УДК: 681.5 DOI 10.33111/mise.104.1

Агутін М.М.,
к.е.н., доцент кафедри системного аналізу та кібербезпеки
КНЕУ імені Вадима Гетьмана

Agutin M.M.,
PhD in Economics, Associate Professor of System Analysis
and Cybersecurity Department
KNEU named after Vadym Hetman

МОДЕЛЮВАННЯ IOT-ІНФРАСТРУКТУРИ РОЗУМНОГО БУДИНКУ

SIMULATION OF THE IOT-INFRASTRUCTURE OF THE SMART HOUSE

***Анотація**. В статті розглядаються питання інтеграції систем Інтернет-речей (IoT) у побутовому та промисловому секторах, зокрема в «розумних будинках», що вимагає надійних методів для аналізу їхньої поведінки, стійкості до відмов та здатності протистояти загрозам. Традиційні методи аналізу часто не враховують конкурентність та асинхронність, притаманні розподіленим IoT системам.*
Мережі Петрі виступають потужним формальним апаратом для моделювання таких систем. Вони дозволяють наочно та строго описувати стани компонентів (позиції), події та дії (переходи), а також взаємодію між ними через рух токенів. Цей підхід був застосований для створення моделі типової системи моніторингу «розумний будинок», де компоненти (датчики руху, дверей, контролер живлення, сервер) відображені у відповідних елементах мережі. Додавання до моделі параметрів, таких як затримки спрацьовування переходів, ємність позицій та пріоритети подій, робить її більш реалістичною для подальшого аналізу. На базі цієї моделі мережі Петрі сформульовано узагальнену математичну модель для аналізу надійності та безпеки IoT системи. Ця модель використовує властивості мережі Петрі для кількісної оцінки рівня безпеки та надійності системи, враховуючи при цьому обмеження у доступних ресурсах (обчислювальних, комунікаційних, енергетичних). Задача зводиться до пошуку такої конфігурації системи (представленої моделлю мережі Петрі), яка забезпечує досягнення мінімально необхідного рівня безпеки, не виходячи за межі встановлених ресурсних обмежень. Моделювання систем IoT за допомогою мереж Петрі надає формальну основу для розуміння їхньої складної поведінки. Розширення цих моделей для включення параметрів та метрик надійності, безпеки та ресурсних витрат дозволяє проводити комплексний аналіз та оптимізацію на етапі проектування. Такий підхід є критично важливим для створення стійких, безпечних та ефективних систем Інтернет-речей в умовах обмежених ресурсів.
***Ключові слова**. Мережі Петрі, система Інтернет-речей, системи моніторингу, комп'ютерна мережа.*

***Abstract**. The paper addresses the integration of Internet of Things (IoT) systems into domestic and industrial environments, particularly smart homes, highlighting the need for reliable methods to analyze system behavior, fault tolerance,*

and resilience to threats. Traditional analytical approaches often fail to account for concurrency and asynchrony inherent in distributed IoT systems. Petri nets offer a formal and expressive modeling tool suitable for such complex systems. They provide a structured way to represent component states (places), events and actions (transitions), and their interactions through token flow. This methodology was applied to model a typical smart home monitoring system, where motion sensors, door contacts, power controllers, and monitoring servers are represented as elements of a Petri net. The inclusion of parameters such as transition delays, place capacities, and event priorities adds realism to the model. Based on this structure, a generalized mathematical model has been developed to analyze the reliability and security of IoT systems. It enables quantitative evaluation of safety under resource constraints—computational, communication, and energy-related—by searching for configurations that ensure minimum acceptable security levels without exceeding resource limits.

Petri net-based modeling offers a formal foundation for understanding IoT system behavior. Extending these models with reliability, security, and resource usage metrics allows for comprehensive analysis and optimization at the design stage, which is critical for building robust and efficient IoT solutions in resource-constrained environments.

***Keywords**. Petri Nets, IoT-system, Monitoring systems, computer network.*

Постановка проблеми у загальному вигляді. Необхідно розробити дискретну математичну модель системи моніторингу «Розумний будинок» за допомогою формалізму мереж Петрі для аналізу її поведінки та взаємодії ключових компонентів. Модель має відображати стани датчиків (руху, відкриття дверей, наявності електроживлення) та логіку обробки інформації центральним сервером з метою виявлення потенційних подій (наприклад, несанкціонованого доступу або зникнення електроживлення) та оповіщення користувача або пункту охорони. Зокрема, модель має дозволити дослідити послідовності подій, які призводять до спрацьовування системи оповіщення, та проаналізувати вплив відсутності електроживлення на функціонування системи.

