УДК 004.056:004.77:621.396.946 **DOI:** 10.31673/2412-9070.2023.061922

Н. В. РУДЕНКО, кан. техн. наук, доцент;
І. В. ЛУЦЮК, магістр;
А. П. СУТИК, магістр,
Державний університет інформаційно-комунікаційних технологій, Київ

ДОСЛІДЖЕННЯ БЕЗПЕКИ ТА ПРИВАТНОСТІ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ У МЕРЕЖАХ МОБІЛЬНОГО ЗВ'ЯЗКУ

Дослідження безпеки та приватності систем Інтернету речей (IoT) у мережах мобільного зв'язку є актуальною та важливою темою в сучасному світі. Зростання популярності та використання IoT-пристроїв, підімкнених до мобільних мереж, створює нові можливості для комунікації, але також вносить важливі виклики, пов'язані з безпекою та захистом приватності.

Мобільні мережі, зокрема 4G і 5G, надають з'єднання для безлічі IoT-пристроїв, від розумних термостатів та вимикачів світла до медичних пристроїв та автомобілів. Однак із кожним новим підімкненим пристроєм зростає потенційна загроза для безпеки мережі та захисту особистих даних користувачів.

У статті проаналізовано різні аспекти безпеки та приватності в контексті IoT у мобільних мережах. Розкрито потенційні загрози та вразливості, а також заходи, які можуть бути вжиті для зменшення ризику.

Особливу увагу приділено підвищенню усвідомленості щодо проблем безпеки та приватності в IoT і мобільних мережах, із сприянням подальшому дослідженню та розробленню заходів для забезпечення безпеки та конфіденційності в цьому напрямку.

Ключові слова: приватність данних; мобільні мережі; шифрування комунікацій; IoT; безпека даних; зв'язок.

Вступ

Із розвитком технологій зв'язку і впровадженням 5-ї генерації мобільного зв'язку (5G) в системі Інтернету речей (IoT) постає низка важливих питань щодо безпеки та приватності. Однією з основних переваг 5G є підвищена швидкість і ефективність передавання даних, але це також створює нові виклики, пов'язані із забезпеченням конфіденційності і захистом великої кількості з'єднаних пристроїв. У запропонованій статті розглянуто вплив 5G на безпеку та приватність у системах IoT та надано рекомендації для їхнього забезпечення.

Основна частина

5G — це мобільна мережа 5-го покоління. Це новий глобальний безпроводовий стандарт після мереж 1G, 2G, 3G і 4G. Мобільна мережа 5-го покоління створює новий тип мережі, розробленої для з'єднання практично всіх і всього разом, включно з машинами, об'єктами та пристроями.

Безпроводова технологія 5G призначена для забезпечення вищої пікової швидкості передавання даних у кілька гігабіт за секунду, наднизької затримки, більшої надійності, великої пропускної здатності мережі, підвищеної доступності та більш однорідного досвіду для більшої кількості користувачів. Вища продуктивність і покращена ефективність створюють новий досвід для користувачів і під'єднують нові галузі (рис. 1).

5G працює на низьких, середніх і високих діапазонах радіочастот. Проте конкретні діапазони, що використовуються, можуть відрізнятися залежно від країни та оператора мережі.

Низькодіапазонний 5G працює на частотах, нижчих за 1 ГГц, зазвичай у діапазоні від 600 до 900 МГц. Ці стрічки забезпечують широке покриття та можуть «пробивати» стіни та інші пере-

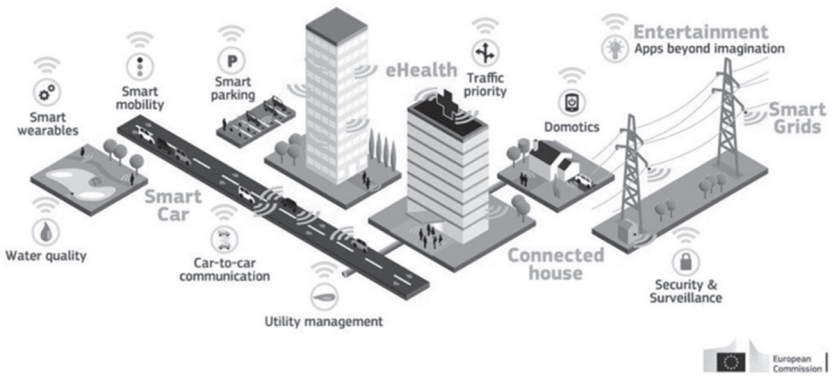

Рис. 1. Приклад можливості використання технологій 5G у комунальному господарстві, у сфері енергетики, охорони здоров'я, індустрії розваг та на транспорті

шкоди, що робить їх ідеальними для використання в сільській місцевості та всередині приміщень.

