УДК 004.056

СИСТЕМА ВИЯВЛЕННЯ ВТОРГЕНЬ В SCADA-СИСТЕМИ ЯК ЕЛЕМЕНТ КІБЕРВІДМОВОСТІЙКОСТІ

С. С. Літвінчук[1], Л. Ю. Гальчинський[1]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

Ця стаття містить інформацію про цілі безпеки та вразливості систем диспетчерського керування та збору даних (SCADA). Також тут розглядається специфіка розробки системи виявлення вторгень (IDS) для SCADA та запропоновано модель виявлення з використанням згорткової нейронної мережі (CNN) та рекурентного блоку зі шлюзом GRU. Вчасне виявлення вторгнення дає можливість системі управління релевантно відреагувати на загрозу і пом'якшити деструктивну дію кібератаки. Дана модель IDS буде протестована з використанням вдіомого датасету NSL-KDD.

Ключові слова: SCADA, IDS, CNN, GRU, глибоке навчання.

Вступ

Системи SCADA (Supervisory Control And Data Acquisition) використовуються для контролю та моніторингу промислових процесів. Сьогодні вони в основному о використовуються в сфері енергетики, водопостачання, транспортування нафтопродуктів та ін., тобто для управління об'єктами критичної інфраструктури. Оскільки сучасні SCADA мають ряд вразливостей, за останні роки було здійснено низку успішних атак на дані системи [1]. У 2015-2016 роках було здійснена серія кібератак на українську енергетику, в результаті якої, близько чверті мільйона жителів країни залишилося без світла [2]. Ці події та численні факти в інших країнах світу ставлять проблему кіберстійкості(кіберрезильєнтності) систем критичної інфраструктури, які управляються з використанням SCADA. Методологія кіберрезильєнтності, розвинутої багатьма авторами [3], передбачає виявлення вторгнень, як один з обов'язкових елементів [4]. Розробка виявлення вторгнення (IDS) для даних систем є актуальною проблемою, яка відзначається своєю специфікою.

1. Цілі безпеки SCADA

Основою безпеки систем SCADA є першочергове забезпечення доступності, а потім – авторизація, автентифікація, збереження цілісності та конфіденційності даних.

Важливо забезпечити безперервний доступ до систем управління, оскільки вони керують критичними процесами в реальному часі, і будь-які затримки можуть бути катастрофічними. Авторизація та автентифікація забезпечують, що тільки належні користувачі мають доступ до контролю систем, що допомагає відвернути неавторизований доступ. Цілісність та конфіденційність даних захищають від небажаних змін та витоку інформації відповідно.

Варто зазначити також те, що вимоги до безпеки IT-систем різняться з вимогами до SCADA-систем. Так, для перших затримка може бути доцільною, однак для систем SCADA навіть невелика затримка може мати погані наслідки, тобто в цих системах час реакції є критично важливим. Так само як і для SCADA-систем, цілісність даних є важливою. Однак для SCADA-систем більш важливою є безпека людини.

2. Вразливості SCADA

Як і будь-яка система, SCADA має ряд вразливостей [1, 5] якими можуть скористатися зловмисники, щоб здійснити атаку та вивести систему з ладу. У 1960-х роках, коли були створені перші SCADA-системи, питанням інформаційної безпеки приділялося мінімум уваги. Ці системи були замкнутими і залежали від спеціалізованого обладнання. Однак, сучасні SCADA-системи, використовуючи розподілені мережі та інтернет-протоколи, стали більш вразливими до кібератак.

В SCADA-системах додатки та служби часто використовують незахищені мережеві порти, що дає змогу атакувальникам отримати доступу до системи, зібрати дані про неї чи отримати права адміністратора. Через відсутність належної перевірки вхідних даних, зловмисники можуть маніпулювати процесами у SCADA-системах.

Велика кількість вразливостей пов'язана з помилками конфігурації безпеки, а використання протоколів без вбудованого захисту, аутентифікації чи шифрування даних сприяє можливості перехоплення зловмисниками конфіденційної інформації.

3. Системи виявлення вторгень

Визначення та загальна класифікація. Виявлення вторгнень – це процес моніторингу подій, що відбуваються в комп'ютерній системі чи мережі, та аналізу їх на наявність ознак можливих інцидентів, які є порушеннями або неминучою загрозою порушення політик комп'ютерної безпеки [6]. Система виявлення вторгнень (IDS), представляє собою програмне чи апаратне рішення, яке ідентифікує зловмисні дії, активність в комп'ютерних системах з метою забезпечення їхньої безпеки.

