Інтелектуальні системи контролю дорожнього руху є новітньою перспективою для зменшення кількості затор та покращення ситуації із дорожнім рухом в містах.

Список використаних джерел

1. Як розумне перехрестя Honda зменшує кількість аварій? – Tkar.ua:
URL: https://tokar.ua/read/28203 (дата звернення: 02.11.2022).
2. Intelligent transportation system:
URL: https://en.wikipedia.org/wiki/Intelligent_transportation_system (дата звернення: 02.11.2022).
3. Sakura-T:
URL: https://cloud.innovinnprom.com/app/ (дата звернення: 02.11.2022).
4. Jun Liu, Chuan-Wei Liang, Min Li, Ke Jian, Lan Qin, and Jing-Cheng Liu. Principle Research on a Novel Piezoelectric 12-DOF Force/Acceleration Sensor/Liu Jun, Liang Chuan-Wei, Li Min, Jian Ke, Qin Lan , and Liu Jing-heng//Journal of Sensors.–V.2017. – Article ID 2836365. –16 pages.
5. INTELLIGENT INTERSECTION & TRAFFIC NODE:
URL: https://www.veronet.eu/solutions/intelligent-intersection.html (дата звернення: 02.11.2022).

УДК 004.56.5(043.2)

Лісовик Є.С., магістр
Крижановський В. Г., д.т.н., професор, професор кафедри інформаційних технологій

ЗАХИСТ ДАНИХ ЗА ДОПОМОГОЮ ПІДХОДУ ARMET

Донецький національний університет імені Василя Стуса, м. Вінниця

ВСТУП

IoT - це все, що забезпечує надзвичайний зв'язок між різними об'єктами в галузях промисловості. Як уже згадувалося раніше, низка перспективних та позитивних тенденцій в інформаційному просторі заклали міцну і стійку основу для візуалізації майбутніх перспектив ідеї IoT.

Однією з найголовніших проблем є безпека мережі[1], оскільки інформація передається ще й по бездротовому середовищу, котре є більш уразливим в наслідок використання відкритого простору. На даний момент це є гострою проблемою та своєрідним бізнесом. Об’єктом дослідження є Інтернет речей (IoT)[2]. Предметом дослідження є методика(алгоритм) для забезпечення максимального захисту IoT.

RSM – Runtime security monitor прототип для виявлення «обчислювальних» атак, який буде виявляти всі спроби порушення визначених умов. Важливо, запрограмованість умов дозволяє динамічно регулювати час виконання нагляду за тим, як нові умови створюються законодавчою базою, що

з’являється. PID – регулятор, який був впроваджений як окрема, незалежна складова RSM.

В результаті вдасться знайти ознаки, за якими можна уникнути кібер-атак та небажаних порушень роботи системи, а також можливість відновлення даних за допомогою моделі довіри. Розроблено програмне забезпечення на основі підходу ARMET[3], результати якого базуються на незалежному PID-контролері.

Проблема, що вирішується - забезпечення інформаційної безпеки IoT, збереження даних в умовах різноманітних атак, впливу навколишнього середовища, а також фізичного втручання в систему. Мета – забезпечення інформаційної безпеки Інтернету речей для захисту даних від можливих подразників шляхом вибору оптимального алгоритму способів(методів) захисту.

Актуальність – у зв'язку з появою комп'ютерів, глобальних розширень комп'ютерних мереж і появою цілого віртуального світу, з'явилася можливість крадіжки інформаційних даних та ресурсів у незахищених користувачів.

Мета – експериментальна перевірка системи на по стороннє втручання в дію автоматизованої роботи контролера та порівняльна характеристика роботи циклу в різних умовах.

ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ АТАК ТА ЇХ ЗАПОБІГАННЯ

ході роботи вагомою потребою стало запровадження контролера, який би контролював затрату часу. Частиною підходу ARMET є PID[4] – регулятор, який був впроваджений як окрема, незалежна складова RSM.

Був проведений експеримент, який проходив на MacBook Pro з процесором Intel Core i7 з частотою 2,8 ГГц. У реальному робочому середовищі PID буде працювати як додаток у програмованому логічному контролері, а наш RSM[5] працюватиме як частина проміжного програмне забезпечення. Таким чином, програма PID буде розроблена через будь-яке середовище розробки додатків, наприклад, з використанням драбинної логіки, тоді як RSM буде частиною операційної системи.

Припустимо, що PID - контролер кожен раз запускає цикл керування в підсистемі довжиною 0,1 с, що є дуже низькою частотою циклів керування для такого контролера. Наш експеримент моделює підсистему протягом 100 с, тобто 1000 циклів керування, і ми спостерігаємо це, коли вмикаємо детальний моніторинг, RSM споживає 8.93 × 10-4 с часу процесора і 9.07 × 10-4 с(Рис. 1) реального часу для кожного циклу алгоритм PID, який дуже малий (менше 2%) порівняно з тривалістю циклу керування (0,1 с)..

