УДК 621.391

О.О. Семенова
А.В. Джус
В.В. Мартинюк

МЕТОДИ ШИФРУВАННЯ ДАНИХ У БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖАХ НА ОСНОВІ ГЕНЕТИЧНИХ АЛГОРИТМІВ

Вінницький національний технічний університет

Анотація

У роботі розглядаються шляхи застосування генетичних алгоритмів для оптимізації шифрування в БСМ, а також переваги та виклики використання цих алгоритмів.

Ключові слова: безпровідні сенсорні мережі, шифрування, генетичний алгоритм.

Abstract

The paper examines ways to apply genetic algorithms to optimize encryption in WSN, as well as the advantages and challenges of using these algorithms.

Keywords: wireless sensor networks, encryption, genetic algorithm.

Вступ

У сучасному світі безпровідні сенсорні мережі (БСМ) набули великого поширення завдяки своїй здатності ефективно збирати і передавати інформацію у різноманітних сферах застосування: від охорони навколишнього середовища до військових та медичних систем. Ці мережі складаються з численних маленьких датчиків (сенсорів), які можуть взаємодіяти між собою через безпровідні канали зв'язку, збираючи дані про різні параметри навколишнього середовища, наприклад, температуру, вологість, тиск або рух.

Проте, незважаючи на численні переваги, БСМ мають і ряд суттєвих обмежень. Одним з найбільших викликів є обмеження ресурсів, таких як енергоспоживання, обчислювальна потужність сенсорів і обмежений обсяг пам'яті. Це ускладнює використання стандартних методів шифрування, які потребують значної обчислювальної потужності або великих обсягів пам'яті.

З цієї причини важливим завданням є розробка ефективних методів шифрування, які забезпечують захист даних, але при цьому враховують обмеження ресурсів сенсорів. Одним із найбільш перспективних підходів до вирішення цієї проблеми є використання генетичних алгоритмів (ГА). Вони є які є частиною класу еволюційних алгоритмів, можуть бути використані для оптимізації процесів шифрування, зокрема для пошуку ефективних методів генерації та розподілу ключів, а також для побудови адаптивних криптографічних систем, що враховують зміни умов роботи мережі.

Результати дослідження

У БСМ існує безліч потенційних загроз, що ставлять під сумнів безпеку та цілісність даних, переданих мережею. Основні загрози включають: підслуховування, фальсифікацію даних, атаки на цілісність мережі, атаки на енергозабезпечення, фізичні атаки [1].

Класичні методи шифрування, незважаючи на їх надійність і безпеку, мають кілька суттєвих обмежень у контексті безпровідних сенсорних мереж. Оскільки ці мережі працюють в умовах обмежених ресурсів (пам'ять, обчислювальна потужність, енергоспоживання), їх використання може бути неефективним [2].

Одним із перспективних підходів для забезпечення ефективного шифрування в БСМ є використання генетичних алгоритмів [3]. ГА є частиною класу еволюційних алгоритмів, які можуть використовуватися для вирішення складних оптимізаційних задач, таких як пошук оптимальних шифрувальних ключів або налаштувань криптографічних систем. Вони імітують процес природного відбору, де "найкращі" рішення, що забезпечують найкращий результат для заданої задачі, виживають і передають свої

властивості наступним поколінням та ґрунтуються на ідеях еволюції, що включають мутації, схрещування та відбір.

ГА можуть бути особливо корисними для шифрування в безпровідних сенсорних мережах з кількох причин. Вони можуть автоматично адаптуватися до змін у мережі. Оскільки БСМ можуть зазнавати змін у топології або в ресурсах, ГА здатні підлаштовувати параметри шифрування в реальному часі, забезпечуючи баланс між безпекою та енергоспоживанням. ГА можуть використовуватися для пошуку оптимальних параметрів шифрування, таких як розміри ключів, методи генерації ключів або алгоритми шифрування, які максимально підходять для умов конкретної мережі. ГА можуть допомогти в пошуку ефективних стратегій для мінімізації енергозатрат під час шифрування та передачі даних. Наприклад, можна оптимізувати частоту генерації нових ключів або використовувати методи шифрування, які вимагають менших обчислювальних ресурсів. Також, ГА можуть допомогти створити нові методи шифрування, комбінуючи різні криптографічні підходи для досягнення більш високого рівня безпеки в БСМ.

