УДК 621.391

ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ПРИСТРОЇВ IoT

Хомич С.В., Федосюк А.В., Куліковський М.І.,

Одеська національна академія зв'язку ім. О.С. Попова,
65029, Україна, м. Одеса, вул. Ковальська,1.

sergey_khomich@mail.ru, fedosiuk.anna@gmail.com, kulikovskymax@gmail.com

ИССЛЕДОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ УСТРОЙСТВ IoT

Хомич С.В, Федосюк А.В., Куликовский М.И.

Одесская национальная академия связи им. А.С. Попова,
65029, Украина, г. Одесса, ул. Кузнечная,1.
sergey_khomich@mail.ru, fedosiuk.anna@gmail.com, kulikovskymax@gmail.com

RESEARCH OF SYSTEM OF IoT DEVICES INFORMATION SECURITY

Khomich S.V., Fedosiuk A.V., Kulikovsky M.I

O.S. Popov Odessa national academy of telecommunications,
1 Kovalska St., Odessa, 65029, Ukraine.
sergey_khomich@mail.ru, fedosiuk.anna@gmail.com, kulikovskymax@gmail.com

Анотація. Розглянуто моделі архітектури Інтернету речей (IoT), виділено особливості необхідні при побудові системи захисту інформації (СЗІ). Досліджено архітектуру СЗІ для пристроїв IoT. Складено математичну модель для визначення навантаження такої СЗІ і проведено імітаційне моделювання навантаження при зростанні кількості пристроїв.

Ключові слова: Інтернет речей, Internet of Things, система захисту інформації, M2M, теорія Ерланга.

Аннотация. Рассмотрены модели архитектуры Интернета вещей (IoT), выделены особенности необходимые при построении системы защиты информации (СЗИ). Исследовано архитектуру СЗИ для устройств IoT. Составлена математическая модель для определения нагрузки такой СЗИ и проведено имитационное моделирование нагрузки при росте количества устройств.

Ключевые слова: интернет вещей, Internet of Things, система защиты информации, M2M, теория Эрланга.

Abstract. It was the Internet of things (IoT) architecture reviewed, highlighted the features necessary for building information security system (ISS). It was proposed ISS for IoT devices. It was designed mathematical model for ISS load determination and simulation were done by device number modification.

Key words: Internet of Things, system of information security, M2M, theory of Erlang.

Бурхливий розвиток телекомунікацій та інформаційних технологій призвів до появи Інтернету речей (Internet of Things, IoT). Попередником даного терміна, був M2M (Machine-To-Machine), що виник в телекомунікаційній індустрії і прив'язаний до обміну даними по мережі між підключеними машинами. Проте на IoT являє собою ширше поняття, усередині якого є значно більше інструментів і технологій, ніж в M2M [1].

Суть концепції IoT полягає в тому, щоб всі предмети побуту, товари, вузли технологічних процесів тощо, були обладнані вбудованими комп'ютерами та сенсорами, мали змогу обробляти інформацію, що надходить із навколишнього середовища, обмінюватися нею та виконувати різні дії в залежності від отриманої інформації. Дана концепція досить цікава, нова та небезпечна. IoT може викликати величезні зміни у повсякденному житті людини, надавши звичайним користувачам абсолютно новий рівень комфорту та доступу. У цей са-

мий час, глобальний зв'язок між усіма пристроями створює істотні проблеми безпеки. Саме тому виникає необхідність провести дослідження системи захисту інформації (СЗІ) для пристроїв IoT та, враховуючи стрімке зростання кількості таких пристроїв та їх користувачів, - навантаження на таку СЗІ.

Метою статті є дослідження системи захисту інформації пристроїв IoT, математичної моделі та імітаційного моделювання навантаження на СЗІ.

