MEANS OF TELECOMMUNICATIONS
ЗАСОБИ ТЕЛЕКОМУНІКАЦІЙ

УДК 621.396.677.49 **DOI:10.30837/rt.2024.1.216.08**

Ю.Ю. КОЛЯДЕНКО, д-р техн. наук, В.О. БАДЕЄВ

МОДЕЛЬ РАННЬОГО ПОПЕРЕДЖЕННЯ ПРО КІБЕРЗАГРОЗИ У МЕРЕЖАХ 5G З ВИКОРИСТАННЯМ МАРКІВСЬКИХ ПРОЦЕСІВ

Вступ

Сучасні безпроводові міські телекомунікаційні мережі мають архітектуру з центральною станцією, яка керує роботою абонентських станцій. Така архітектура є основою технології 5G.

Однією з особливостей таких мереж є складність протоколу підрівня управління доступом до середовища, який відповідає за організацію доступу абонентів до загального каналу зв'язку. Крім того, у таких мережах є багато невизначених частин, у яких стандартизовані лише деякі механізми мережевого взаємодії.

Безпека телекомунікаційних мереж, у яких канал передачі може використовуватися одночасно багатьма користувачами, є особливо важливою проблемою. У безпроводових міських мережах ця проблема ускладнюється тим, що канал зв'язку є загальнодоступним.

Іншими словами, інформація, яка передається в таких мережах, може бути легко перехоплена зловмисниками. Це може призвести до крадіжки персональних даних, фінансових збитків або навіть до порушення безпеки критичної інфраструктури.

Безпека інформації є важливим фактором, який визначає надійність 5G [1 – 5]. Основною загрозою безпеці таких систем є вразливості, особливо в програмних компонентах. Пошук вразливостей у програмних компонентах є складним і трудомістким завданням, яким займаються здійснюють великі компанії та дослідницькі центри. Інформацію про вразливості можна знайти у загальнодоступних джерелах, таких як Open Source Vulnerability Database, Common Vulnerabilities and Exposures та Natioal Vulnerability Database.

Незважаючи на те, що інформація про вразливості програмних продуктів є загальнодоступною, існуючих даних недостатньо для того, щоб кількісно оцінити безпеку цих продуктів за одним загальним критерієм. Також неможливо прогнозувати, наскільки вони будуть захищені від атак у майбутньому. Одна з основних проблем вибору найбільш захищеної конфігурації 5G полягає в складності кількісної оцінки рівня інформаційної безпеки. Крім того, важко обрати адекватні показники для оцінки, які враховують всі фактори, що впливають на успішне проникнення в мережу та розмір потенційних збитків [6 – 8].

Метою цієї статті є вивчення методів оцінки та прогнозування рівня інформаційної безпеки програмних засобів 5G. Ці методи базуються на моделюванні процесів виявлення та усунення вразливостей за допомогою марківських процесів.

Основна частина

Інформаційна безпека може бути порушена відмовами, які впливають на доступність, цілісність або конфіденційність інформації. Ці відмови можуть бути викликані вразливостями – дефектами в програмному або апаратному забезпеченні, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до інформації.

Результати попереднього аналізу процесів виявлення та усунення вразливостей свідчать про те, що їх можна представити як систему масового обслуговування (СМО) з необмеженою довжиною черги. Параметри цієї системи можна визначити на основі статистичних даних про виявлення та усунення вразливостей таким чином [5]:

- кількість каналів обслуговування n залежить від кількості організацій або груп розробників, які відповідають за усунення вразливостей конкретного програм-

ного продукту 5G. У найпростішому випадку може бути достатньо одного каналу обслуговування;

- інтенсивність надходження заявок λ, яка відповідає інтенсивності виявлення вразливостей в програмному продукті 5G, можна оцінити на основі кількості вразливостей, опублікованих за аналізований проміжок часу (тиждень, місяць, рік). Ця оцінка може бути отримана на основі аналізу бази даних вразливостей CVE (первинної бази);
- інтенсивність обслуговування заявок μ, яка відповідає інтенсивності усунення вразливостей (випуску оновлень, що виправляють вразливості), може бути оцінена з використанням інформації з бюлетенів безпеки, що публікуються компаніями-виробниками програмного продукту 5G, а також баз вразливостей NVD та OSVDB (вторинні бази);
- час обслуговування $T_{обсл}$ окремих вразливостей в програмному продукті 5G, який також називають «кількістю днів ризику» [2, 5], визначається як середній період між появою та усуненням цих вразливостей;
- ймовірність того, що заявка на усунення вразливості буде оброблена Q, теоретично дорівнює одиниці. Однак на практиці існують випадки, коли деякі вразливості окремих програмних компонентів не усуваються;
- ймовірність відмови $P_{відм}$ вразливості – це ймовірність того, що вразливість не буде усунена;
- середня кількість заявок в СМО $z_{ср}$ відображає середню кількість вразливостей, які існують в мережі на даний момент часу та для яких ще не випущено програмне оновлення. Цей показник є одним з найважливіших, адже він визначає число потенційних можливостей для атаки на інфокомунікаційну мережу;
- за середньою кількістю заявок в черзі $r_{ср}$ можна судити про те, скільки вразливостей потребують випуску оновлення;
- середній час очікування заявки в черзі $t_{оч.ср}$ показує, скільки в середньому потрібно часу для усунення вразливості з моменту її виявлення;
- середня кількість зайнятих каналів $k_{ср}$ свідчить про те, скільки робочих груп в середньому зайняті виправленням вразливостей. Цей показник дає уявлення про те, наскільки активно ведеться робота з виправлення вразливостей.