Попри значний потенціал, застосування генетичних алгоритмів для шифрування в БСМ стикається з кількома серйозними викликами та проблемами, які потребують подальшого дослідження і вирішення. Так, ГА можуть бути обчислювально затратними, оскільки вимагають значної кількості ітерацій для досягнення оптимального результату. Це може бути проблемою в умовах БСМ, де сенсори мають обмежені обчислювальні можливості. Також застосування генетичних алгоритмів вимагає налаштування кількох параметрів, таких як розмір популяції, кількість ітерацій, параметри схрещування та мутації. Це може бути складно для реальних мереж, де сенсори часто працюють в умовах змінної топології та обмежених ресурсів. Інтеграція генетичних алгоритмів у вже існуючі мережі потребує значних зусиль для забезпечення стабільності та ефективності шифрування в реальному часі.

Висновки

Генетичні алгоритми є перспективним інструментом для оптимізації шифрування в безпровідних сенсорних мережах, оскільки вони дозволяють забезпечити адаптивність, підвищити безпеку і знизити енергозатрати. Проте їх застосування має певні обмеження, такі як високі обчислювальні витрати і складність налаштування в реальних мережах. Для подальшого розвитку цієї технології необхідно вдосконалювати алгоритми з урахуванням ресурсних обмежень сенсорів і забезпечувати їх ефективну інтеграцію в існуючі мережі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. S. B. Sasi, N. Sivanandam, and Emeritus, “A Survey on Cryptography using Optimization algorithms in WSNs,” Indian Journal of Science and Technology, vol. 8, no. 3. Indian Society for Education and Environment, p. 216, Feb. 01, 2015. doi: 10.17485/ijst/2015/v8i3/59585.
2. Burhan, I. M., Ibrahim, S. khalil, Jebur, Z. T., Abdul Zahra, M. M., Salih, M. A., & Adnan Jaleel, R. (2021). Secure wireless sensor network using cryptographic technique based hybrid genetic firefly algorithm. In Periodicals of Engineering and Natural Sciences (PEN) (Vol. 9, Issue 4, p. 1159). International University of Sarajevo. https://doi.org/10.21533/pen.v10i1.2608
3. Hamici, Z. (2018). Towards Genetic Cryptography for Biomedical Wireless Sensor Networks Gateways. In IEEE Journal of Biomedical and Health Informatics (Vol. 22, Issue 6, pp. 1814–1823). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/jbhi.2018.2860980

Семенова Олена Олександрівна – канд. техн. наук, доцент кафедри інфокомунікаційних систем і технологій, Вінницький національний технічний університет, м. Вінниця, e-mail: semenova.o.o@vntu.edu.ua

Джус Андрій Васильович – аспірант групи 172-23а, факультет інформаційних електронних систем, Вінницький національний технічний університет

Мартинюк Володимир В’ячеславович – аспірант групи 172-23а, факультет інформаційних електронних систем, Вінницький національний технічний університет

Semenova Olena O. – Cand. Sc. (Eng), Associate professor at the Department of Infocommunication systems and technologies, Vinnytsia National Technical University, Vinnytsia, e-mail: semenova.o.o@vntu.edu.ua

Dzhus Andrii V. – post-graduate student of 172-23a group, Faculty of Information Electronic Systems, Vinnytsia National Technical University

Martyniuk Volodymyr V. – post-graduate student of 172-23a group, Faculty of Information Electronic Systems, VinnytsiaNational Technical University