Основна частина

У загальному випадку пристрій IoT можливо розглядати як будь-який предмет побутового чи промислового користування з вбудованим мікрокомп'ютером та інтерфейсами управління й обміну інформацією, елементарною периферією. Враховуючи вузький напрямок роботи таких пристроїв значної популярності набирають рішення на базі RISC-процесорів (від англ. restricted (reduced) instruction set computer – комп'ютер зі скороченим набором команд), які надають можливість зменшити розміри та витрати на побудову таких пристроїв. Керування таким мікрокомп'ютером можуть виконувати як спеціалізовані операційні системи (RIOT, Contiki), так і операційні системи загального користування (Windows, Linux). На сьогодні вже існує значна кількість різних типів таких пристроїв: від побутових лампочок з дистанційним керуванням до високотехнологічних фармако-біометричних вимірювачів.

Враховуючи особливість концепції IoT, можливо запропонувати два основних варіанти архітектури системи захисту інформації (СЗІ) – це розподілена та централізована СЗІ. Структура взаємодії пристроїв IoT один з одним та з блоком керування безпекою зображено на рис. 1 (а, б). В рамках розподіленої основні функції СЗІ реалізовано на пристрої IoT, а з централізованої винесено в окремий пристрій (сервер, вузол, блок).

Оскільки сама концепція не припускає використовування продуктивних комп'ютерних систем, тоді, краще систему захисту інформації винести в окреме місце (сервер, сервіс і т.п.).

А враховуючи схожість характеру взаємодії пристроїв IoT з типовими телекомунікаційними пристроями, можна застосувати теорію Ерланга для формування математичної моделі визначення навантаження СЗІ [2, 3].

Теорія Ерланга – це аналітична модель, створена датським ученим А. К. Ерлангом для оцінки різних характеристик комутаційних телефонних станцій: числа вхідних/вихідних ліній, необхідних для зв'язку з телефонною мережею, інтенсивності навантаження та ін. [4].

Під інтенсивністю навантаження, розуміють навантаження за одиницю часу, як правило, за 1 годину. За одиницю вимірювання інтенсивності навантаження прийнято Ерланг (Ерл). Ерланг – це безрозмірна одиниця інтенсивності навантаження або одиниця навантаження, використовувана для вираження величини навантаження, потрібного для підтримки зайнятості одного пристрою впродовж певного періоду часу.

Один Ерланг – навантаження в одне годино-зайняття за 1 годину [5].

$$1 \text{ Ерл} = 1 \text{ годино-зайняття/год.} \quad (1)$$

Таким чином, за допомогою теорії Ерланга, можна розрахувати кількість каналів для підключення, чи, як у даному випадку, кількість процесів на сервері, кожен з яких обслуговує підключення одного користувача.

В цьому випадку ймовірність блокування виклику P_b обчислюється за формулою [5]:

$$Pb = \frac{A^C / C!}{\sum_{i=0}^{C} \frac{A^i}{i!}}, \quad (2)$$

де C – число каналів трафіка, A – загальне навантаження (в Ерлангах).

У цьому випадку ймовірність утримання підключення пристрою IoT (ймовірність, що підключення буде поставлено в чергу) P_d обчислюється за формулою ймовірності, еквівалентної до телекомунікаційних пристроїв [5]:

$$P_d = \frac{A^C}{A^C + C!\left(1 - \frac{A}{C}\right)\sum_{k=0}^{C-1}\frac{A^k}{k!}}, \tag{3}$$