Аналіз останніх досліджень і публікацій. Модель кольорової мережі Петрі (CPN) для оцінки продуктивності та ефективності механізму пріоритетів, передбаченого стандартом IEEE 802.11e, представлено у статті [1]. Модель дозволяє аналізувати різні сценарії функціонування бездротових мереж, зокрема з урахуванням прихованих вузлів, які суттєво впливають на ефективність механізму доступу до середовища. Автори виявили низку недоліків у реалізації механізмів пріоритетів у поточній версії протоколу, зокрема обмеження запропонованих налаштувань параметрів у реальних умовах. Особливістю моделі є її гнучкість і модульна структура — завдяки цьому її можна легко адаптувати для аналізу нових модифікацій стандарту, зокрема IEEE 802.11ax. Отримані результати є актуальними для проєктування бездротових мереж, особливо в умовах сільської місцевості, де характерні великі відстані між вузлами та складна радіообстановка.

Кольорові мережі Петрі застосовуються для моделювання [4] подій в системі моніторингу типу «сенсор —> обробка — > дія». Кольорові мітки відображають тип події (наприклад, спрацьовування сигналізації, вмикання світла, регулювання температури). Модель дозволяє формально перевірити відсутність гонок подій та визначити, чи всі критичні умови обробляються належним чином.

У комп'ютерних мережах за допомогою CPN моделюють маршрутизацію[2] даних між IoT-пристроями, обираючи кольори для позначення типів пакетів (наприклад, критичні, фонові, оновлення прошивки). Це дозволяє перевіряти коректність пріоритезації трафіку та виявляти можливі вузькі місця.

Моделі CPN застосовуються також для формального опису процедур автентифікації користувачів та пристроїв.[3] Кольори використовуються для кодування різних рівнів доступу та станів аутентифікації. За допомогою моделі перевіряють можливість атак типу DDOS, «людина посередині»(MITM) або повторного використання токенів.

Виділення невирішених раніше частин загальної проблеми. У контексті зростаючої складності та критичності систем Інтернет-речей (IoT), зокрема у сфері автоматизації будівель та моніторингу безпеки, постає гостра потреба у використанні формальних методів для моделювання та аналізу їхньої поведінки. Мережі Петрі, завдяки своїй здатності ефективно представляти паралелізм, синхронізацію та асинхронні події, є визнаним інструментом для таких цілей. Відповідно до поставленої задачі, наступним кроком є побудова моделі мережі Петрі для системи моніторингу «Розумний будинок», що дозволить формалізувати її функціонування та взаємодію ключових компонентів. Використання кольорових мереж Петрі забезпечує зручність детального моделювання складних систем моніторингу IoT, включаючи різноманітні потоки даних, що сприяє ранньому виявленню неефективних рішень та потенційних проблем, тим самим підвищуючи економічну та енергоефективність проектованої системи ще до її впровадження.

Кольорові мережі Петрі (Coloured Petri Nets, CPN) — це потужне розширення класичних мереж Петрі, що дозволяє моделювати складні дискретні системи, поєднуючи графічну наочність із виразністю формального опису. Основна їхня особливість полягає у введенні «кольорів» — типів даних, які маркери можуть нести, що відкриває можливість оперувати не лише фактом наявності маркера в позиції, але й його змістом.

Це дозволяє істотно зменшити розмір моделі завдяки використанню параметризованих переходів, які узагальнюють множину

схожих дій. У порівнянні з іншими методами моделювання, зокрема класичними мережами Петрі, діаграмами станів або системами автоматів, CPN мають виразну перевагу у можливості формалізувати як поведінкові, так і інформаційні аспекти системи в одному формалізмі. Їх модульна природа дозволяє розбивати систему на логічні підсистеми, підтримуючи ієрархічне моделювання та сприяючи повторному використанню фрагментів моделей. Важливо, що кольорові мережі Петрі підтримують як детерміноване, так і стохастичне моделювання, що дає змогу аналізувати поведінку систем з урахуванням ймовірностей і часу.

