УДК 681.518.5

Р. І. Банах, А. З. Піскозуб
Національний університет “Львівська політехніка”,
кафедра захисту інформації

ОЦІНКА НАДІЙНОСТІ ЕЛЕМЕНТІВ СИСТЕМИ-ПРИМАНКИ У МЕРЕЖІ СТАНДАРТУ IEEE 802.11 ЯК РОЗГАЛУЖЕНОЇ СИСТЕМИ ЗІ СКЛАДНИМ ПІДПОРЯДКУВАННЯМ

Запропоновано метод оцінювання надійності елементів системи-приманки для мережі стандарту IEEE 802.11 як розгалуженої системи зі складним підпорядкуванням. Оцінка можливостей працездатності елементів може запевнити у надійності системи або у протилежному. Такий підхід забезпечить процес безперервного вдосконалення системи, оскільки з його впровадженням можна прогнозувати виникнення проблем та успішно їм запобігати.

Ключові слова: система-приманка, надійність, система-приманка бездротової мережі як сервіс, розгалужена система.

The method of honeypot’s elements reliability assessment for IEEE 802.11 based network as ramified system with complex subordination is suggested. Possibility assessment of elements’ workability can assure that system is either reliable or not. This approach provides continuous improvement of system as it can help to predict issues and help to prevent them.

Keywords: honeypot, reliability, Wireless Honeypot as a Service, extensive systems.

Вступ

Як відомо, системи-приманки за типом поділяються на низькоінтерактивні та високоінтерактивні. Низькоінтерактивні дають змогу імітувати окремі сервіси, а високоінтерактивні – операційні системи, мережеві ресурси та цілі інфраструктури. На відміну від провідних мереж, застосування систем-приманок у бездротових мережах має низку особливостей. Все це зумовлено тим, що підключення до бездротових та провідних мереж не здійснюється за одним і тим самим алгоритмом.

Для того, щоб підключитись до провідної мережі стандарту IEEE 802.x, користувачеві необхідно перебувати біля мережевої розетки чи кабелю, який, своєю чергою, підключений до певної ланки певного мережевого ресурсу. Очевидно, що доступ до таких ресурсів може бути фізично контрольований, чого не можна сказати про бездротові мережі.

Для того, щоб підключитись до бездротової мережі стандарту IEEE 802.11, у випадку більшості сучасних операційних систем (ОС) користувачеві потрібно лише зайти у меню керування бездротовими з’єднаннями і обрати потрібну мережу. Пристрій користувача пропонує йому список мереж, які знаходяться поряд, оскільки ці мережі відсилають в ефір інформацію про свою присутність.

Низькоінтерактивні приманки для бездротових мереж надсилають велику кількість спеціальних кадрів, маячків в ефір. Такі кадри створюють велику кількість підробних точок доступу, з якими неможливо провести жодних маніпуляцій. Високоінтерактивні системи-приманки для бездротових мереж дозволяють створити інфраструктуру, яка цілком відтворить легітимну, тобто для зловмисника процес атаки на приманку проходитиме так само, як і на справжню.

Контроль за працездатністю будь-якого сервісу є обов'язковою умовою надання послуг у сучасних хмарних обчисленнях. Для низькоінтерактивної приманки потрібно перевіряти стан лише одного елемента на працездатність, а саме елемента, який імітує сервіси. У високоінтерактивних приманках необхідно контролювати велику кількість елементів, особливо це стосується систем-приманок для бездротових мереж.

Аналіз досліджень та публікацій

Якщо для провідних мереж приманку можна розгорнути навіть у виробничому сегменті мережі, не використовуючи додаткового фізичного обладнання, то розгортання приманок для бездротових мереж вимагає встановлення додаткового обладнання у локації, де планується її застосування. Для того, щоб розгорнути систему-приманку для бездротової мережі стандарту IEEE 802.11, необхідно фізично розмістити саму приманку. У роботі [1] запропоновано використання зовнішніх елементів на базі сучасних одномодульних комп'ютерів, описано проблеми впровадження систем-приманок у бездротові мережі, поставлено вимоги до систем виявлення вторгнень у бездротові мережі.