Per 1 x 10^{-1} Cycle	CPU	Real-time
Full RSM	9.06 x 10^{-4}	9.07 x 10^{-4}
No Data Flow Checks	2.24 x 10^{-5}	3.19 x 10^{-5}
End to End	2.98 x 10^{-4}	3.01 x 10^{-4}

Рис. 1 - Продуктивність виконання програми

Для демонстрації, ми змоделювали PID-регулятор із чотирма параметрами: задане значення та три вагові коефіцієнти Kp, Ki і Kd.
Виконаємо наступні дії:
1) Використаєм значення датчика, щоб оцінити стан системи.
2) Обчислити різницю між оцінюваною системою стану і задане значення контролера (термін помилки).
3) Обчисліть локальну похідну похибки.
4) Інтеграція помилки.
5) Обчислити відповідну поправку:
   а) похибку помножити на Kp;
   б) інтеграл похибки помножити на Ki;
   в) похідну похибки помножити на Kd.
6) Обчисліть і виведіть суму цих трьох умов як термін корекції.

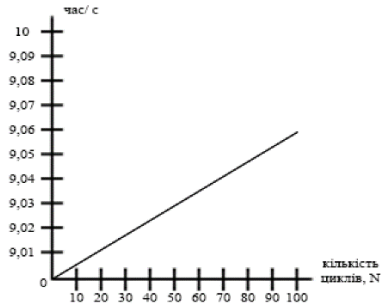

Рис. 2 - Цикл відпрацював коректно

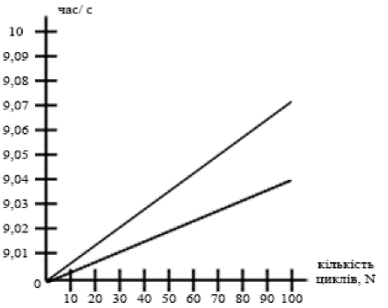

Рис. 3 - Максимальне допустиме відхилення

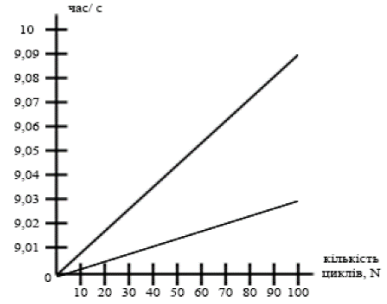

Рис. 4 - Показники стороннього втручання в роботу циклу

На підставі отриманих даних було проаналізовано і визначено коректність роботи циклу(Рис. 2),допустимі(Рис. 3) і не допустимі(Рис.4) відхилення в роботі

датчика, який дає зрозуміти, що в разі хакерської атаки відхилення часу буде не в межах допустимості, яке сповістить про некоректність роботи системи.

ВИСНОВОК

В ході проведення тестування на захищеність даних в системі Інтернету речей нерідко буває ситуація, коли важливі дані або викрадають, або спеціально змінюють для заподіяння шкоди. Через що людство втрачає велику кількість інформації, а також страждають фінансові капітали.

Було обраховано кількість затрати часу на виконання одного циклу роботи програми та однієї тисячі циклів керування. Також було визначено допустиме максимальне відхилення та недопустиме відхилення, що буде значити, що хтось втрутився в роботу нашої системи. Це дає змогу оцінити якість і швидкість роботи PID-контролера. Адже, він є ключовою частиною в роботі всієї системи, що в комплексі з RSM дає потужну захист системи.

Список використаних джерел

1. *Cornelia Győrödi, Robert Győrödi, Roxana Sotoc, "A Comparative Study of Relational and Non-Relational Database Models in a Web- Based Application" in International Journal of Advanced Computer Science and Applications, vol. 6, No. 11, pp78-82, 2015, DOI: 10.14569/IJACSA.2015.061111.*
2. *J. Siegel and S. Sarma, "A Cognitive Protection System for the Internet of Things," in IEEE Security & Privacy, vol. 17, no. 3, pp. 40-48, May-June 2019, doi: 10.1109/MSEC.2018.2884860.*
3. *Howard Shrobe, Dimitrios Serpanos, Muhammad Taimoor Khan, "ARMET: Behavior-Based Secure and Resilient Industrial Control Systems" in Proceedings of the IEEE, PP(99):1-15, doi: 10.1109/JPROC.2017.2725642.*
4. *A. Salisu, Aminu Bugaje, A. Z. Loko, "IOT BASED HOUSEHOLD ELECTRICITY ENERGY MONITORING AND CONTROL" in FUDMA Journal of Sciences, Vol. 4 No. 4, December, 2020, pp 77 – 84, doi: 10.33003/fjs-2020-0404-466.*
5. *Muhammad Taimoor Khan, Dimitrios Serpanos, Howard Shrobe, "Sound and Complete Runtime Security Monitor for Application Software" in arXiv, pp 1-3, 17 Jan 2016, doi: 10.48550/ arXiv:1601.04263v1.*

УДК 316.485.26:316.776.23](477)(043.2)

Мазур Ю.О., здобувачка 4 курсу спеціальності 125 «Кібербезпека»
Крижановський В. Г., д.т.н., професор, професор кафедри інформаційних технологій

ПРАВИЛА ІНФОРМАЦІЙНОЇ ГІГІЄНИ ПІД ЧАС ВІЙНИ