Застосування CPN значно полегшує формальну верифікацію — перевірку властивостей моделі, таких як досяжність, відсутність тупиків, живучість, правильність протоколів обміну тощо. Вагомою практичною перевагою є наявність професійного інструменту CPN Tools, який забезпечує побудову моделей, симуляцію та автоматизований аналіз. Таким чином, кольорові мережі Петрі вирізняються серед інших методів моделювання завдяки гнучкому опису даних, підтримці складної логіки поведінки, можливості інтеграції з аналізом систем і практичній придатності для моделювання як технічних, так і організаційно-інформаційних процесів.

Основною метою дослідження є розроблення дискретної математичної моделі системи «Розумний будинок» із використанням формалізму кольорових мереж Петрі (CPN) для аналізу її поведінки та взаємодії ключових компонентів. Модель має описувати логіку реагування системи моніторингу на зміни станів сенсорів (руху, відкриття дверей, наявності електроживлення) з метою виявлення потенційних подій, зокрема несанкціонованого доступу або зникнення живлення. Кольорові мережі Петрі обрано через їхню здатність поєднувати поведінкові та інформаційні аспекти системи, підтримку параметризації, модульність і можливість формальної верифікації. Такий підхід дозволяє не лише точно моделювати логіку функціонування системи, а й адаптувати модель до змін, розширень або нових сценаріїв. Результати дослідження можуть бути використані для проєктування надійних систем безпеки в розумних будинках.

Виклад основного матеріалу. Побудова моделі мережі Петрі для системи моніторингу «Розумний будинок» передбачає формалізацію ключових аспектів функціонування системи «Розумний будинок» за допомогою стандартних елементів мереж Петрі. Структура мережі Петрі базується на двох фундаментальних типах елементів, які відображають статичні та динамічні аспекти системи:

Позиції (Places). Ці елементи слугують для представлення дискретних станів системи або умов, які мають місце у певний момент часу. У контексті системи «Розумний будинок», позиції можуть моделювати логічні стани датчиків або внутрішні стани сервера системи моніторингу. Наявність одного або декількох токенів у певній позиції вказує на істинність відповідного стану чи умови.

Переходи (Transitions). Ці елементи моделюють події або дії, які спричиняють зміну станів системи. Перехід може «спрацювати» (fire), якщо виконуються певні умови. Спрацьовування переходу призводить до споживання токенів з вхідних позицій та розміщення токенів у вихідних позиціях, тим самим змінюючи позначку (стан) мережі. Для системи моніторингу «Розумний будинок», переходи можуть відповідати активації датчика, зміні стану, або діям сервера.

Конкретизація цих абстрактних елементів для представленої системи «Розумний будинок» здійснюється шляхом визначення відповідних позицій та переходів, що відображають специфіку її функціонування. Приклади таких вузлів мережі Петрі, включаючи їх ключові параметри, такі як часові затримки спрацьовування, ємність позицій (обмеження на кількість токенів) та пріоритети спрацьовування переходів, які є критично важливими для моделювання динамічної поведінки та ресурсних обмежень системи, детально відображені у наведеній нижче таблиці. 1.

Таблиця 1

ОПИС ВУЗЛІВ МЕРЕЖІ ПЕТРІ НА ПРИКЛАДІ РОЗУМНОГО БУДИНКУ

Вузол Мережі Петрі	Тип	Опис	Затримка (час)	Ємність	Пріоритет	Початкова позначка (токенів)
p_motion_idle	Позиція	Датчик руху знаходиться у стані спокою (рух не виявлено).	-	1	-	1
p_motion_detected	Позиція	Датчик руху виявив рух.	-	1	-	0
p_door_closed	Позиція	Двері зачинені.	-	1	-	1
p_door_opened	Позиція	Двері відчинені.	-	1	-	0
p_power_ok	Позиція	Електроживлення в нормі.	-	1	-	1
p_power_loss	Позиція	Відсутнє електроживлення.	-	1	-	0