Розглянуту вище систему масового обслуговування можна представити у вигляді системи станів, де кожному стану буде відповідати певна кількість виявлених вразливостей, присутніх в системі, для яких ще немає рекомендації або програмного оновлення для їх усунення. Такі вразливості будемо називати активними. Подібні процеси ефективно описуються марківськими ланцюгами. Марківські ланцюги мають порівняно мало інженерних застосувань, тому що досить рідко на практиці моменти можливих переходів системи з одного стану в інший заздалегідь відомі та зафіксовані. Набагато частіше переходи з одного стану в інший можуть відбуватися не в фіксовані моменти часу, а в випадкові.

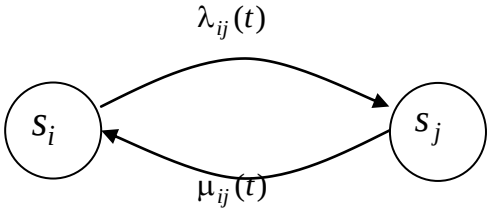

Рис. 1. Перехід із стану S_i в один із сусідніх станів S_j і потім назад в початковий стан під впливом $\lambda_{ij}(t)$ та $\mu_{ij}(t)$

Вважатимемо, що система змінює свій стан під впливом випадкових подій. Ці події відбуваються незалежно одна від одної і слідують пуассонівському закону. Пуассонівський потік не має післядії. Це означає, що ймовірність настання події в майбутньому не залежить від того, що відбувалося в минулому. Знаючи поточний стан системи s_i в момент t, можемо

прогнозувати її майбутню поведінку, не враховуючи, як вона опинилася в цьому стані. Це значно спрощує аналіз поведінки систем, що описуються пуассонівськими потоками.

Нехай на графі станів системи S існує стрілка, яка веде зі стану s_i в один із сусідніх станів s_j (рис. 1).

Вважатимемо, що перехід системи зі стану s_i в стан s_j здійснюється під впливом пуассонівського потоку подій з інтенсивністю $\lambda_{ij}(t)$. Перехід з s_i в s_j відбувається в момент настання першої події потоку.

На осі часу $0t$ виділимо малий проміжок Δt, який примикає до точки t (рис. 2). Знайдемо ймовірність того, що за цей проміжок часу Δt система перейде зі стану s_i в стан s_j, якщо в момент часу t вона знаходилась в стані s_i.

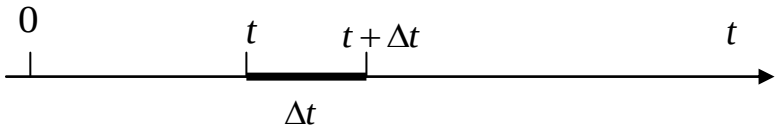

Рис. 2. Елементарний відрізок часу Δt на осі $0t$

Ця ймовірність дорівнює $p_i(t) = \lambda_{ij}(t)\Delta t$, тому що випадкова величина, що дорівнює числу подій потоку, які потрапляють на елементарний відрізок Δt, має математичне очікування $m = \lambda_{ij}(t)\Delta t$, і з точністю до нескінченно малих вищих порядків дорівнює ймовірності p_i попадання на елементарний відрізок однієї події. Знаючи інтенсивності пуассонівських потоків подій, що переводять систему з одного стану в інший, можна сформувати систему диференціальних рівнянь для ймовірностей перебування системи в цих станах.

Для будь-якої пари станів системи s_i, s_j існує інтенсивність $\lambda_{ij}(t)$ пуассонівського потоку подій, що переводять систему зі стану s_i в будь-який інший стан s_j ($i \neq j$). Якщо прямий перехід зі стану s_i в стан s_j неможливий, вважаємо цю інтенсивність нульовою.