Сучасні обчислення неможливо уявити без застосування хмарних рішень. На основі роботи [1] у роботі [2] описано концепцію побудови системи-приманки для бездротових мереж із застосуванням хмарних обчислень. У роботі описано мінімальний набір елементів, за допомогою яких можна побудувати таку систему; регламентовано комунікацію елементів між собою та взаємодію комплексу із користувачем. У посібнику [3] наведено приклади ієрархічних розгалужених систем та їхніх елементів. Описано, як на основі твірних функцій будуються вирази для розрахунку ймовірнісних, часових та експлуатаційних характеристик надійності ієрархічних систем; наведено приклади розрахунків.

Формулювання цілі статті

Основною задачею систем-приманок є вивчення поведінки порушників, відвернення їхньої уваги від виробничих систем та затримка в середині приманки з метою збирання доказів і виявлення точного місцезнаходження. Та відмова одного із елементів може спричинити відмову усієї системи. Найкритичнішою є відмова під час дослідження чи атаки системи-приманки зловмисником.

З використанням незалежних сенсорів для ідентифікації вторгнень у мережі стандарту IEEE 802.11 можна швидко ідентифікувати атаку і визначати приблизне місцезнаходження зловмисника в момент проведення атаки. Проте існує велика кількість чинників, які можуть вплинути на функціонування як одного елемента, так і системи-приманки загалом.

Одним із основних показників якості є надійність, прогнозування параметрів якої на етапі проектування дає змогу визначити ймовірності і часові характеристики стійкості системи до відмов. Але існують фактори впливу, які можуть бути ідентифіковані вже після введення системи в дію.

Метою дослідження є розроблення математичної моделі для розрахунку надійності як окремих елементів моделі "Система-приманка для бездротової мережі, як сервіс", так і системи-приманки для мережі стандарту IEEE 802.11 загалом.

Вплив на незалежні елементи системи-приманки у мережах стандарту IEEE 802.11

Існує велика кількість факторів, які можуть вплинути на працездатність системи-приманки як загалом, так і на кожен елемент окремо. Для зовнішніх елементів системи-приманки це може бути:

- зашумлення каналу в діапазоні 2,412-2,484 ГГц;
- неможливість елемента системи-приманки доступитись до мережі Інтернет;
- відімкнення електроенергії на певній ділянці, де підключено елемент системи-приманки.

Хоч у своїй більшості провайдери хмарних обчислень гарантують понад 99% доступності своїх сервісів, та все ж є імовірність того, що важливий обчислювальний елемент перестане відповідати.

Для виявлення й усунення причин перебоїв у роботі важливо з'ясувати, чи вони є систематичними. Постійні присутність і контроль інженера є не доцільними, оскільки існує висока

імовірність людської помилки. Таку роль може виконувати комп'ютер, який із набагато вищою точністю передбачатиме можливість виникнення інцидентів.

Моніторинг та збирання статистичних даних про елементи системи-приманки

Задля забезпечення якісного функціонування будь-якої системи необхідно забезпечити її моніторингом, що дасть змогу вчасно реагувати, а також збирати статистику відносно інцидентів. Не є винятком і системи-приманки, безперервне збирання інформації про працездатність яких є необхідним для подальшого покращення їх роботи.

Автори пропонують модель перевірки елементів системи-приманки, у якій протягом усього життєвого циклу проводяться перевірки з періодом *T*. Існує два статуси, які можуть бути повернуті моніторингом у результаті перевірки того чи іншого елемента – це результат успішності та неуспішності. Оскільки існує імовірність отримання помилкових спрацювань, то існує необхідність у повторній перевірці елемента у випадку, коли від нього було отримано неуспішний результат. Після першого неуспішного результату перевірки елемент у моніторингу перейде у "гнучкий стан", який є необхідним для уникнення помилкових спрацювань. У гнучкому стані інформація про те, що з тим чи іншим елементом системи щось трапилось, не передаватиметься як нотифікації, а перевірки відбуваються з періодичністю *T/2*. Скорочення періоду перевірок після першого спрацювання дає змогу максимально прискорити нотифікацію про наявну проблему у системі. У разі, якщо і друга перевірка дасть неуспішний результат – стан проблеми перейде у постійний, у якому перевірки відбуватимуться і далі з періодичністю *T*. Дані про елемент та час, коли було зафіксовано інцидент, записується у базу даних чи інший ресурс, а власник ресурсу отримує нотифікацію.

Час визначення інциденту обчислюють за формулою:

$$t_D = t_C - T/2, \tag{1}$$

де t_C – поточний час.

Парою для запису t_D буде відмітка часу, коли елемент змінить статус з неуспішного на успішний t_R.