5G у середньому діапазоні частот працює на частотах від 1 до 6 ГГц, зазвичай у діапазоні від 2,5 до 3,7 ГГц. Ці діапазони забезпечують вищу швидкість передавання даних, ніж низькочастотний 5G, але з меншим покриттям.

Високосмуговий 5G працює на частотах понад 24 ГГц, також відомих як частоти міліметрових хвиль (mmWave). Ці діапазони забезпечують надзвичайно високу швидкість передавання даних, але мають обмежене покриття та легко блокуються такими перешкодами, як будівлі та дерева. Вони переважно використовуються в густонаселених районах.

Інтернет речей, або IoT, — це мережа взаємозв'язаних пристроїв, які з'єднуються й обмінюються даними з іншими пристроями IoT і хмарою. Пристрої IoT зазвичай оснащені такими технологіями, як давачі та програмне забезпечення, і можуть мати у своєму складі механічні і цифрові машини та споживчі об'єкти (рис. 2).

Організації в різних галузях все частіше використовують IoT, щоб працювати ефективніше, надавати поліпшене обслуговування клієнтів, удосконалювати процес ухвалення рішень і підвищувати цінність бізнесу. Завдяки IoT дані можна передавати через мережу, не потребуючи взаємодії «людина-людина» або «людина-комп'ютер».

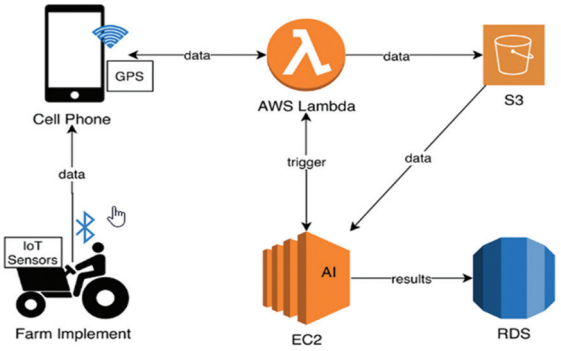

Рис. 2. Зв'язок між пристроями Інтернету речей (IoT) і хмарою

Річчю в Інтернеті речей може вважатися людина з імплантатом серцевого монітора, сільськогосподарська тварина з транспондером із біочіпом, автомобіль із вбудованими давачами, які сповіщають водія про низький тиск у шинах, або будь-який інший природно чи штучно зроблений об'єкт, якому можна призначити адресу Інтернет-протоколу та який може передавати дані через мережу.

Якщо говорити конкретніше, то 5G привносить переваги IoT у наведених далі семи важливих аспектах.

1. *Збільшена ємність:* мережі 5G розроблені для роботи з чималою кількістю пристроїв, що ідеально підходить для розгортання IoT, де велика кількість давачів і пристроїв потребують обміну даними один з одним.

2. *Менша затримка:* менший час затримки 5G свідчить про те, що пристрої IoT можуть швидше спілкуватися між собою та хмарою, що важливо для чутливих до часу програм, зокрема промислової автоматизації та безпілотних автомобілів.

3. *Вищі швидкості:* вищі швидкості 5G забезпечують більш високу швидкість передавання даних для пристроїв IoT, що важливо для застосунків, які потребують швидкого передавання великих обсягів даних, зокрема відеоспостереження та віддаленого моніторингу.

4. *Підвищена надійність:* підвищена надійність 5G гарантує, що пристрої IoT можуть завжди залишатися на зв'язку, навіть у місцях із поганим покриттям мережі.

5. *Розрізання мережі:* 5G також дає можливість розділяти окремі мережі на кілька віртуальних мереж або сегментів зі своїми особливими характеристиками та вимогами. Ці підмережі є самодостатніми та можуть бути оптимізовані для конкретних програм або випадків використання, таких як промислова автоматизація, автономні транспортні засоби або дистанційна хірургія.

