ТЕОРЕТИКО-ІГРОВА МОДЕЛЬ ДЛЯ АНАЛІЗУ ВЗАЄМОДІЇ АТАК І ЗАХИСТУ В МЕРЕЖІ МОБІЛЬНОГО ЗВ'ЯЗКУ 5G

Бадєєв В.О., Коляденко О.В., Коляденко Ю.Ю., Москалець М.В.

Харківський національний університет радіоелектроніки,
кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Україна
E-mail: valerii.badieiev@nure.ua,
yuliia.koliadenko@nure.ua,
mykola.moskalets@nure.ua,

Abstract

This article examines an active approach to combating unauthorized interference in 5G networks. Preventive measures are planned based on known software vulnerability data. The open National Vulnerability Database (NVD) database is used. The most dangerous threats are predicted using a game between two partners: an attacker and a defender. The outcome of the game is information security recommendations for the software system under study.

Аналіз взаємодії атак та захисту можна представити у вигляді теоретико-ігрової моделі [1,2]. Гра – це математична модель колективної поведінки: кілька учасників впливають на ситуацію, причому їхні інтереси (виграші чи втрати за різних можливих ситуаціях) різні. При такому уявленні у взаємодії динамічних систем S_i, $i=\overline{1,n}$ можливі три характерні стратегії поведінки. У загальному випадку ці стратегії можуть бути класифіковані таким чином:

1) антагоністична стратегія, коли учасники мають протилежні інтереси;

2) кооперативна стратегія, коли у всіх гравців є спільна мета та їх стратегії узгоджені;

3) стратегія байдужості або гра з природою, коли стратегія j-го гравця не залежить від стратегії i-го гравця.

Відомі та інші типи стратегій – чисті чи змішані [2]. Гра в чистих стратегіях передбачає детерміністський підхід, і виходячи з теорії, рідко коли призводить до рівноважних рішень. На відміну від цього, для ігор у змішаних стратегіях, при стохастичному підході коло рівноважних рішень значно розширюється.

Очевидно, що процеси атак та захистів видаються антагоністичною стратегією або загалом – змішаною. При невеликих відхиленнях в інформації про апріорні дані поведінку такої системи можна представити моделлю взаємодій і фазових станів атак і захистів.

Основні параметри та стани атак $x_i(t)$ зазвичай відомі, і часто їх можна прийняти детермінованими. Випадковим є макростан всього угруповання атак [1–3]. Ця обставина пояснюється впливом безлічі невизначених і випадкових умов. У результаті випадкових впливів $y_i(t)$, $i=\overline{1,n}$, де n - число атак, стану параметрів атак змінюються. У мережі є відповідні динамічні взаємодії, які можуть бути виявлені та проаналізовані в результаті вимірювань та спостережень і характеризуються вектором $\vec{y}(t)$. Динаміку випадкових змін стану параметрів атак можна описати системою диференціальних рівнянь

$$\frac{d\vec{x}(t)}{dt} = F(t)\vec{x}(t) + B(t)\vec{u}(t) + G(t)\vec{\xi}(t), \quad (1)$$

де $\vec{x}(t)$ – вектор стану параметрів атак;

$F(t)$ и $B(t)$ – матриця стану та управління відповідно;

$\vec{u}(t)$ – вектор управління відповідними параметрами;

$\vec{\xi}(t)$ – процес, що породжує, часто апроксимується білим гаусовим шумом, що відображає випадковий механізм;

$G(t)$ – матриця, що масштабує випадкові обурення $\vec{\xi}(t)$.

Параметри стану загроз атак, що спостерігаються, описується системою алгебраїчних рівнянь:

$$\vec{y}(t) = R(\vec{x}(t), t), \tag{2}$$

де $R(\cdot)$ – матриця спостереження.

У цьому можна припустити, якщо весь вектор атак ми спостерігаємо, то вживаються заходи щодо їх запобігання, тобто виробляється захист, з тією чи іншою імовірністю.