Продовження табл. 1

Вузол Мережі Петрі	Тип	Опис	Затримка (час)	Ємність	Пріоритет	Початкова позначка (токенів)
p_server_idle	Позиція	Сервер Розумного будинку знаходиться у стані очікування даних.	-	1	-	1
p_server_processing	Позиція	Сервер Розумного будинку обробляє дані від датчиків.	-	1	-	0
p_alert_pending	Позиція	Сервер виявив потенційну подію, що потребує оповіщення.	-	1	-	0
p_notified	Позиція	Господар або пункт охорони повідомлені.	-	1	-	0
t_detect_motion	Перехід	Датчик руху виявляє рух.	0.1	-	5	-
t_motion_cleared	Перехід	Рух припинився, датчик повертається у стан спокою.	2.0	-	3	-
t_open_door	Перехід	Двері відчиняються.	0.2	-	5	-
t_close_door	Перехід	Двері зачиняються.	0.2	-	4	-
t_power_fails	Перехід	Відбувається зникнення електроживлення.	0.5	-	6	-
t_power_restores	Перехід	Електроживлення відновлюється.	5.0	-	2	-
t_send_data_to_server	Перехід	Датчики надсилають дані на сервер (наприклад, при зміні стану).	0.1	-	5	-
t_process_data	Перехід	Сервер обробляє отримані дані.	0.3	-	4	-
t_identify_alert	Перехід	Сервер ідентифікує ситуацію, що вимагає оповіщення.	0.1	-	7	-
t_send_notification	Перехід	Сервер надсилає сповіщення господареві або на пункт охорони.	1.0	-	6	-

Закінчення табл. 1

Вузол Мережі Петрі	Тип	Опис	Затримка (час)	Ємність	Пріоритет	Початкова позначка (токенів)
t_reset_server	Перехід	Сервер завершив обробку або відправив сповіщення і готовий до нових даних.	0.5	-	1	-
t_handle_power_loss	Перехід	Сервер реагує на зникнення електроживлення.	0.4	-	6	-

Джерело даних: власна розробка

Опис параметрів, наведених в таблиці 1.

- *Затримка* (час): Вказано гіпотетичний час, необхідний для виконання переходу. Одиниці часу можуть бути секундами або іншими зручними одиницями залежно від масштабу моделювання.
- *Ємність*. Максимальна кількість токенів, які може містити позиція. Для цієї моделі встановлено ємність 1 для всіх позицій, що означає, що позиція може бути або «активною» (містити один токен), або «неактивною» (не містити токенів). Це відповідає бінарним станам датчиків в даній спрощеній моделі.
- *Пріоритет*. Використовується для вирішення конфліктів, коли декілька переходів стають активними одночасно. Перехід з вищим числом пріоритету буде виконано першим. Пріоритети відображають гіпотетичну важливість або швидкість реакції системи на певні події (наприклад, виявлення руху або зникнення живлення можуть мати вищий пріоритет обробки).

Розроблені позиції та переходи станів в системі відображено на рис. 1, що дозволяє візуально уявити та проаналізувати вузькі місця в роботі системи моніторингу.

Узагальнена математична модель розрахунку безпеки та надійності системи Інтернет-речей. Для формалізації задачі використаємо розширення мереж Петрі, наприклад, Стохастичні Мережі Петрі (Stochastic Petri Nets — SPN) або Узагальнені Стохастичні Мережі Петрі (Generalized Stochastic Petri Nets — GSPN), де переходи мають асоційовані з ними часові затримки (моделюють тривалість подій) або ймовірності спрацьовування. Для моделювання безпеки можуть бути використані також Кольорові Мережі

Петрі (Colored Petri Nets — CPN), де токени мають додаткові атрибути (колір), що можуть представляти різні типи даних, дозволів або рівні доступу.

