

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ БЕЗПЕКИ СЕНСОРНИХ МЕРЕЖ

Максим Івасів

USING ARTIFICIAL INTELLIGENCE TO SECURE SENSOR NETWORKS

Maksym Ivasiv

Міжрегіональна Академія Управління Персоналом, вул. Фрометівська 2, Київ, 03039, Україна.

Abstract. *The study examines modern approaches and methods for protecting WSNs with AI, emphasizing its efficiency and speed. Key challenges and strategies for protecting advanced algorithms are also discussed.*

Сенсорні мережі (Wireless Sensor Networks, WSN) — це сукупність автономних пристроїв, які збирають та передають дані про навколишнє середовище. Вони широко застосовуються в різних сферах, включаючи охорону здоров'я, промисловість та військову справу. Однак через обмежені ресурси та відкриту природу бездротового середовища WSN є вразливими до різноманітних атак. Використання штучного інтелекту (ШІ) може значно підвищити рівень безпеки таких мереж.

З розвитком Інтернету речей (IoT) та зростанням кількості підключених пристроїв, забезпечення безпеки сенсорних мереж стає критично важливим. Традиційні методи захисту не завжди ефективні в умовах обмежених ресурсів. ШІ пропонує нові підходи до виявлення та запобігання загрозам у реальному часі.

Основними напрямками застосування ШІ в безпеці WSN є виявлення вторгнень в систему та прогнозування можливих загроз на основі історичних даних, що дозволяє проактивно реагувати на потенційні атаки. Наприклад, модель MLSTL-WSN використовує машинне навчання для виявлення складних шаблонів та аномалій у даних WSN, що дозволяє ефективно виявляти нові техніки атак.

Але використання ШІ для безпеки сенсорних мереж мають як свої переваги, так і виклики та обмеження.

Моделі ШІ можуть навчатися на нових даних та адаптуватися до змін у мережі та виявляти та реагувати на загрози в реальному часі. Але може виникнути необхідність в оптимізації алгоритмів для роботи на пристроях з обмеженими обчислювальними можливостями. Також потрібно враховувати безпеку самих алгоритмів ШІ.

Інтеграція штучного інтелекту в системи безпеки сенсорних мереж відкриває нові можливості для підвищення їх захищеності. Незважаючи на існуючі виклики, перспективи використання ШІ в цій сфері є багатообіцяючими. Подальші дослідження повинні зосередитися на розробці легких та енергоефективних моделей, здатних працювати в реальному часі та адаптуватися до нових загроз.

Бібліографія

1. Ramana, K. et al. WOGRU-IDS—An intelligent intrusion detection system for IoT-assisted Wireless Sensor Networks. *Comput. Commun.* 196, 195–206 - 2022.
2. Batiha T. and Krömer P., Design and analysis of efficient neural intrusion detection for wireless sensor networks, *Concurrency and Computation: Practice and Experience* 33(23) (2021), e6152.