АНАЛІЗ ІГРОВОЇ МОДЕЛІ ВЗАЄМОДІЇ "АТАКА-ЗАХИСТ" СИСТЕМ МОБІЛЬНОГО ЗВ'ЯЗКУ 5 G

Коляденко Ю.Ю., Бадеєв В.О.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
м. Харків, Україна
e-mail: yuliia.koliadenko@nure.ua

Abstract

An active way of organizing the fight against unauthorized interference in the operation of a software-configurable 5G communication network is considered. Preventive measures are planned based on known data on the vulnerability of software products. An open database is used. The forecast of the most dangerous threats is conducted in the form of a game of two partners: the attacker and the defending one. The result of the game is recommendations for protecting information for the program system under study. The results of the analysis of non-equilibrium states in the network grouping were obtained, which allow for proving the possibility of the existence of equilibrium states and determining the stability limits of the functioning of dynamic interacting networks under different values of threat effectiveness.

Вступ

Мережа стільникового зв'язку характеризується величезною вартістю та великими термінами будівництва. Зміни у стандартах зв'язку відбуваються регулярно, але перехід до нового стандарту потребує нових вкладень та заміни обладнання, яке часто ще не виробило свій ресурс. Зараз для запуску мережі 5G все стає простіше завдяки технології програмних мереж, що конфігуруються. У мережах 5G основні функції комутаторів та маршрутизаторів перенесені на центральний мережевий контролер, що спрощує застосування мережевих політик, та моніторинг стану мережі. При такому підході передавальні пристрої відповідають лише за передачу даних, спираючись на таблицю потоків, яка будується централізованим мережевим контролером, що взаємодіє з передавальним пристроєм.

Взаємодія між мережним контролером і передавальними пристроями реалізується за допомогою програмного інтерфейсу, який використовується для прямого управління групами пристроїв. Архітектура комутатора базується на одній чи декількох таблицях правил, які визначають механізм обробки потоків мережного трафіку. Кожне правило є записом у таблиці комутатора. Запис зіставляється з певним потоком трафіку. Залежно від результату зіставлення, застосовується відповідна дія (блокування, передача, модифікація тощо) до пакетів з даного потоку.

Архітектура мережі, припускаючи істотно інший підхід до реалізації мережевої інфраструктури, не позбавлена потенційних вразливостей з погляду інформаційної безпеки. Необхідність поділу доступу мережевих додатків при роботі з контролером, питання аутентифікації та авторизації при роботі додатків з контролером – це лише мала частина аспектів безпеки, які доводиться брати до уваги при проектуванні мереж. Контролер як ключовий компонент в управлінні усією інфраструктурою мережі є найуразливішим елементом, атака на який може спричинити критичні для всієї інфраструктури наслідки.

Завдання безпеки стає особливо актуальним для мереж [1], де канал передачі часто розділяється між великою кількістю користувачів. У безпроводових мережах постає ще одна проблема — загальнодоступність каналу зв'язку.

Для забезпечення безпеки безпроводових міських мереж необхідно провести аналіз за тих чи інших ситуацій виникнення несанкціонованого доступу. З цією метою розробляються математичні моделі. Таким чином, розробка моделі взаємодії атак та захистів є актуальною науковою задачею.

Об'єктом дослідження є процес організації безпеки в безпроводових мережах зв'язку 5G.

Предмет дослідження становлять моделі взаємодії атак та захистів.

Метою даної роботи є розробка моделі взаємодії атак та захистів.

Ігрова модель взаємодії атак і захисту

Аналіз взаємодії атак та захистів можна представити у вигляді теоретико-ігрової моделі [2-4]. Гра - це математична модель колективної поведінки: кілька учасників впливають на ситуацію, причому їх інтереси (виграші або втрати за різних можливих ситуацій) 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 гравця не залежить від стратегії гравця i.

Відомі й інші типи стратегій - чисті чи змішані [4]. Гра в чистих стратегіях передбачає детерміністський підхід, і як випливає 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 представляються 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. Слід зазначити, що у відомих роботах відсутнє уявлення мережі як теоретико-ігровой моделі з антагоністичною стратегією поведінки.

Запропоновано теоретико-ігрову модель стану взаємодії атак та захистів у вигляді нелінійної системи Вольтерра [5]:

$$\frac{dy_i(t)}{dt} = y_i(t)(\varepsilon_i - \sum_{s=1}^{n} \nu_s y_s(t) - \sum_{s=1}^{n}\sum_{j=1}^{n} \nu_{sj} y_s(t) y_j(t)), \quad (1)$$

де $y_i(t)$ - випадковий вплив атак, $i = \overline{1,n}$, $s = \overline{1,n}$, $j = \overline{1,n}$ n - число атак; ε_i - ефективність i-ї атаки; ν_s - параметр:

$$\nu_s = \frac{a_s y_s}{\sum_{s=1}^{n} a_s y_s}; \quad 0 \le \nu_s \le 1; \quad \sum_{s=1}^{n} \nu_s = 1. \quad (2)$$

a_s - нормативна кількість ресурсів s-го захисту.

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

$$\frac{dy_i(t_{k+1}) - dy_i(t_k)}{t_{k+1} - t_k} = y_i(t_k)(\varepsilon_i - \sum_{s=1}^{N} \nu_s y_s(t_k) - \sum_{s=1}^{N}\sum_{j=1}^{N} \nu_{sj} y_s(t_k) y_j(t_k)), \quad (3)$$

де $t_{k+1} - t_k = T_d$ - интервал дискретизации.