Позначимо $p_i(t)$ – можливість, що у момент часу t система перебуває у стані s_i ($i = 1,2,...,n$). Тепер додамо t збільшення Δt і знайдемо ймовірність $p_i(t + \Delta t)$ того, що в момент $t + \Delta t$ система буде перебувати в стані s_i. Позначимо цю подію A: $A = \{S(t + \Delta t) = s_i\}$.

Ця подія може статися двома способами: або станеться подія B, що полягає у тому, що у момент t система вже була у стані s_i, і протягом часу Δt не вийшла із цього стану; або станеться подія C, що полягає у тому, що у момент t система була у одному із сусідніх станів s_j, з яких можливий перехід в s_i і за час Δt перейшла зі стану s_j в s_i.

Вочевидь, $A = B + C$. Знайдемо ймовірність подій B та C. Згідно з правилом множення ймовірностей ймовірність події B дорівнює ймовірності $p_i(t)$ того, що система в момент t була у стані s_i, помноженої на умовну ймовірність того, що за час Δt вона вийде з цього стану, тобто. у сумарному потоці подій, що виводять систему зі стану s_i, не з'явиться жодної події .

Так як сумарний потік подій, що виводить систему зі стану s_i, як і всі його складові, – пуассонівський з інтенсивністю, що дорівнює сумі інтенсивностей доданків: $\sum_{j=1}^{n} \lambda_{ij}(t), i \neq j$,

то умовна ймовірність того, що на ділянці Δt з'явиться хоча б одна подія, дорівнює

$$p_i(t) = \sum_{j=1}^{n} \lambda_{ij}(t)\Delta t, i \neq j,$$

а умовна ймовірність протилежної події

$$1 - \sum_{j=1}^{n} \lambda_{ij}(t)\Delta t .$$

Таким чином,

$$P(B) = p_i(t)\left[1 - \sum_{j=1}^{n} \lambda_{ij}(t)\Delta t\right]. \quad (1)$$

Знайдемо тепер ймовірність події C. Представимо його у вигляді суми несумісних варіантів:

$$C = \sum_j C_j , \quad (2)$$

де підсумовування поширюється на всі стани s_j, з яких можливий безпосередній перехід у s_i. Подія C, з ординарності потоків, вважатимуться несумісними. За правилом складання ймовірностей:

$$P(C) = \sum_j P(C_j). \quad (3)$$

За правилом множення ймовірностей:

$$P(C_j) = p_j(t)\mu_{ji}(t)\Delta t ,$$

звідки

$$P(C) = \sum_{j=1}^{n} p_j(t)\mu_{ji}(t)\Delta t \quad (i \neq j). \quad (4)$$

Отже,

$$P(A) = P(B) + P(C) = p_i(t)\left[1 - \sum_{j=1}^{n} \lambda_{ij}(t)\Delta t\right] + \sum_{j=1}^{n} p_j(t)\mu_{ji}(t)\Delta t$$

Таким чином,

$$p_i(t + \Delta t) = p_i(t)\left[1 - \sum_{j=1}^{n} \lambda_{ij}(t)\Delta t\right] + \sum_{j=1}^{n} p_j(t)\mu_{ji}(t)\Delta t . \quad (5)$$

Віднімаючи з (5) $p_i(t)$, отримаємо збільшення функції на ділянці $t, t + \Delta t$:

$$p_i(t + \Delta t) - p_i(t) = \sum_{j=1}^{n} p_j(t)\mu_{ji}(t)\Delta t - p_i(t)\sum_{j=1}^{n} \lambda_{ij}(t)\Delta t .$$

Поділяючи прирощення функції на приріст аргументу Δt та спрямовуючи $\Delta t \to 0$, отримаємо для ймовірностей $p_i(t)$ систему звичайних диференціальних рівнянь зі змінними коефіцієнтами:

$$\frac{dp_i(t)}{dt} = \sum_{j=1}^{n} p_j(t)\mu_{ji}(t) - p_i(t)\sum_{j=1}^{n}\lambda_{ij}(t) \ . \tag{6}$$

Ці рівняння називаються рівняннями Колмогорова. Перша сума у правій частині формули (6) поширюється на ті значення j, для яких можливий безпосередній перехід із стану s_j в s_i, а друга – на ті значення, для яких можливий безпосередній перехід із стану s_i в s_j.