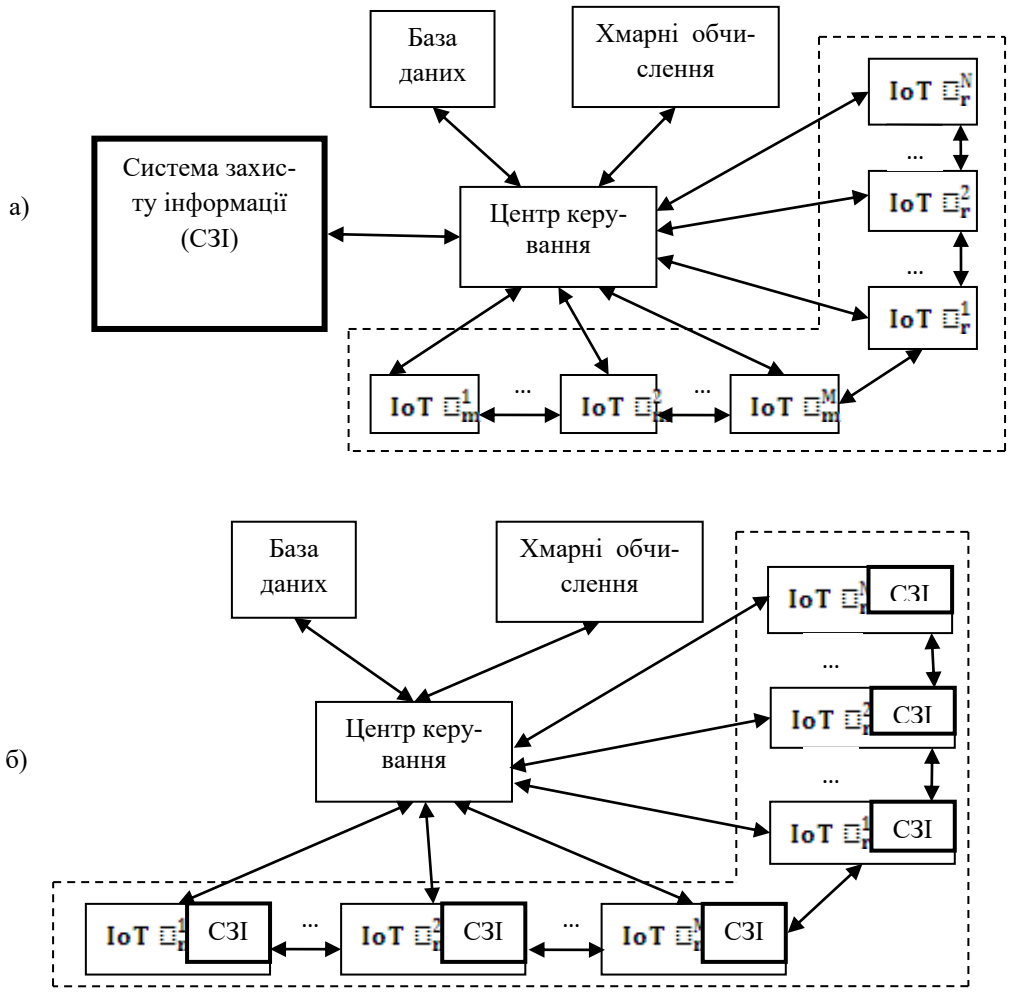

Рисунок 1 – Структура взаємодії пристроїв IoT один з одним та з централізованим (а), розподіленим (б) керування безпекою

А ймовірність того, що утримане підключення знаходитиметься в черзі більш, ніж година $t\left(P_{(W>t)}\right)$,визначається за таким самим принципом [5]:

$$P_{(W>t)} = P_d \cdot e^{-(C-A)\cdot t/H}, \tag{4}$$

де, H – середній час утримання каналу на одного користувача (під час найбільшого навантаження); A – корисне навантаження, яке може бути визначене як (4) [5]:

$$A = \frac{M \cdot \lambda \cdot H}{3600}, \tag{5}$$

де, M – кількість пристроїв IoT, λ – кількість підключень на одного користувача.

Ймовірність того, що будь-яке підключення буде затримане на деякий час більше, ніж t, визначається за формулою [5]:

$$P_{(W>t)} = P_d \cdot e^{-(C-A)\cdot t/H}, \quad (6)$$

Вирази (2), (3), (5) складають математичну модель навантаження СЗІ.

Проведемо імітаційне моделювання створення СЗІ, використовуючи наступні вихідні параметри. Для прикладу використаємо звичайний житловий будинок, в якому знаходиться 10 квартир, допустимо, що в квартирі проживає дві або більше людини. Для початку беремо мінімум пристроїв, тобто у кожній квартирі по одному смарт-годиннику, а далі збільшуємо кількість пристроїв IoT на квартиру, результати надані в табл. 1, 2 і 3.

