УДК 004.732
Базан І.В., Коваль А.А.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИЯВЛЕННЯ КІБЕРАТАК В «РОЗУМНОМУ МІСТІ» НА ОСНОВІ МАШИННОГО НАВЧАННЯ

I. Bazan, A. Koval

DETECTING CYBERATTACKS IN A SMART CITY BASED ON MACHINE LEARNING

Технологічні винаходи змінили динаміку розвитку світу. Інфраструктура в кожній галузі автоматизується за допомогою Інтернету речей та бездротових мереж зв'язку. «Розумні міста» формуються на бездротовому зв'язку, де інфраструктура за своєю природою уможливлює велику кількість кібератак. Тому вразливості в «розумних містах» потребують належного вирішення. Сфера «розумних міст» досить різноманітна і має багато застосувань, включаючи електронний уряд, «розумні» будинки, інтелектуальний транспорт, телемедицину, «розумні» мережі, моніторинг, енергетику та багато іншого [1].

Безпека мереж передачі даних є темою для багатьох дослідників у всьому світі через постійне зростання кількості кібератак. Система виявлення вторгнень - це система, яка повинна ідентифікувати фальшиві пакети даних. Оптимальний алгоритм системи виявлення вторгнень балансує між високою точністю та показниками хибнонегативних і хибнопозитивних спрацьовувань. Крім того, основною її метою є виявлення можливих кібератак. «Розумні міста» потребують захищених каналів зв'язку, тому система виявлення вторгнень відіграє важливу роль [2]. Різноманітні технології, такі як ланцюги Маркова, машинне навчання, оптимізація та пуассонівський розподіл, використовуються для покращення систем виявлення сигнатур, аномалій та гібридних вторгнень.

Мережі IoT є вразливими до кібератак, тому в «розумному місті» протидія таким загрозам є великим викликом. DOS, DDOS, Sybil-атаки, SQL-ін'єкції та атаки зловмисного програмного забезпечення є поширеними типами атак в середовищі IoT, тому «розумні міста» постійно піддаються цим атакам. Результатом незахищеної мережі сенсорних вузлів може бути збій системи або припинення роботи сервісу, якщо не застосовувати превентивні засоби для забезпечення надійності і захищеності.

Існує багато рішень, які можуть бути використані відповідно до потреб захисту [3]. Найкращим підходом у виявленні різних загроз у «розумних містах» є машинне навчання. Машинне навчання для виявлення кіберзагроз у мережах «розумного міста». Існує три основні типи підходів машинного навчання: на основі аномалій, на основі сигнатур та гібридний. Виявлення на основі аномалій відбувається за допомогою інтелекту системи, навченого різними методами, підхід на основі сигнатур порівнює мережевий трафік з існуючими сигнатурами або шаблонами атак, що призводить до виявлення загроз, а гібридна система є сумішшю активів обох підходів, що робить її більш ефективною та точною, ніж обидва. Залежно від сценаріїв середовища, різні дослідники розробили різні типи системи виявлення вторгнень, використовуючи різні підходи, алгоритми з різними цільовими системами і порівнюючи точність і достовірність запропонованого ними алгоритму з іншими алгоритмами в своїх тематичних дослідженнях .

Література

1. Cimen, H., Palacios-García, E. J., et al. Smart-Building Applications: Deep Learning-Based, Real-Time Load Monitoring. IEEE Industrial Electronics Magazine, 15(2), 4-15.

2. Rincy N, T., & Gupta, R. Design and development of an efficient network intrusion detection system using machine learning techniques. Wireless Communications and Mobile Computing, 2021, 1-35.

3. Al-Turjman, Fadi, Hadi Zahmatkesh, and Ramiz Shahroze. "An overview of security and privacy in smart cities' IoT communications." Transactions on Emerging Telecommunications Technologies 33.3 (2022): e3677.