Усі потоки, що переводять систему S з одного стану в інший, є найпростішими – (стаціонарними пуассонівськими). Системи, у яких відбувається такий процес, називають найпростішими системами. Для найпростішої системи ймовірності станів визначаються рівняннями Колмогорова з постійними коефіцієнтами. Застосуємо перетворення Лапласа до розв'язання системи рівнянь Колмогорова. Позначимо зображення ймовірності стану $p_i(t)$ функцією $\pi_i(x)$:

$$p_i(t) \to \pi_i(x) \, . \tag{7}$$

Тоді системі рівнянь Колмогорова для ймовірностей станів відповідатиме система рівнянь для їх зображень:

$$x\pi_i(x) = \sum_{j=1}^{n}\pi_j(x)\mu_{ji} - \pi_i(x)\sum_{j=1}^{n}\lambda_{ij} + p_i(0) \, , i = 1,2,...,n \, . \tag{8}$$

Звідки

$$\pi_i(x) = \frac{\sum_{j=1}^{n}\pi_j(x)\mu_{ji} + p(0)}{x + \lambda_i} \, , \tag{9}$$

де $\lambda_i = \sum_{j=1}^{n}\lambda_{ij}$.

Таким чином, замість системи однорідних диференціальних рівнянь з постійними коефіцієнтами для ймовірностей станів отримана система однорідних алгебраїчних рівнянь з постійними коефіцієнтами для зображень ймовірностей станів.

Цю систему потрібно вирішувати з урахуванням нормувальної умови

$$\sum_{i=1}^{n} p_i(t) = 1 \, . \tag{10}$$

Отже, одне з рівнянь можна замінити на

$$\sum_{i=1}^{n}\pi_i(t) = \frac{1}{x} \, , \tag{11}$$

яке є зображенням нормувальної умови.

Знаючи інтенсивності λ_{ij} та μ_{ij} появи подій, що породжуються потоком, можна зіміту-вати випадковий інтервал між двома подіями в цьому потоці:

$$\tau_{ij} = -\frac{1}{\lambda_{ij}}\ln(r) \, , \ \tau_{ji} = -\frac{1}{\mu_{ij}}\ln(r) \, .$$

де τ_{ij} – інтервал часу між знаходженням системи в i -му і j -му стані; r – рівномірно розподілене від 0 до 1 випадкове число, яке береться з генератора випадкових чисел (ГВЧ).

Далі, очевидно, система з будь-якого i -го стану може перейти в один із кількох станів j, j + 1, j + 2, …, пов'язаних з ним переходами. У j-й стан вона перейде через τ_{ij}; в (j + 1)-й стан вона перейде через τ_{ij+1}; в (j +2)-й стан вона перейде через τ_{ij+2} і т. д.

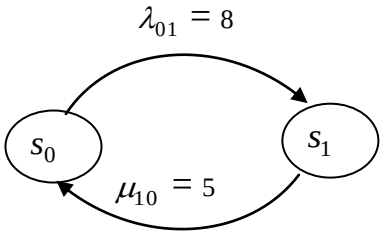

Рис. 3. Граф станів

Зрозуміло, що система може перейти з i -го стану тільки в один із цих станів, причому в той, перехід в який настане раніше.

Тому з послідовності часів: τ_{ij}, τ_{ij+1}, τ_{ij+2} і т. д. треба вибрати мінімальне і визначити індекс j, що вказує, в який стан відбудеться перехід.

Розглянемо приклад. Нехай надходять заявки на виявлення вразливостей. Позначимо стани (рис. 3): s_0 – немає заявки, s_1 – надійшла заявка. Задамо інтенсивність потоків:

$\lambda_{01} = 8$ заявок на хвилину; $\mu_{10} = 5$ оброблених заявок на хвилину.

Вважатимемо, що система в початковий момент перебувала в стані s_0 (немає заявки).