6. *Граничні обчислення:* підтримання периферійних обчислень 5G дає змогу пристроям Інтернету речей обробляти та аналізувати дані локально, зменшуючи затримку та підвищуючи ефективність.

7. *Енергоефективність:* енергозберігальний дизайн мережі 5G допомагає подовжити термін служби батареї пристроїв IoT, що важливо для таких програм, як віддалений моніторинг і відстеження активів.

Однак зі зростанням кількості підімкнених пристроїв і обсягу оброблюваних даних збільшується ризик щодо безпеки та приватності. Експерти з безпеки попереджають про загрози середовищу 5G-IoT, зокрема підвищений ризик атак на відмову в обслуговуванні (DDoS) і вторгнень у службу близькості (ProSe). Величезне поширення децентралізованих мереж малого стільникового зв'язку, яких потребує 5G-IoT, ускладнить підтримання кожної системи в оновленому стані та її здатність протистояти кібератакам, що швидко розвиваються. А отже, керування безпекою є ключовим завданням для вирішення тонкощів 5G-IoT.

Порушення безпеки IoT можуть відбуватися на одному з трьох архітектурних рівнів: рівні сприйняття, мережному рівні або рівні застосунків.

Рівень сприйняття — це давачі, лічильники, приводи, камери та інші підімкнені пристрої. Порушення безпеки на цьому рівні зазвичай пов'язані з крадіжкою пристрою, атаками з перехопленням і безпекою термінала або радіочастотної ідентифікації (RFID).

Мережний рівень — дім для IoT-маршрутизатора або шлюзу — це місце, де безпека середовища 5G-IoT дійсно починає «гру». Атаки на цей рівень зазвичай пов'язані з безпекою мережі або локальної мережі, проблемами маршрутизації або безпекою даних під час передавання.

Рівень застосунків охоплює сервери та хмару, які можуть бути чутливими до атак через помилки програмного забезпечення, контролю доступу, проблем інтерфейсу програмування застосунків (API) або атак типу «відмова в обслуговуванні/розподілена відмова в обслуговуванні» (DoS/DDoS).

Інвестиції в неклієнтський безпроводовий WAN-маршрутизатор 5G можуть спростити виявлення та запобігання загрозам безпеки, забезпечуючи вбудовану наскрізну видимість мережі. Окрім ефективного апаратного рішення функції накладання безпеки 5G, включно з доступом до мережі з нульовою довірою та нарізкою мережі, відіграють значну роль у ефективному зменшенні поверхні атаки на межі глобальної мережі. Для розв'язання проблем безпеки передусім потрібні безпечні мережні архітектури, механізми та протоколи як основа для орієнтованого на 5G IoT, дотримуючись правил безпеки за проєктом, а також безпеки за функціонуванням. Крім того, оскільки в мережах 5G буде передано навіть більшу кількість даних користувачів і мережного трафіку, слід шукати вирішення безпеки великих даних за допомогою технологій штучного інтелекту, щоб визначити масштаби обсягу даних і забезпечити безпеку.

Коли хмарні обчислення та мережі хмарного радіодоступу (CRAN) інтегровані з IoT у розумних містах із підтриманням 5G, щоб розширити обчислювальну здатність масивних терміналів і підвищити енергоефективність, режим централізованого оброблення створює додаткові проблеми для безпеки та конфіденційності користувачів. Незважаючи на те, що сервери на основі периферійних обчислень тепер здатні отримувати значущу аналітику з вузлів Інтернету речей, що є критично важливим для інтелектуального трафіку або Інтернету транспортних засобів (IoV), зростає занепокоєння щодо конфіденційності постачальників даних, коли вони надають крайові застосунки і прямий доступ до вбудованих давачів.

Отже, як регулятори конфіденційності, користувачі 5G, так і промислові зацікавлені сторони почали бачити нагальну потребу в просуванні наукового прогресу в галузі безпеки та технологій збереження конфіденційності, спрямованих на забезпечення ефективного захисту інформації для орієнтованих на 5G технологій оброблення IoT. Тому все викладене має посприяти передовим дослідженням, зосередженим на різних темах, пов'язаних із безпекою та захистом конфіденційності для IoT із підтриманням 5G.