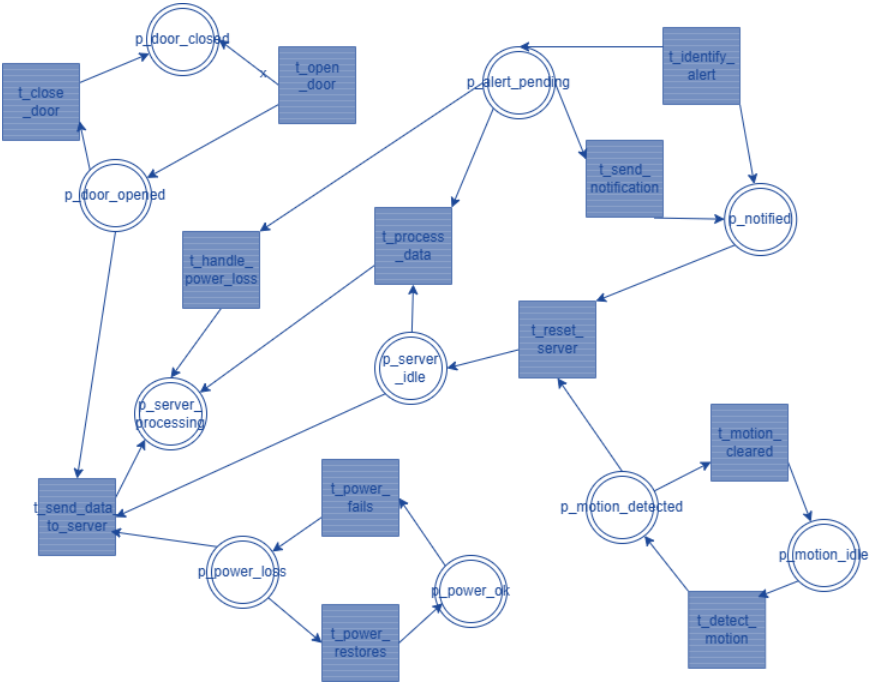

Рис. 1. Позиції та структура переходів (transition)
для моніторингу подій в мережі Петрі

Система Інтернет-речей моделюється як мережа Петрі:

$$PN = (P, T, F, W, M_0, \Omega), \quad (1),$$

де:

- P — скінченна множина позицій (станів), як описано у таблиці (p_motion_idle, p_motion_detected, etc.).
- T — скінченна множина переходів (подій/дій), як описано у таблиці (t_detect_motion, t_open_door, etc.).
- $F \subseteq (P \times T) \cup (T \times P)$ — множина дуг, що з'єднують позиції та переходи.
- $W: F \rightarrow N^+$ — функція ваги дуг.
- $M_0: P \rightarrow N_0$ — початкова позначка (розподіл токенів у позиціях).

- $\boldsymbol{\Omega}$ — множина параметрів переходів (наприклад, інтенсивності експоненційного розподілу для timed transitions у SPN/GSPN, або ймовірності спрацьовування для immediate transitions), що пов'язані із затримками, вказаними у таблиці. Також сюди можуть входити параметри, пов'язані з ємністю позицій та пріоритетами переходів.

Таким чином, мережі Петрі є потужним та гнучким інструментом для формального моделювання складних, конкурентних та розподілених систем Інтернет-речей, таких як система моніторингу «Розумний будинок». Моделювання на рівні станів та подій, з можливістю додавання часових та пріоритетних параметрів, дозволяє детально описати динаміку системи. Розроблена узагальнена математична модель є значним кроком від чисто функціонального моделювання до кількісного аналізу критично важливих нефункціональних властивостей — якості, безпеки та ефективності.

Висновки та пропозиції. Наведена узагальнена математична модель використовує формалізм мереж Петрі з розширеннями для стохастичного або кольорового аналізу для представлення системи моніторингу «Розумний будинок». Параметри мережі Петрі неведені у таблиці (затримки, ємність, пріоритети), є вхідними даними для побудови конкретної стохастичної або часової моделі мережі Петрі. Перспективним напрямком розвитку моделі системи є розрахунок надійності та безпеки та аналізу властивостей запропонованої моделі (наприклад, досяжності станів, часових характеристик переходів), тоді як ресурсні обмеження інтегруються через функцію вартості. Розв'язання такої задачі вимагає визначення конкретних функцій надійності, безпеки та ресурсоємності системи на основі детального аналізу загроз, відмов та архітектури системи, а також використання відповідних інструментів для моделювання та аналізу мереж Петрі.

Список використаних джерел

1. Verma, S., Gupta, A., Kumar, S., Srivastava, V. and Tripathi, B.K. Resource allocation for efficient IOT application in fog computing. International Journal of Mathematical, Engineering and Management Sciences, 5(6). — 2020. — p. 1312.

2. Ren, W., Yu, L., Ma, L., & Ren, Y. (2013). RISE: A Reliable and Secure scheme for wireless Machine to Machine communications. Tsinghua Science and Technology, 18(1), 100–117. https://doi.org/10.1109/tst.2013.6449413

3. Zhang C., Green R. Communication security in internet of thing: preventive measure and avoid DDoS attack over IoT network // Proceedings of the 18th symposium on communications & networking. — 2015. — С. 8–15.
4. Теслюк В.М.; Казарян А.Г.; Казимира І.Я. Опрацювання даних у системах «розумного» будинку з використанням моделей на підставі мереж Петрі. Scientific Bulletin of UNFU, 2021, 31.1: 131–136.

Статтю подано до редакції: 18.11.2024