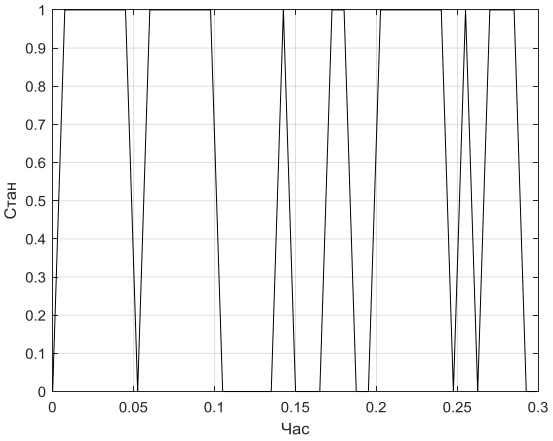

Рис. 4. Часова діаграма надходження заявок на виявлення вразливостей

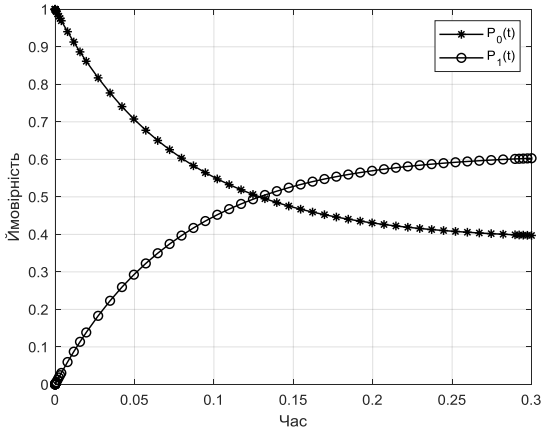

Рис. 5. Зміна ймовірностей станів: s_0 – немає заявки, s_1 – надійшла заявка

За допомогою імітаційного моделювання в середовищі Matlab отримано часову діаграму надходження заявок на виявлення вразливостей (рис. 4). Таким чином, знаючи інтенсивність потоків, можна в реальному масштабі часу моделювати процеси надходження заявок на виявлення вразливостей. На рис. 5 показано зміну ймовірностей станів: $P_0(t)$ – це ймовірність, що система знаходиться у стані s_0 (немає заявки), $P_1(t)$ – це ймовірність, що система знаходиться у стані s_1 (надійшла заявка). Як видно з наведених графіків, ймовірність стану s_0 спочатку дорівнює одиниці, потім різко зменшується та досягає 0,4 в сталому стані. Ймовірність стану s_1 навпаки спочатку дорівнює нулю, потім з плином часу збільшується та досягає значення 0,6 в сталому стані.

Висновок

Інформаційна безпека є однією із складових гарантоспроможності 5G. Основну загрозу безпеці таких систем становлять вразливості насамперед програмних компонентів. Пошук вразливостей у програмних компонентах є актуальним та ресурсомістким завданням, яким останнім часом займаються великі компанії та дослідницькі центри. Аналіз процесів виявлення та усунення вразливостей показує, що вони можуть бути описані системою масового обслуговування з необмеженою довжиною черги. Розроблено модель виявлення та усунення вразливостей у мережах зв'язку 5G на основі апарату марківських процесів. За допомогою даної моделі, знаючи інтенсивності потоків, можна в реальному масштабі часу моделювати процеси надходження заявок на виявлення вразливостей.

Список літератури:

1. Nick McKeown. Openflow: enabling innovation in campus networks/ Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, Jonathan Turner // ACM SIGCOMM Computer Communication Review, 38[2]. 2008. P. 69–74.

2. OpenFlow Switch Specification Ver 1.5.1, 2016 [accessed January 11, 2016]. https://www.opennetworking.org/images/stories/downloads/sdnresources/ onf-specifications/openflow/openflow-switch-v1.5.1.pdf.

3. Партика Т.Л., Попов І.І. Інформаційна безпека : навч. посіб. для студентів закладів середньой професійної освіти. Москва : ФОРУМ: ІНФРА-М, 2002. 368с.

4. Лукацький А. Інформаційна безпека 2015 // Іт-безпека. Стандарти. Засоби захисту. Заходи. 2013. № 12. С.64–69.

5. Ложковський А.Г. Теорія масового обслуговування в телекомунікаціях : підручник. Одеса : ОНАС ім. А. С. Попова, 2012. 112 с. ISBN 978-966-7595-43-3.

6. Ложковський А.Г. Моделювання багатоканальної системи обслуговування з організацією черги / А.Г. Ложковський, Н.С. Салманов, О.В.Вербанов // Східно-європейський журнал передових технологій. 2007. №3/6(27). С.72–76.

7. Muliar B., Koliadenko Y., Moskalets M., Loshakov V. and Ageyev D. 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.

8. Koliadenko Y., Moskalets M., Badieiev V., Savchenko R. (2023). Method Radio Resource Allocation in Cognitive Radio Network // 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

Надійшла до редколегії 03.02.2024

Відомості про авторів:

Коляденко Юлія Юріївна – д-р техн. наук, професор, Харківський національний університет радіоелектроніки, професор кафедри інфокомунікаційної інженерії ім. В.В. Поповського; Україна; e-mail: yuliia.koliadenko@nure.ua; ORCID: https://orcid.org/0000-0002-0247-2736

Бадеєв Валерій Олександрович – Харківський національний університет радіоелектроніки, аспірант кафедри інфокомунікаційної інженерії ім. В.В. Поповського; Україна; e-mail: valerii.badieiev@nure.ua; ORCID: https://orcid.org/0009-0005-4982-1840