Позначивши дискретний час $t_k = k$ отримаємо різницеве рівняння:

$$y_i(k+1) = y_i(k) + T_d \times [y_i(k)(\varepsilon_i - \sum_{s=1}^{n} \nu_s y_s(k) - \sum_{s=1}^{n}\sum_{j=1}^{n} \nu_{sj} y_s(k) y_j(k))],$$

або

$$y_i(k+1) = y_i(k) \cdot (1 + T_d) \times (\varepsilon_i - \sum_{s=1}^{n} \nu_s y_s(k) - \sum_{s=1}^{n}\sum_{j=1}^{n} \nu_{sj} y_s(k) y_j(k)). \quad (4)$$

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

Аналіз ігрової моделі взаємодії атак і захисту

Використовуючи імітаційне моделювання, проаналізовано динаміку взаємодій і фазових станів атак і захисту мережі 5G залежно від ефективності атак.

Рис. 1. Залежність загроз та при малій ефективності атак .

Рис. 2. Залежність загроз та при середній ефективності атак .

На рис. 1 представлена залежність загроз від атак $y_1(t)$ та $y_2(t)$ при малій ефективності атак $\varepsilon << 1$. Номери кривих відповідають номеру атаки. Як видно з рис. 1, при малих, але різних значеннях ε загрози від атак зростають до настання усталеного режиму. Відмінність полягає в тому, що $\varepsilon_1 > \varepsilon_2$. Фізичний сенс цієї нерівності полягає в тому, що перша атака створює більшу загрозу порівняно з другою атакою. Тому й вплив $y_1 > y_2$ є значним.

На рис. 2 представлена залежність загроз від атак $y_1(t)$ та $y_2(t)$ при середній ефективності атак $\varepsilon \approx 1$. При значеннях $\varepsilon \approx 1$ (рис. 2) відзначаються дві характерні області графіків:

1. Початкова область, де спостерігається різке збільшення загрози як від першої, так і від другої атаки.
2. Стаціонарна (нерівноважна) частина з помітними коливаннями в часі, що пов'язано з перерозподілом загроз і захисту.

Було проаналізовано випадок роботи мережі при великих значеннях інтенсивностей $\varepsilon >> 1$ (рис. 3), за яких система набуває граничного насиченого стану (або надмірно насиченого стану).

Отримані результати, представлені на рис. 3 свідчать про те, що при досить великих значеннях ефективності атак динаміка стану мережі стає непередбачуваною: може відбуватися як різке збільшення загроз, так і різке їхнє зниження, що характерно для ситуацій, які виникають у мережі при нештатному режимі роботи, – з'являється так званий детермінований хаос.

Проведемо аналіз роботи мережі для визначення рівноважних станів та стійкості динамічної системи. Для цього побудовано фазовий портрет, тобто залежність стану загроз y від параметра ε. На рис. 4 представлено фазовий портрет динамічної системи при $T_d = 1$. Судячи з фазового портрета (рис. 4), критичним числом ε при $T_d = 1$, за якого мережа ще не втрачає стійкості, є $\varepsilon \cong 1{,}4$. З цього графіка випливає, що в області $\varepsilon > 1{,}4$ відзначаються роздвоєння траєкторій (біфуркація стану). В області $\varepsilon \geq 1{,}4$ зміни стану досліджуваної системи можуть виявитися значними та неоднозначними при незначних змінах ефективності атак

Рис. 3. Залежність загроз та при великих значеннях ефективності атак .

Рис. 4. Фазовий портрет динамічної системи при

Висновки

У роботі знайшла подальший розвиток теоретико-ігрова модель, у якій реалізовано антагоністичну стратегію. На підставі створення бази даних уразливості програмного забезпечення вдається поставити задачу прогнозування найбільш ефективних загроз інформаційній безпеці конкретного об’єкта атаки.

Задача прогнозу може бути поставлена як гра двох осіб: атакуючого і захисника (або нападника і того, хто захищається). Правомірність такої постановки випливає з можливості розглядати площину платіжної матриці гри як поле станів об'єкта у процесі зміни його станів.

Отримано результати аналізу нерівноважних станів у групуванні мережі, які дозволяють довести можливість існування рівноважних станів та визначити межі стійкості функціонування динамічних мереж, що взаємодіють, при різних значеннях ефективності загроз.

Література

1. Коляденко Ю.Ю., Бадеєв В.О. Модель раннього попередження про кіберзагрози у мережах 5G з використанням марківських процесів. РАДІОТЕХНІКА Всеукраїнський міжвідомчий науково-технічний збірник, 2024, Вип. 216. с. 87-93. DOI: https://doi.org/10.30837/rt.2024.1.216.08

2. Коляденко Ю.Ю. Анализ взаимодействия и фазовые состояния группировки радиоэлектронных средств систем абонентского радиодоступа / Коляденко Ю.Ю. - Прикладная радиоэлектроника. Всеукр. Межвед. Научн.-техн. сб. - 2004. - Том.3, №3. - С. 37-42.

3. Коляденко Ю.Ю. Модель динамики неравновесных состояний при распределении ресурсов в сети абонентского радиодоступа /Коляденко Ю.Ю., Величко Т.В. - Радиотехника, Всеукр. Межвед. Научн.-Техн. сб. - 2005. - Вып. 142. - С. 34—39.

4. Лесик Р.А. Теоретико-игровая модель атак в городских беспроводных сетях/Лесик Р.А. - Материалы XVII Международного молодежного форума «Радиоэлектроника и молодежь в XXI веке» Харьков, 2013. - с. 103-104.

5. Коляденко Ю.Ю., Бадеєв В.О. Теоретико-ігрова модель взаємодії атак і захисту Міжнародна науково-практична конференція “Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку” 14 березня 2024 року, м. Харків. С.170 -172. https://nangu.edu.ua/uploads/files/Zbirnyk%20tez%20MNPK%2014.03.2024.pdf