

УДК 621.3.006.357

Коляденко Ю.Ю., Бадєєв В.О.

ТЕОРЕТИКО-ІГРОВА МОДЕЛЬ ВЗАЄМОДІЇ АТАК І ЗАХИСТУ

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, 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.

Аналіз взаємодії атак та захистів можна представити у вигляді теоретико-ігрової моделі [1-3]. 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 [3]. Гра в чистих стратегіях передбачає детерміністський підхід, і як впливає 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-ігрової моделі з антагоністичною стратегією поведінки.

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

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

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; v_s - параметр:

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

a_s - нормативна кількість ресурсів s -го захисту.

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

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

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

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

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

або

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

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

Список використаних джерел

1. 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.
2. 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.

3. 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.