УДК 004.056

В.О. Ключківський
В.В. Лукічов

МЕТОД ЗАХИСТУ ДАНИХ, ОТРИМАНИХ ЗА ДОПОМОГОЮ СЕНСОРІВ 6G

Вінницький національний технічний університет

Анотація

У роботі здійснено дослідження існуючих методів захисту даних отриманих за допомогою сенсорів 6G та розроблено власний методу захисту даних отриманих за допомогою сенсорів 6G

Ключові слова: *сеснсори 6G, обфускація, принцип незв'язності, конфідеційна інформація.*

Abstract

The paper explores existing methods of protecting data obtained through 6G sensors and develops its own method of securing data acquired via 6G sensors.

Keywords*: 6G sensors, obfuscation, principle of independence, confidential information.*

Вступ

Технологія 6G, яка наступає за 5G, має на меті забезпечити ще вищі швидкості передачі даних та низьку затримку, сприяючи інноваціям у багатьох сферах, включаючи автомобільну промисловість [1]. Незважаючи на величезний потенціал прогресу, виникає ряд викликів і проблем, особливо у зв'язку з безпекою обміну даними в таких мережах. Збільшення обсягів оброблюваної інформації та різноманітність джерел її походження роблять питання захисту конфіденційності та цілісності даних надзвичайно актуальними. Особливу увагу слід приділити інформації від сенсорів, яка може включати величезний спектр особистих та конфіденційних даних, викликаючи необхідність впровадження ефективних заходів для забезпечення конфіденційності та захисту особистої інформації.

Результати дослідження

Технологія 6G, що стає наступником 5G, націлена на вдосконалення швидкостей передачі даних та зниження затримок, сприяючи інноваціям у багатьох галузях, включаючи автомобільну промисловість. Використання вдосконаленого бездротового зв'язку в системах 6G може значно підвищити безпеку та автономію автомобілів, забезпечуючи точний обмін даними між транспортними засобами та інфраструктурою, таким чином, створюючи базу для розумних мереж доріг та систем автопілоту в основі, яких лежать сенсори.

Сенсор для збору даних є технічним пристроєм, який вимірює фізичні величини або реєструє події, перетворюючи їх на електричні сигнали або цифрові дані. Ці дані використовуються для аналізу, моніторингу, керування та інших цілей.

Серед передових сенсорів в цій галузі виділяється AWR2944, який надалі буде використовуватись в нашому досліджені, як експерементальний - це високочастотний сенсор, який відзначається високою роздільною здатністю та широким частотним діапазоном (76-81 ГГц) [2]. Висока чутливість та точність вимірювань роблять його найкращим у своєму класі для виявлення та вимірювання об'єктів в різних умовах, відкриваючи нові можливості для збору та обробки даних з винятковою ефективністю. Принцип збору даних базується на використанні мікрохміліметрових хвиль, що видаються

Найчастіше AWR2944 використовується в автомобільних системах допомоги водієві (ADAS), тощо.

Однак, наряду з величезним потенціалом прогресу, виникає низка викликів і проблем, особливо щодо безпеки обміну даними в цих мережах. Збільшення обсягів інформації, які обробляються, а також різноманітність джерел її походження, роблять питання захисту конфіденційності та цілісності даних надзвичайно актуальними.

Особливу увагу в цьому контексті слід приділити інформації, здобутої від сенсорів, яка може включати в себе величезний спектр особистих та конфіденційних даних. Ця інформація може виявитися вразливою перед різноманітними загрозами, починаючи від несанкціонованого доступу та закінчуючи можливістю використання трекінгів, які на основі зібраних даних, можуть відстежувати рух користувача. Тим самим, виникає належне питання про необхідність впровадження ефективних заходів для забезпечення конфіденційності та захисту особистої інформації.

Трекінг - це процес визначення та фіксації місцезнаходження об'єкта в просторі протягом часу [3]. Цей термін широко використовується в різних контекстах, включаючи технології, спорт, дослідження та інші області

Запропонований метод базується на створені захисту даних, ще на етапі їх збору за принципом незв’язності. Основна мета якого полягає в тому, щоб зробити інформацію максимально незалежною, ускладнити або навіть унеможливити ідентифікацію взаємозв'язків між різними частинами даних чи об'єктами, що в свою чергу унеможливлює використання трекерів для порушення її приватності та конфідеційності.

