки між ними. Вузли утримують стани випадкових величин та форму умовної ймовірності [3].

Для набору випадкових змінних $X = \{x_1, \dots, x_n\}$ у мережі Байєса, функція спільної щільності ймовірності визначається за формулою 1, де $P_a(x_i)$ представляє відповідне значення ймовірності змінних у батьківських вузлах мережі, а $P(x_i/Pa(x_i))$ – умовна ймовірність у дочірніх вузлах.

$$P(x_1, \dots, x_n) = \prod_{i=1}^{n} P(x_i/Pa(x_i)) \quad (1)$$

У Байєсових мережах, ймовірності зв'язків оновлюються за допомогою теореми Байєса, за фактом надходження нової інформації. Таким чином, з появою нових загроз для мережі, побудована мережа Байєса оновлюється та надає актуальні прогнози про рівні загроз.

Реалізацію прогнозування рівня загроз з використанням мереж Байєса необхідно розділити на дві частини:

1. «Офлайн режим» – побудова мережі Байєса на основі сповіщень, отриманих від встановлених IDS систем та передбачення в цілому рівня загроз для системи.

2. «Онлайн режим» – передбачення ймовірності майбутніх загроз, шляхом подачі на вхід побудованій мережі Байєса інформації про нові загрози.

На вхід алгоритму подаються сповіщення системи IDS у форматі IDMEF (Intrusion Detection Message Exchange Format). Сповіщення такого типу включає в себе, як мінімум, наступні поля:

– Time – час створення сповіщення;

– Alert type – тип сповіщення;

– Source – адреса джерела атаки;

– Destination – адреса призначення атаки.

Після отримання сповіщень виконується їх агрегація за типом оповіщення для послідовних часових значень їх створення (формула 2).

$$A_{t1}[AlertType] = A_{t2}[AlertType] = \cdots = A_{tn}[AlertType], \quad (2)$$

де $t_1, \dots, t_n$ – послідовні часові значення створення сповіщень. Для агрегованого сповіщення A_0 типу $AlertType_A$, зберігаються значення адреси джерела атаки та адреси призначення атаки кожного зі сповіщень A_t.

Після агрегації сповіщень за типом, виконується обчислення кореляції між двома послідовними агрегованими сповіщеннями A_0 типу

$AlertType_A$ та B_0 типу $AlertType_B$. Сповіщення про загрози A_t , B_t вважаються корельованими, якщо виконується одна з двох умов:

1) $\{A_t[Source] = B_t[Source],\ A_t[Destination] = B_t[Destination]\}$;
2) $\{A_t[Destination] = B_t[Source]\}$.

Для кожної пари корельованих сповіщень обчислюється ймовірності їх виникнення за формулою 3:

$$P(B/A) = \frac{Corr(A,B)}{Corr\ (A,*)}, \quad (3)$$

де $Corr(A,B)$ – кількість зв'язків між сповіщеннями A та B,

$Corr(A,*)$ – загальна кількість зв'язків, спричинена сповіщенням A (може бути виражена у кількості $Source$ адрес для сповіщення A).

В результуючій Байєсовій мережі вузлами виступають агреговані сповіщення, а ребрами між ними – обчислені ймовірності їх виникнення.

Створені за вказаним алгоритмом мережі зображені на рисунках 1, 2.

