Сагайдачний О.М., студент
Гвоздецька К.П., студентка
Харківський національний університет радіоелектроніки, м. Харків
Кафедра Електронних обчислювальних машин

ПРОБЛЕМИ БЕЗПЕКИ В БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖАХ

Безпека і конфіденційність – величезні проблеми у всіх типах бездротових мереж, які є привабливими мішенями для проникнень і інших атак. У мережах, створених для відстеження цілей та моніторингу інфраструктури, порушення коректного алгоритму функціонування мережі можуть мати дуже серйозні наслідки [1]. Сенсорні мережі часто використовуються в віддалених областях, без можливості постійного контролю за працездатністю мережі, і тим самим вони стають легкою мішенню для фізичних атак, несанкціонованого доступу і пошкоджень.

Сенсорні вузли зазвичай дуже обмежені ресурсами і працюють в суворих умовах, що полегшує дискредитацію вузлів [2]. У порівнянні з традиційними атаками і механізмами безпеки, розробленими для Інтернету, бездротові сенсорні мережі мають безліч унікальних проблем, які потрібно розглянути, звертаючись до проблем безпеки:

- Обмеження ресурсу. Традиційні механізми безпеки не придатні для бездротових сенсорних мереж з обмеженими ресурсами [3]. Багато механізмів безпеки в обчислювальному відношенні дороги або вимагають зв'язку з іншими вузлами або віддаленими пристроями (наприклад, з метою авторизації), що призводить до енергетичних витрат. Маленькі сенсорні пристрої також обмежені в своїй доступною пам'яті. Традиційні алгоритми безпеки, що вимагають істотної кількості пам'яті і простору пам'яті, неможливі для таких сенсорів.
- Відсутність центрального управління. Часто неможливо мати центральну точку управління в сенсорних мережах, наприклад, через їх великого масштабу, обмежень ресурсу і мережевий динаміки (топологічних змін, поділу

мережі). Тому рішення щодо забезпечення безпеки повинні бути децентралізовані і вузли повинні співпрацювати, щоб досягти безпеки [4].

- Віддалене розташування. Перша лінія захисту проти атак безпеки - це забезпечення контрольованого фізичного доступу до сенсорного вузла. Багато бездротових сенсорних мереж розміщуються у віддалених і важкодоступних місцях, розгорнутих в середовищах, відкритих для публічного доступу, або настільки великих, що буде неможливо постійно контролювати і захищати сенсорні вузли від фізичних атак.

З іншого боку, певні характеристики сенсорних мереж спрощують умови безпеки. Наприклад, самоврядування і самовідновлення функціонування бездротової сенсорної мережі можуть дозволити їй продовжувати роботу, навіть якщо сенсорний вузол або область сенсорної мережі були поставлені під загрозу [5].

Література

1. Tkachov, V., Kovalenko, A., Kuchuk, H., & Ni, I. (2021). Метод забезпечення живучості високомобільної комп'ютерної мережі. Advanced Information Systems-Sučasnì ìnformacìjnì sistemi, 5(2), 159-165.

2. Kuchuk, N., Kovalenko, A., Tkachov, V., Rosinskiy, D., & Kuchuk, H. (2021). Predicting traffic anomalies in container virtualization. Computer And Information Systems And Technologies.

3. Коваленко А.А. Метод забезпечення живучості комп’ютерної мережі на основі VPN-тунелювання / А.А. Коваленко, Г.А. Кучук, В.М. Ткачов // Системи управління, навігації та зв’язку. Збірник наукових праць. – Полтава: ПНТУ, 2021. – Т. 1 (63). – С. 90-95. – doi:https://doi.org/10.26906/SUNZ.2021.1.090.

4. Tkachov V. Principles of Constructing an Overlay Network Based on Cellular Communication Systems for Secure Control of Intelligent Mobile Objects / Vitalii Tkachov, Andriy Kovalenko, Mykhailo Hunko and Kateryna Hvozdetska // Информационные технологии и безопасность. Материалы XIX Международной научно-практической конференции ИТБ-2020. – К.: ООО «Инжиниринг», 2020.

5. Ткачев, В. Н., & Токарев, В. В. (2017). Спосіб передачі цифрових даних мультикоптерною системою між сегментами розподіленої сенсорної мережі та базовою станцією. Пат. на корисну модель 118921 Україна; ХНУРЕ. – 2017.