Після того, як роботу елемента буде відновлено, її стан знову перейде у постійний, періодичність перевірки в якому становить *T* (рис. 1).

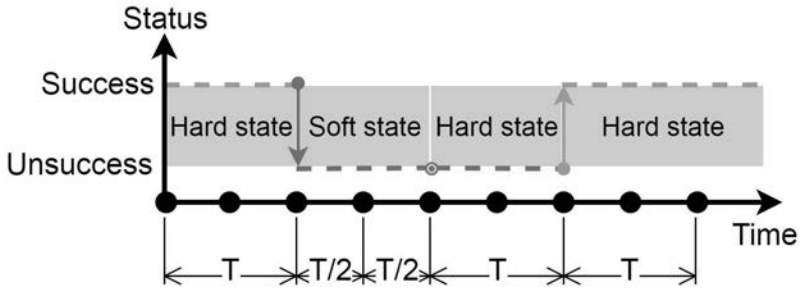

Рис. 1. Схематичне зображення алгоритму моніторингу елементів системи-приманки

Просумувавши весь час, протягом якого елемент перебував у неуспішному статусі, можемо визначити кількість невдалих перевірок для нього (2).

$$m_U = \frac{\sum t_R - t_D}{T}. \tag{2}$$

Розділивши відрізок часу, цікавий для дослідження на період перевірок, можна отримати кількість проведених перевірок за цей час (3):

$$n = \frac{t}{T}. \tag{3}$$

Різниця загальної кількості перевірок і кількості неуспішних перевірок дасть кількість перевірок із успішним результатом (4):

$$m_S = n - m_U . \tag{4}$$

Володіючи статистичними даними, можемо визначити імовірність появи успішного результату перевірки, а отже, й імовірність працездатності певного елемента системи-приманки (5):

$$P(A) = \lim_{n \to t} \frac{m_S}{n} \tag{5}$$

Обчислення надійності розгалуженої системи зі складним підпорядкуванням

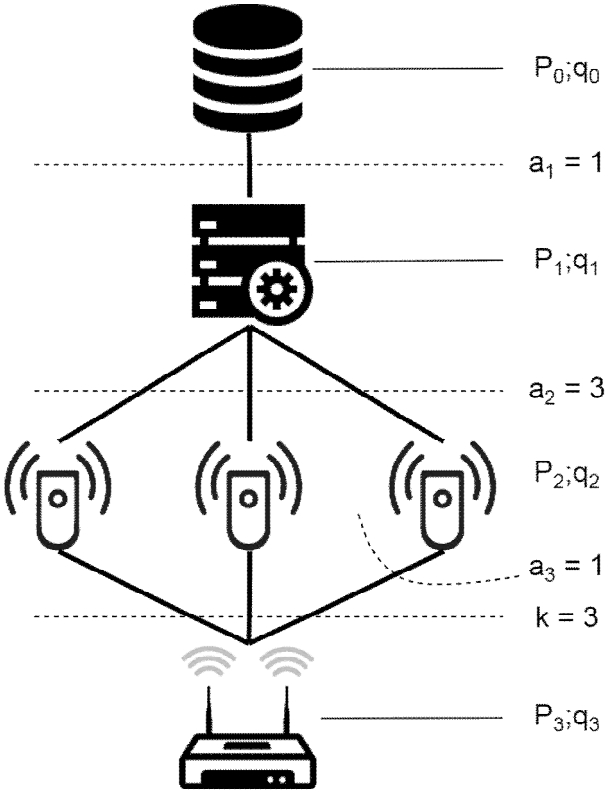

Рис. 2. Модель WHaaS як розгалужена система із складним підпорядкуванням

Елементами системи-приманки моделі Wireless Honeypot as a Service (WHaaS) є база даних, сервер обробки даних, незалежні сенсори ідентифікації вторгнень та сама система-приманка [2]. Відповідно до [3] класифікуємо елементи, які зображено на рис. 2. Основним елементом, звичайно, є елемент “приманка”, який водночас є і вихідним вузлом. Незалежні сенсори, сервер обробки даних та база даних є проміжними вузлами. База даних знаходиться на рівні 0, сервер обробки даних – на рівні 1, незалежні сенсори на рівні 2 і приманка на рівні 3.