Загалом система рівнянь (1) може бути нелінійною, тоді без конкретизації самої нелінійності векторне рівняння (1) може бути представлене у вигляді

$$\frac{d\vec{x}(t)}{dt} = F\Phi[\vec{x}(t), \vec{y}(t)], \tag{3}$$

де F – матриця стану розмірності $n \times n$, при цьому $F = \mathrm{diag}\left(f_i, i \in \overline{1,n}\right)$, якщо x_i незалежні.

Успішність вирішення завдання захисту стосовно атак залежить від готівкових ресурсів $g_k = g_k(\vec{x}(t), t)$, $k \in \overline{1,K}$, а також від відомих апріорних ймовірностей $p_i = p_i(\vec{x}(t), t);\ i \in \overline{1,n}$.

За наявності динаміки зміни стану системи у часі рівняння (3) можна представити у вигляді:

$$\frac{d\vec{x}(t)}{dt} = K\Phi[\vec{x}(t), \vec{y}(\vec{x}(t), t)]. \tag{4}$$

Наявні ресурси g_k визначаються фізичними величинами. Весь ресурс можна представити у вигляді виваженої суми спостережуваних величин:

$$g_k(\vec{x}(t), t) = \sum_{i=1}^{n} c_{ik} y_i,\ y_i \geq 0,\ k \in \overline{1,K},\ i \in \overline{1,n}. \tag{5}$$

c_{ik} – наявність зв'язку між i-ю атакою та k-м захистом. Відповідні зв'язки визначаються матрицею C, які складаються з 0-ї та 1-ї, що визначають наявність або відсутність таких зв'язків.

У мережі 5G, як і в будь-якій динамічній системі, в процесі функціонування здійснюється відповідний перерозподіл ресурсів, що визначається моделями стаціонарних станів, які описуються завданнями максимізації виразу [1–3]:

$$H(Y) = \max\left[\sum_{i=1}^{n} y_i \ln\frac{p_i}{y_i} + y_i\right] \tag{6}$$

за відповідних обмежень на ресурси.

Динаміка стану процесу визначається рішенням $\vec{y}(t)$ задачі (3), яке, як випливає з (5) та (6), залежить від її параметрів p_i, c_{ik} і g_k.

Таким чином, модель динаміки стану атак набуває наступного вигляду:

$$\frac{d\vec{x}(t)}{dt} = \Phi[\vec{x}(t), \vec{y}(\vec{x}(t), t)], \tag{7}$$

$$\vec{y}(\vec{x}(t), t) = \mathrm{argmax}\left[H(Y) \middle| \sum_{i=1}^{n} c_{ik} y_i = g_k(\vec{x}(t), t)\right], \tag{8}$$

де $H_k(Y) = \sum_{i=1}^{n} y_i \ln\frac{a_{ik}}{y_i} + y_i$, a_{ik} – нормативна кількість ресурсу у платіжній матриці.

У нерівноважній системі, що розглядається, мають місце два основні процеси (потоку): атак і погроз від атак.

Позначимо через $\Phi[\vec{x}(t),\vec{y}(t)]$ - потік атак, а $Q[\vec{x}(t),\vec{y}(t)]$ потік погроз від атак. Ці потоки залежать від стану $\vec{x}(t)$ та стану $\vec{y}(t)$. У рамках припущень про те, що час загрози атаки більший за час появи самої атаки [3,4], можна записати наступну, в загальному випадку, нелінійну систему рівнянь:

$$\frac{d\vec{x}(t)}{dt} = \Phi[\vec{x}(t),\vec{y}(\vec{x}(t),t)], \quad (9)$$

$$\varepsilon\frac{d\vec{y}(t)}{dt} = Q[\vec{x}(t),\vec{y}(\vec{x}(t),t)], \quad (10)$$

де ε – матриця, що визначає ефективність атак у мережі.