Для забезпечення конфідеційності та приватності пропонується розділення інформації на конкретні типи об’єктів відповідно до характеристик (висота, ширина, довжина і т. д.), що допоможе захистити конфідеційні дані ще на етапі збор за принципом незв’язності.

На рисунку 1 представлено приклад типу “Піщоходний”.

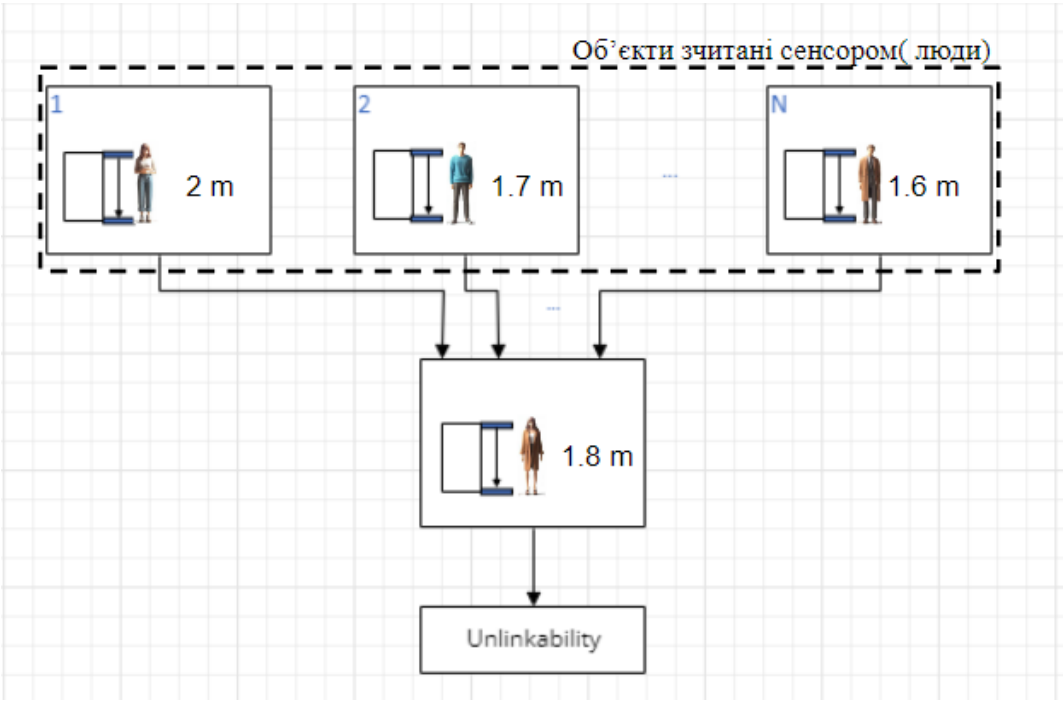

Рисунок 1 – Тип об’єкта “Пішоходний”

Після процесу обфускації за принципом незв’язності дані передаються на центральний комп’ютер автомобіля(Onboard) після чого на вишку RSU(Roadside Unit) та на центральний комп’ютер інших учасників руху за умови, якщо вони є поруч.

Даний механізм обміну інформацією сприяє взаємодії та спільному використанню безпечних та анонімізованих даних між автомобілями та іншими елементами інфраструктури. За допомогою принципу незв’язності, який забезпечує абстракцію та високий рівень захисту конфіденційності, система може взаємодіяти з іншими учасниками руху, не ризикуючи витоком особистої інформації.

Загальна сруктурна схема обміну даними в автомобільній мережі 6G зображено на рис. 2.