Елементи на кожному рівні володіють такими характеристиками, як ймовірність праці p_i і ймовірність відмови q_i. Принцип ієрархії реалізується так, що у разі відмови елемент верхнього рівня виводить з роботи елемент нижнього рівня. Тому робота елемента верхнього рівня, наприклад, рівня 3, передбачає одночасну роботу елемента рівня 0. Зазвичай система-приманка може функціонувати і надавати сервіс, а незалежні сенсори передаватимуть дані на сервер обробки, але після обробки дані не можна записати.

Виведемо твірну функцію для розрахунку надійності системи, зображеної на рис. 2 (6), згідно з [3].

$$S_3(z) = P_0(P_1^{a_1}(P_2^{a_2}(P_3 z + q_3)^{a_3} + (1 - P_2^{a_2})) + (1 - P_1^{a_1})) + q_0 = P_0(P_1^{a_1} P_2^{a_2}(P_3 z + q_3)^{a_3} + P_1^{a_1}(1 - P_2^{a_2}) +$$

$$+(1 - P_1^{a_1})) + q_0 = P_0 P_2^{a_2} P_1^{a_1} \times \sum_{x_3=0}^{a_3} C_{a_3}^{x_3} P_3^{x_3} q_3^{a_3 - x_3} z^{x_3} + P_0 P_1^{a_1}(1 - P_2^{a_2}) + P_0(1 - P_1^{a_1}) + q_0 \quad (6)$$

$$0 < x_3 \le N_3$$

$$N_3 = a_3$$

За формулою (6) отримаємо рекурентний вираз (7):

$$P_3(x_3) = P_0 P_1^{a_1} C_{a_3}^{x_3} P_2^{a_2} P_3^{x_3} q_3^{a_3 - x_3}. \quad (7)$$

Використавши формулу (7), можемо отримати, наприклад, ймовірність того, що жоден елемент не працює (8):

$$P_3(0) = P_3(x_3 = 0) + P_0 P_1^{a_1}(1 - P_2^{a_2}) + P_0(1 - P_1^{a_1}) + q_0. \quad (8)$$

Висновок

Сучасні онлайн-сервіси дають своїм користувачам змогу розпочати роботу без додаткових зусиль, часто навіть не даючи їм шансу на зміну налаштувань. Прикладом такої концепції є WHaaS, яка дає змогу розпочати роботу без втручання у програмне чи апаратне забезпечення її елементів. Тобто, обслуговування цих елементів лягає на плечі постачальника даного сервісу. Хоч такий підхід здається не вигідним для постачальника сервісу, проте допомагає уникнути помилок, яких може допуститися кінцевий користувач.

Та без використання характеристик надійності важко вирішити низку питань проектування й експлуатації систем-приманок. Це вибір структури, організація контролю і профілактики, оновлення програмного чи апаратного забезпечення.

Як вже зазначалось вище, одним із основних показників якості є надійність. Описана вище модель, яка працює за принципом безперервного моніторингу, дає змогу прогнозувати ймовірності і часові характеристики стійкості приманки до відмов.

Для системи-приманки, основаної на моделі WHaaS, застосовано математичну модель з розрахунку надійності як окремих елементів, так і загалом системи-приманки для мережі стандарту IEEE 802.11. Запропонований підхід дає змогу безперервно покращувати працездатність і вирішувати проблеми.

1. Banakh R. External elements of honeypot for wireless network / R. Banakh., A. Piskozub, Y. Stefinko // Modern Problems of Radio Engineering, Telecommunications, and Computer Science: Proceedings of the XIIIth International Conference TCSET'2016. 23–26 February 2016 : proceedings. – Lviv-Slavsko, Ukraine: Lviv Publishing House of Lviv Polytechnic, 2016. – P. 480–482. 2. Banakh. R. Wi-Fi Honeypot as a service. Conception of business model / R. Banakh, // ENGINEER OF XXI CENTURY : VI INTER UNIVERSITY CONFERENCE OF STUDENTS, PHD STUDENTS AND YOUNG SCIENTISTS, 02 December 2016 : proceedings. – Bielsko-Biała, Poland : dr inż. Jacek Rysiński, 2016. – P. 59–64. 3. Марунчак Д. Є. Надійність розгалужених систем : навч. посібник / Д. Є. Марунчак, А. Р. Сидор. – Львів : Видавництво Національного університету "Львівська політехніка", 2007. – 124 с. 4. Гнатюк С. О. Сучасні системи віртуальних приманок на основі технології honeypot */ С. О. Гнатюк, В. В. Волянська, С. В. Карпенко // Наук.-практ. журнал "Захист інформації". – 2012. – № 3. – С. 107–114.*