Висновки

Розвиток 5G та IoT приніс багато переваг, але також створив нові виклики для безпеки та приватності. Забезпечення безпеки та приватності в системах IoT на базі 5G потребує комплексного підходу та використання сучасних методів захисту. У статті було наведено ключові виклики та заходи, які можна вжити для забезпечення безпеки та приватності в цих системах. Розвиток технології має супроводжуватися відповідними заходами забезпечення безпеки для успішного впровадження 5G у майбутніх IoT-системах.

Список використаної літератури

1. ***Sklar B.*** *Digital Communications, Fundamentals and Applications. 2nd ed. Prentice Hall PTR, 2001.*

2. ***World's*** *most advanced broadband satellite internet. Starlink [Online]. URL: https://www.starlink.com/technology*

3. ***Cakaj S.*** *The Parameters Comparison of the 'Starlink' LEO Satellites Constellation for Different Orbital Shells // Frontiers in Communications and Networks. 2021. Vol. 2, no. 7.*

4. ***Broadband*** *LEO constellations for navigation / T. G. Reid [et al.] //Navigation, Journal of the Institute of Navigation. 2018. Vol. 65, no. 2. P. 205–220.*

5. ***Position,*** *Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications / T. G. Reid [et al.] // Wiley-IEEE. 2020. Vol. 1. Ch. Navigation from Low Earth Orbit: Part 1: Concept, Capability, and Future Promise. P. 1359–1380.*

6. ***Kassas Z. M.*** *Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications // Wiley-IEEE. 2020. Vol. 1. Ch. Navigation from Low Earth Orbit: Part 2: Models, Implementation, and Performance. P. 1381–1412.*

7. ***Tradespace*** *exploration of the next generation communication satellites / A. Aguilar, P. Butler, J. Collins, M. Guerster // AIAA Scitech 2019 Forum, 2019.*

8. ***Proakis J. G., Salehi M.*** *Digital Communications. 5th ed. McGraw-Hill, 2007.*

N. V. Rudenko, I. V. Lutsiuk, A. P. Sutyk

SECURITY AND PRIVACY RESEARCH OF INTERNET OF THINGS SYSTEMS IN MOBILE NETWORKS

The escalating integration of Internet of Things (IoT) devices with mobile networks presents unprecedented opportunities and challenges in the context of security and privacy. This paper offers a comprehensive overview of recent research focusing on the security

and privacy concerns associated with IoT systems operating within mobile networks. The fundamental concepts, emerging threats, and potential solutions in this dynamic landscape are examined.

The distinctive characteristics of IoT devices and their unique security and privacy requirements are outlined. The paper discusses inherent vulnerabilities, including limited computational resources, device heterogeneity, and the expansive attack surface resulting from interconnected devices. Additionally, the growing risks associated with data collection, transmission, and storage within mobile network environments are explored, emphasizing the importance of protecting user privacy and sensitive information.

State-of-the-art security mechanisms and protocols designed to safeguard IoT systems in mobile networks are surveyed. Approaches such as encryption, authentication, access control, and intrusion detection systems are discussed as means to mitigate potential threats. The paper addresses the challenge of secure device onboarding and underscores the importance of ensuring the integrity and authenticity of IoT components within the network.

Furthermore, the role of standards and regulatory frameworks in shaping security and privacy requirements for IoT systems is examined. Initiatives by organizations such as the Internet Engineering Task Force (IETF) and the European Union's General Data Protection Regulation (GDPR) are discussed in relation to their influence on the development and deployment of secure IoT solutions.

In conclusion, this review highlights the ongoing need for continuous research and development in the security and privacy domains of IoT systems in mobile networks. As the adoption of IoT devices and mobile network technologies continues to grow, maintaining vigilance in addressing evolving threats and ensuring compliance with emerging regulations is imperative. This paper aims to provide valuable insights into the evolving landscape of IoT security and privacy, catering to researchers, practitioners, and policymakers, and paving the way for a more secure and privacy-preserving future for IoT deployments in mobile networks.

Keywords: data privacy; mobile networks; communication encryption; IoT; data security; communication.