При цьому допускається, що:

– кількість пристроїв IoT з розрахунком на одну квартиру;

– інтервали між підключенням пристроїв випадкові;

– середній час роботи з пристроями у діапазоні 15-200 с.;

– кількість використань пристроїв IoT за одну годину 3-4 рази (за основу візьмемо смарт-годинник);

– відсоток повторних підключень пристроїв IoT до СЗІ у діапазоні 20-100%;

– кількість відмов у підключені пристроїв IoT до СЗІ 1…3% від загальної кількості абонентів.

Таблиця 1 – Розрахунки навантаження системи захисту інформації для підключення вхідних пристроїв IoT

№ з/п	Кількість пристроїв IoT на житловий будинок	Кількість відмов у підключені пристроїв IoT до СЗІ	Відсоток повторних підключень пристроїв IoT до СЗІ, %	Кількість процесів на сервері, кожен з яких обслуговує підключення одного користувача IoT
1	10	0,3	80	20
2	20	0,4	65	33
3	30	0,6	50	43
4	40	0,4	35	56
5	50	0,5	20	66

Таблиця 2 – Розрахунки навантаження системи захисту інформації для вихідних підключень пристроїв IoT

№ з/п	Кількість пристроїв IoT на житловий будинок	Середній час роботи з пристроями IoT, с.	Кількість використань пристроїв IoT за одну годину	Кількість відмов у підключені пристроїв IoT до СЗІ	Кількість процесів на сервері, кожен з яких обслуговує підключення одного користувача IoT
1	10	15	4	0,3	3
2	20	30	8	0,4	7
3	30	60	12	0,6	13
4	40	120	15	0,4	25
5	50	200	20	0,5	37

Залежність кількості процесів на сервері СЗІ від кількості пристроїв IoT показано на рис. 2

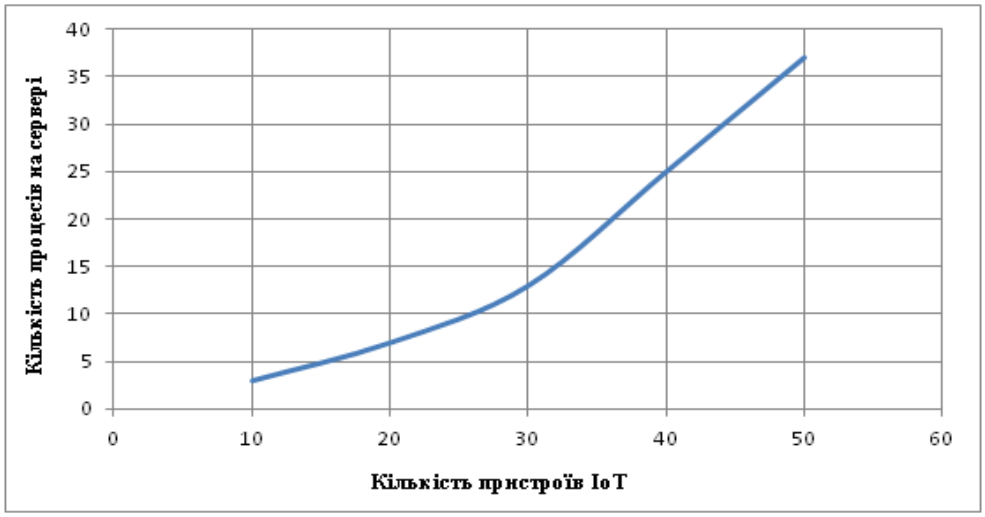

Рисунок 2 – Залежність кількості процесів на сервері СЗІ від кількості пристроїв IoT

Висновки

1. Інтернет речей є однією з найперспективніших технологій останніх років, що вже сьогодні фактично створює сотні нових продуктів для різних сфер життя. Особливу роль у розвитку Інтернету речей відіграють рішення програмного забезпечення, створення нових продуктів та розвиток сфер застосування.

