Секція 1

ЗАХИСТ СИСТЕМ РОЗПІЗНАВАННЯ ДОРОЖНІХ ЗНАКІВ ВІД АТАК ТА ВТРУЧАННЯ

Ганжа Д. Є.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Шостак А. В.

Актуальність. З розвитком технологій машинного навчання, штучного інтелекту та автономних транспортних засобів системи розпізнавання дорожніх знаків стали невід'ємною частиною сучасної транспортної інфраструктури. Вони дозволяють автомобілям "читати" і розуміти дорожні знаки, дотримуватись правил дорожнього руху і, таким чином, підвищувати безпеку на дорогах [1]. Однак із зростанням значущості цих систем зростає й потенційна загроза їхній безпеці. У цьому контексті аналіз та захист від уразливостей у системах розпізнавання дорожніх знаків стають актуальними завданнями, які потребують серйозної уваги та досліджень. Як і багато інших комп'ютерних систем, системи розпізнавання дорожніх знаків стають об'єктами уваги кіберзлочинців.[2] Злом і втручання в такі системи можуть призвести до створення хибних знаків, зміни дорожніх інструкцій та підвищення ризику аварій. З появою нових технологій, таких як нейронні мережі та комп'ютерний зір, системи розпізнавання дорожніх знаків стають все більш точними та здатними. Однак із зростанням їхньої складності зростає і потенційна вразливість.

Метою даної роботи є аналіз та дослідження методів захисту систем розпізнавання дорожніх знаків від атак та втручання.

Автори дослідження провели ряд експериментів, націлених на обхід моделей, заснованих на обмеженні глибокого навчання, та продемонстрували їхню здатність обманювати системи "зору" при розпізнаванні дорожніх знаків. В рамках експерименту було обрано знак "STOP", і за допомогою внесених змін зловмисники змогли скласифікувати його моделлю як «SPEED LIMIT 45» [3]. Основним методом було виявлення таких областей на дорожньому знаку, які найбільше вносять спотворення та призводять до помилок у роботі класифікатора. Цікаво, що запропонований підхід до обману був успішно адаптований та перевірений на інших дорожніх знаках, що наголошує на його ефективності [4].

Основні положення. Для забезпечення своєчасного виявлення атак або втручання в систему розпізнавання дорожніх знаків рекомендується застосовувати комплексний підхід, що включає систему виявлення атак, механізм оповіщення та реагування, а також застосування додаткових заходів захисту на основі виявлених атак. Цей підхід сприяє ефективному

захисту системи від потенційних загроз та забезпечує надійне функціонування системи розпізнавання дорожніх знаків.

Висновки. Системи розпізнавання дорожніх знаків перебувають у стадії активного розвитку та інтеграції до сучасних автомобілів. У міру поширення розумних доріг та автономних автомобілів, забезпечення їхньої безпеки стає все більш актуальним завданням. Системи розпізнавання дорожніх знаків можуть також включати відеоспостереження і збір даних про дорожню обстановку. Захист цих даних від незаконного доступу та використання також є вкрай важливим. Виходячи з цих факторів, стає зрозумілим, що забезпечення безпеки та надійності систем розпізнавання дорожніх знаків – це необхідність, яка сприяє покращенню дорожньої безпеки та захисту даних користувача.

Список літератури

1. A. Geiger, P. Lenz, and R. Urtasun. Are we ready for autonomous driving? the KITTI vision benchmark suite. In Computer Vision and Pattern Recognition (CVPR), 2012 IEEE Conference on, pages 3354–3361. IEEE, 2012;
2. Безпека машинного навчання: чи ефективні методи захисту чи нові загрози? *Habr*. URL – https://habr.com/companies/pt/articles/416691/ (дата звернення: 11.10.2023);
3. A. Nguyen, J. Yosinski, and J. Clune. Deep neural networks are easily fooled: High confidence predictions for unrecognizable images. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 428–435, 2015;
4. Robust Physical-World Attacks on Deep Learning Visual Classification. *Arxiv*. URL – https://arxiv.org/pdf/1707.08945.pdf (дата звернення: 15.10.2023).

Відомості про авторів

Ганжа Дмитро Євгенійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.hanzha@student.csn.khai.edu
Шостак Анатолій Васильович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., доцент, a.shostak@csn.khai.edu