Класифікація IDS:

1. За місцем розгортання:
   - Host-based iDS – розміщені безпосередньо на окремих пристроях, аналізують дані локально.
   - Network-based IDS – розгорнуті на ключових точках мережевої інфраструктури для моніторингу мережевого трафіку.
   - Hybrid-based IDS – інтегрують функціональність як мережевих, так і хост-базованих систем виявлення вторгнень.
2. За методами виявлення вторгень:
   - Signature-based IDS – використовують відомі шаблони, сигнатури атак для ідентифікації вторгнень.
   - Anomaly-based IDS – аналізують відхилення від звичайної поведінки, що можуть вказувати на вторгнення.

Специфіка IDS для SCADA. Системи виявлення вторгнень (IDS) мають критичне значення у захисті кіберфізичних систем, виявляючи потенційні атаки. Правильно налаштовані IDS можуть автоматично ідентифікувати загрози, знижуючи ризики і збитки.

Оскільки SCADA-системи мають жорсткі вимоги до обробки даних у реальному часі, збереження їх цілісності, стандартизовані шаблони трафіку та обмежена кількість телекомунікаційних протоколів, вимагається створення та впровадження спеціалізованих та складних систем для виявлення вторгнень у дані системи. А так як, SCADA критично залежить від реального часу та цілісності даних, IDS повинні забезпечувати швидку реакцію без затримок, щоб запобігти можливим катастрофам. Важливо, що такі системи повинні ефективно обробляти і аутентифікувати команди від користувачів, а також забезпечувати достовірність даних, що передаються.

4. Запропонована модель

Для вирішення проблем захисту SCADA-систем пропонується наступна модель виявлення вторгнень [7]. Вона використовує передові алгоритми глибокого навчання для підвищення ефективності виявлення та зменшення помилкових спрацьовувань. Основою цієї моделі є інтеграція згорткових нейронних мереж (CNN) та рекурентний блок зі шлюзом (GRU).

CNN включатиме чотири блоки згортки, а кожен блок матиме три рівні: рівень згортки, рівень нормалізації та рівень максимального об'єднання. Вихідний результат останнього рівня згорткового блоку подаватиметься на вхід до наступного блоку згортки. На вхід CNN подаватимуться дані одновимірного ряду з кількома часовими кроками.

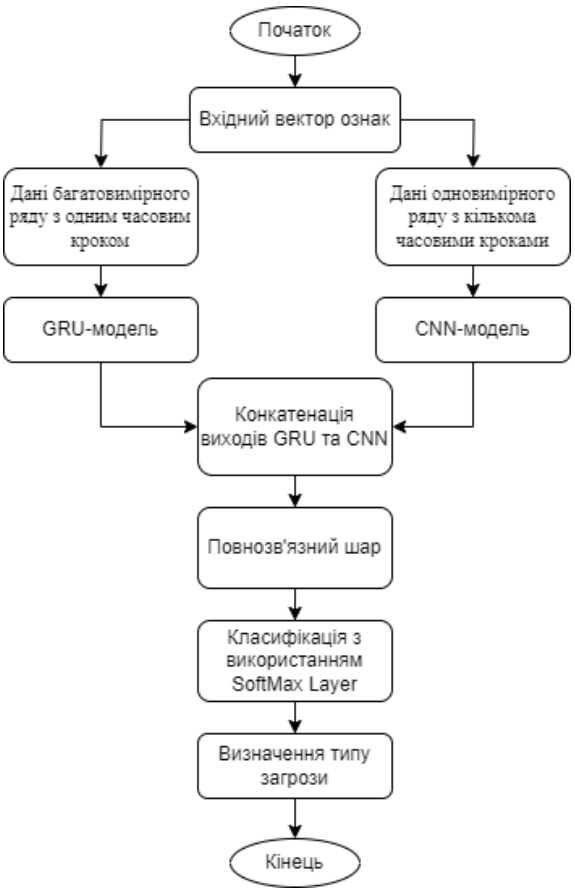

Рис. 1. Запропонована модель виявлення вторгень.

Що до GRU, то він представляєтиме собою шлюзи оновлення та скидання для обробки часових послідовностей даних. Перед модулем GRU винуватиметься процес перетасування розмірів. На вхід подаватимуться дані багатовимірного часового ряду з одним часовим кроком. Вихід першого шару передаватиметься на вхід для другого шару.

Кінцевий результат роботи обох моделей (CNN та GRU) об'єднуватимуться перед подачею на повністю зв'язаний шар, який виконуватиме класифікацію потенційних загроз. Далі виходи класифікуватимуться за допомогою шару SoftMax, який визначає ймовірність належності вхідних даних до певного класу атак.

Набір даних NSL-KDD. Для перевірки ефективності роботи запропонованої моделі виявлення вторгнень, буде використовуватися датасет NSL-KDD [8], що є вдосконаленою версією відомого набору даних KDD Cup 99. NSL-KDD містять записи про мережевий трафік, який реєструється простою системою виявлення вторгнень та містить 4 класи атак: Probe, DoS, R2L, U2R.