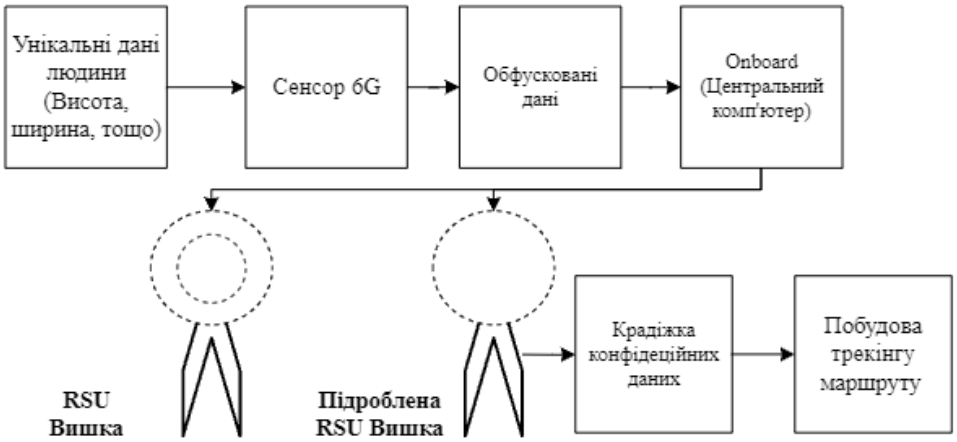

Рисунок 2 – Загальна сруктурна схема обміну даними в автомобільній мережі 6G

На основі проведеного аналізу можна впевнено стверджувати, що запропонований метод забезпечує високий рівень захисту інформації ще на етапі її збору. Навіть у випадку успішного перехоплення даних зловмисником шляхом підміни легітимної вишки RSU(Roadside Unit), що зображено на рисунку 2, система використовує принцип незв'язності, що унеможливлює побудову трекінгу маршруту особи, що сприяє уникненю можливих загроз конфідеційності та збереження приватної інформації.

Результати моделювання руху людини в середовищі MATLAB з використанням трекера JPDA (Joint Probabilistic Data Association) без застосування обфускації на основі даних із сенсорів 6G щераз підкреслили серйозні загрози для конфіденційності та приватності користувачів. Невідповідна захищеність може легко дозволити зловмисникам створювати трекінг руху осіб і порушувати їхню конфідеційність та приватність. У той же час, спроба моделювання з обфускацією завершилася невдачею, що підкреслює актуальність та ефективність дослідженя .

Висновки

Результатом дослідження є розроблений метод захисту даних на етапі збору, спрямований на вирішення актуальних проблем конфіденційності даних у мережі 6G. Розроблений метод має важливе практичне значення, забезпечуючи високий рівень безпеки та конфіденційності даних у високотехнологічному світі майбутнього.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Грінвуд, Д. "Безпека високошвидкісних бездротових мереж 6G." Журнал мережевих технологій, 2022, № 3, с. 45-56.*
2. *Technical characteristics and principles of operation of the AWR2944 sensor. [Електронний ресурс] URL: https://www.ti.com/tool/AWR2944EVM (дата звернення: 14.12.2023).*
3. *Track Closely Spaced Targets Under Ambiguity in Simulink [Електронний ресурс]. URL: https://www.mathworks.com/help/fusion/ug/tracking-closely-spaced-targets-under-ambiguity-in-simulink.html 14.12.2023).*

Ключківський Володимир Олександрович - студент групи 1БС-22м, факультет інформаційних технологій, спеціальність 125 Кібербезпека Освітньо-професійна програма – Безпека інформаційних і комунікаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: kingv8086@gmail.com.

Лукічов Віталій Володимирович - к-т техн. наук, доцент, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: lukichov.vitalyi@vntu.edu.ua.

Volodymyr Oleksandrovych Klyuchkivskyi - student of the 1BS-22m group, Faculty of Information Technologies, majoring in 125 Cybersecurity, Educational and Professional Program - Information and Communication Systems Security, Vinnytsia National Technical University, Vinnytsia, email: kingv8086@gmail.com.

Vitalii Volodymyrovych Lukichov - Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Information Security, Vinnytsia National Technical University, Vinnytsia, email: lukichov.vitalyi@vntu.edu.ua.