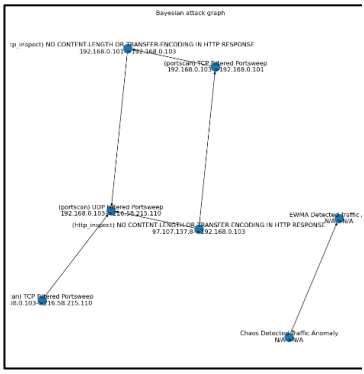

Рисунок 1- Баєсова мережа сповіщень про загрози для періоду 3 дні

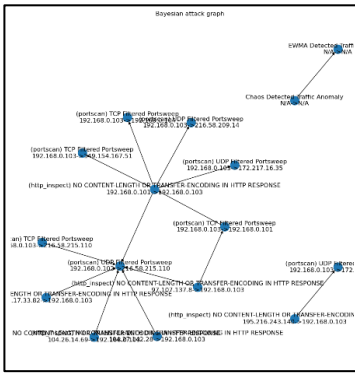

Рисунок 2 – Баєсова мережі сповіщень про загрози для періоду 7 днів

Відзначимо, що кількість агрегованих сповіщень про загрози зростає зі збільшенням періоду агрегації. Баєсова мережа добудовується, як тільки надходить інформація про нову загрозу.

Отримана Баєсова мережа використовується в онлайн режимі для прогнозування рівня загроз за обраний проміжок часу t.

Для здійснення передбачення рівня загроз в онлайн режимі, спочатку обирається період прогнозування для формування в офлайн режимі відповідної Баєсової мережі. Наступним кроком, в створену в офлайн режимі Баєсову мережу, передається назва останнього сповіщення про загрозу з бази даних. У результаті, алгоритм повертає ймовірності появи усіх інших сповіщень, наявних у побудованій мережі, обчислені за формулою 1.

Отже, досліджений метод дозволяє не тільки прогнозувати рівень загроз для корпоративної комп'ютерної мережі, але й досліджувати послідовність їх виникнення, адресу джерела та призначення, тип загрози, тощо. Алгоритм є адаптивним, оскільки його робота не залежить від конфігурації корпоративної комп'ютерної мережі.

Література

1. The Mayhem Cyber Reasoning System / Thanassis Avgerinos, David Brumley, John Davis та ін.] // Security&Privacy / Thanassis Avgerinos, David Brumley, John Davis та ін.]., 2018. – С. 52-60.
2. Cyber Reasoning Systems: Automating Cyber Warfare [Електронний ресурс] // Medium. – 2016. – Режим доступу до ресурсу: https://medium.com/@joey_rideout/cyber-reasoning-systems-automating-cyber-warfare-3329f339edeb .
3. Martin Husák. Predictions of Network Attacks in Collaborative Environment : дис. докт. / Martin Husák. – Brno, 2019. – 144 с.
4. O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing. "Automated generation and analysis of attack graphs". / Security and privacy, 2002. Proceedings. 2002 IEEE Symposium on. IEEE. 2002, С. 273-284.
5. Z. t. Li, J. Lei, L. Wang, and D. Li. "A Data Mining Approach to Generating Network Attack Graph for Intrusion Prediction". / Fuzzy Systems and Knowledge Discovery, 2007. FSKD 2007. Fourth International Conference on. Vol. 4. Aug. 2007, С. 307-311

УДК 004.056.55: 004.032: 004.93

SIMULATING AND RESEARCH OF BLOCK PARAMETRIC MATRIX AFFINE-PERMUTATION CIPHERS (BP_MAPCS) FOR CRYPTOGRAPHIC TRANSFORMATIONS

V.G. Krasilenko, A.A. Lazarev, D.V. Nikitovich
Vinnytsia National Technical University

Introduction, **analysis of recent publications, formulation of the problems.** In the era of electronic communications, the need to transmit and cryptographic transformations (CTs) specific text and graphic documents (TGDs) in the form of table data, 2-D, 3-D, 4-D arrays, drawings, diagrams, resolutions has essentially increased [1-7]. Many TGDs contain restricted access information that in encrypted form, to transmit over communication channels, providing only access with their digital signatures. For security purposes technologies of cryptography, tools for CTs [1-7] and protocols for the formation of keys and their exchange [8, 9] are used, but only small part is devoted to methods oriented on matrix models (MM) [2, 3] and tools. That is why the search and research of new matrix models (MM) of CT, improvement of matrix ciphers are actual strategic task. In works [1, 2] generalized algorithms for CTs, so-called matrix affine-permutation ciphers