Оцінка ефективності. Щоб оцінити роботу IDS буде обчислено наступні показники точності класифікації атак:

- True positive (TP): кількість правильно ідентифікавоних зловмисних дій.
- True negative (TN): кількість дій, що були правильно розпізнані як такі, що не становлять загрози безпеці.
- False negative (FN): кількість шкідливих дій, що були помилково класифіковані як безпечі.
- False positive (FP) або False Alarm (FA): кількість безпечних дій, що помилково індентифікуються системою як шкідливі.

На основі зазначених показників можна визначити додаткові метрики, що відіграють ключову роль у оцінці ефективності IDS:

- Рівень помилкових позитивних результатів (FPR): вказує на частку безпечних дій, помилково класифікованих як шкідливі, відносно загальної кількості безпечних дій.

$$\text{FPR} = \frac{\text{FP}}{\text{FP} + \text{TN}}$$

- Рівень помилкових негативних результатів (FNR) показує, яка частка шкідливих дій не була виявлена системою, відносно загальної кількості шкідливих дій.

$$\text{FNR} = \frac{\text{FN}}{\text{TP} + \text{FN}}$$

- Частота виявлення (DR, також відома як True Positive Rate (TPR) або Recall): вимірює частку правильно ідентифікованих шкідливих дій від усіх справжніх загроз.

$$\text{DR} = \text{TPR} = \text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

- Рівень помилкових негативних результатів (TNR): вимірює частку правильно ідентифікованих безпечних дій, що не є загрозами, від загальної кількості безпечних дій.

$$\text{TNR} = \frac{\text{TN}}{\text{FP} + \text{TN}} = 1 - \text{FPR}.$$

- Загальна точність (Accuracy): визначає частку дій, які правильно класифіковано.

$$\text{Accurancy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}.$$

- Точність ідентифікації шкідливих дій (Precision): визначає частку правильно виявлених шкідливих дій від усіх дій, що система класифікувала як шкідливі.

$$\text{FPR} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

- F-міра є зваженим гармонійним середнім між Precision і Recall.

$$\text{F-measure} = \frac{2}{\left(\frac{1}{\text{Precision}}\right) + \left(\frac{1}{\text{Recall}}\right)}$$

Висновки

З огляду на низку вразливостей у сучасних системах диспетчерського контролю та збору даних, актуальною є розробка систем виявлення вторгнень для SCADA. Вирішення цієї проблеми дозволить підвищити рівень кіберрезильєнтності системи управління і, як наслідок, покращить виживаємість обєкта критичної інфраструктури в цілому. У даній роботі запропоновно модель системи виявлення вторгень на основі методів глибокого навчання: CNN та GRU. У подальшому запропонована IDS буде практично застосовано до набору даних NSL-KDD та проведено детальний аналіз ефективності її роботи.

Перелік використаних джерел

1. A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics / D. Pliatsios, P. Sarigiannidis, T. Lagkas, A. G. Sarigiannidis // IEEE Communications Surveys & Tutorials. — 2020. — Vol. 22, no. 3. — P. 1942–1976. — DOI: 10.1109/COMST.2020.2987688.
2. *Wired.* Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. — 03/2016. — URL: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (visited on 05/03/2024).
3. Cyber Resiliency Metrics and Scoring in Practice-Use Case Methodology and Examples / D. J. Bodeau, R. D. Graubart, R. McQuaid, J. Woodill. — 2019.
4. *Гальчинський Л., Личик В.* Метрики оцінки кібервідмовостійкості (аналітичне оглядове дослідження) // Інформаційні технології та суспільство. — 2023. — Т. 8, № 2. — С. 27—33.
5. *Alanazi M., Mahmood A., Chowdhury M. J. M.* SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues // Computers & Security. — 2023. — Vol. 125. — P. 103028. — ISSN 0167-4048. — DOI: 10.1016/j.cose.2022.103028.
6. Intrusion detection system: A comprehensive review / H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, K.-Y. Tung // Journal of Network and Computer Applications. — 2013. — Vol. 36, issue 1. — P. 16–24. — ISSN 1084-8045. — DOI: 10.1016/j.jnca.2012.09.004.
7. *Diaba S. Y., Shafie-khah M., Elmusrati M.* On the performance metrics for cyber-physical attack detection in smart grid // Soft Computing. — 2022. — Т. 26. — С. 13109—13118. — DOI: 10.1007/s00500-022-06761-1. — URL: https://doi.org/10.1007/s00500-022-06761-1.
8. *Anonymous.* A comparison of the NSL-KDD dataset and its predecessor the KDD Cup '99 dataset // International Journal of Scientific Research and Management (IJSRM). — 2022. — Т. 10, вип. 04. — С. 832—839. — DOI: 10.18535/ijsrm/v10i4.ec05. — URL: https://doi.org/10.18535/ijsrm/v10i4.ec05.