2. Концепція IoT припускає інтеграцію комунікаційного устаткування і різних пристроїв. Особливість роботи таких пристроїв вимагає побудови системи захисту інформації, а особливість їх технічної реалізації – визначає централізований характер такої СЗІ .

3. Складено математичну модель навантаження централізованої СЗІ на базі теорії Ерланга та проведено імітаційне моделювань при варіації параметрів. Запропонований підхід можливий для використання при проектуванні та побудові реальних систем.

ЛІТЕРАТУРА

1. Намиот Д.Е. International Journal of Open Information Technologies ISSN 2307-8162 vol. 3, no. 5, 2015: Об учебных программах Internet of things [электронный ресурс]. – Режим доступу: http://cyberleninka.ru/article/n/ob-uchebnyh-programmah-po-internet-of-things.

2. Ложковский А.Г. Исследование параметров телефонной нагрузки на сотовой сети мобильной радиосвязи: статья / [Ложковский А.Г.] // Праці УНДІРТ. – 2001. – 10–14 с.

3. Павлушков И.В. Математика: учебник / Павлушков И.В., Розовский Л.В., Наркевич И.А. – 2013. – 320 с.

4. Nyt Tidsskrift for Matematik: The Theory of Probabilities and Telephone Conversations, vol. 20, no. B, 1909. – 33–39 с.

5. Чивилев С.В. Профессиональная радиосвязь: Теория Эрланга: как рассчитать количество каналов базовой радиостанции [Электронный ресурс]. – Режим доступу: http://www.mforum.ru/063945.htm.

6. Сучасні телекомунікації: Мережі, технології, безпека, економіка, регулювання / [Довгий С.О., Воробієнко П.П., Гуляєв К.Д. та ін.]. – К.: Азимут-Україна, 2013. – 608 с.

7. Ложковський А.Г. Теорія масового обслуговування в телекомунікаційних системах: підручник / Ложковський А.Г. – О.: ОНАЗ ім. О.С. Попова, 2012. – 112 с.

8. Защита информации в телекомуникационных системах: учеб. пособ. / Г.Ф.Конахович, В.П.Климчук, С.М.Паук, В.Г.Потапов — К.: МК-Пресс, 2005. — 288 с.

9. Левенчук А. Архитектура интернета вещей: блокчейны и онтологии [Электронный ресурс]. – Режим доступу: http://ailev.livejournal.com/1159439.html.

10.Интеграционная платформа для Интернета вещей: архитектура системы [Электронный ресурс]. – Режим доступу: http://aggregate.tibbo.com/ru/technology/architecture.html.

REFERENCES

1. Namiot D.E. “On curricula Internet of Things”. International Journal of Open Information Technologies ISSN (2015): 2307-8162. Print.

2. Lozhkovskui A.G. “Study parameters telephone burden on cellular mobile radio network”, 2001.10-14. Print.

3. Pavlyshkov I.V., Rozovskii L.V., Narkevich I.A. Mathematics, 2013. 320. Print.

4. Nyt Tidsskrift for Matematik: The Theory of Probabilities and Telephone Conversations (1909): - 33-39. Print.

5. 5.Chivilev S.V. Professional radio: Theory Erlang: how to calculate the number of channels the radio base station. Print.

6. Dovhyi S.O., Vorobiienko P.P., Huliaiev K.D., and others. Modern Telecommunications: Networks, Technology, Safety, Economy, Regulation. Kyiv: Azimuth-Ukraine, 2013. 608. Print.

7. Lozhkovskui A.G. Queueing theory in telecommunication systems. Odessa: O.S. Popov ONAT, 2012. 112. Print.

8. Konakhovich G.F., Klimchyk V.P., Spider S.M., Potapov V.G. Information security in telecommunication systems. Kyiv: MK-Press, 2005. 288. Print.

9. Levenchyk A. Architecture Internet of Things: blokcheyny and ontologies. Print.

10.Integration platform for the Internet of things: architecture.