У ході перетворень отримаємо систему Вольтерра, що характеризує динаміку співіснування атак та захистів в умовах антагоністичної боротьби [1,5,6]:

$$\frac{dy_i(t)}{dt} = y_i(t)\left(\varepsilon_i - \sum_{s=1}^{n} v_s y_s(t)\right). \quad (11)$$

Якщо використовувати для опису функції $\varphi(y)$ квадратичну апроксимацію, то отримаємо нелінійну систему Вольтерра, яка описує стан взаємодії атак і захистів, тобто. стан погроз від атак:

$$\frac{dy_i(t)}{dt} = y_i(t)\left(\varepsilon_i - \sum_{s=1}^{n} v_s y_s(t) - \sum_{s=1}^{n}\sum_{j=1}^{n} v_{sj} y_s(t) y_j(t)\right). \quad (12)$$

Перетворимо цей диференціальний вираз до різницевого. Позначимо t_k – дискретний час.

$$\frac{dy_i(t_{k+1}) - dy_i(t_k)}{t_{k+1} - t_k} = y_i(t_k)\left(\varepsilon_i - \sum_{s=1}^{N} v_s y_s(t_k) - \sum_{s=1}^{N}\sum_{j=1}^{N} v_{sj} y_s(t_k) y_j(t_k)\right), \quad (13)$$

де $t_{k+1} - t_k = T_d$ – інтервал дискретизації.

Позначивши дискретний час $t_k = k$ отримаємо різницеве рівняння

$$y_i(k+1) = y_i(k) + T_d\left[y_i(k)\left(\varepsilon_i - \sum_{s=1}^{n} v_s y_s(k) - \sum_{s=1}^{n}\sum_{j=1}^{n} v_{sj} y_s(k) y_j(k)\right)\right], \quad (14)$$

або

$$y_i(k+1) = y_i(k)\cdot(1+T_d)\left(\varepsilon_i - \sum_{s=1}^{n} v_s y_s(k) - \sum_{s=1}^{n}\sum_{j=1}^{n} v_{sj} y_s(k) y_j(k)\right). \quad (15)$$

Дана модель дозволяє виконувати аналіз при різних конкретних параметрах та взаємодій атак та захистів.

Література:

1. Москалець М.В., Коляденко Ю.Ю., Коляденко О.В. Методи доступу у перспективних системах мобільного зв'язку. Монографія. Харків: ХНУРЕ. 2021. 539 с. DOI 10.30837/978-966-659-296-8.

2. Поповський В.В., Олійник В.Ф.. Математичні основи управління та адаптації в телекомунікаційних системах: підручник. Харків: 2011. 362 с.

3. Математичні основи теорії телекомунікаційних систем : Підруч. для студ. вищ. навч. закл., які навчаються за напрямом "Телекомунікації". Харків : Компанія СМІТ, 2006. 564 с.

4. Popovskij V., Barkalov A., Titarenko L. Control and Adaptation in Telecommunication Systems. Berlin, Heidelberg : Springer Berlin Heidelberg, 2011. 172 p. URL: https://doi.org/10.1007/978-3-642-20614-6.

5. B. Muliar, Y. Koliadenko, M. Moskalets, V. Loshakov and D. Ageyev, "Interaction Model and Phase States at Frequency Resource Allocation in a Grouping of Radio-Electronic Equipment of 5G Mobile Communication Network," *2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2022, pp. 495-501, doi: 10.1109/PICST57299.2022.10238581.

6. Koliadenko, Y., Moskalets, M., Badieiev, V., Savchenko, R. (2023). Method Radio Resource Allocation in Cognitive Radio Network. In: Dovgyi, S., Trofymchuk, O., Ustimenko, V., Globa, L. (eds) Information and Communication Technologies and Sustainable Development. ICT&SD 2022. Lecture Notes in Networks and Systems, vol 809. Springer, Cham. Pp. 102-115 https://doi.org/10.1007/978-3-031-46880-3_7