

ІДЕНТИФІКАЦІЯ ХАРАКТЕРИСТИК НЕПОМІТНОЇ АТАКИ НА АВТОМАТИЗОВАНІ СИСТЕМИ УПРАВЛІННЯ ОБ'ЄКТАМИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

В. М. Дудуладенко¹, М. І. Ільїн¹, О. М. Новіков¹, І. В. Стьопочкіна¹

¹ Навчально-науковий Фізико-технічний інститут

Анотація

Кількість кібератак на об'єкти критичної інфраструктури постійно збільшується. Так само зростає їх складність, організованість та здатність обходити традиційні засоби захисту, що породжує необхідність їх глибокого дослідження та вдосконалення існуючих методів виявлення.

В даній роботі розглянуто модель непомітної атаки (stealthy attack), що має на меті максимізувати вплив на систему керування. Досліджено основні характеристики такої атаки та запропоновано поетапний алгоритм для їх визначення.

Ключові слова: непомітна атака, кібербезпека, критична інфраструктура

Вступ

У сучасному світі об'єкти критичної інфраструктури (ОКІ) – це стратегічно важливі елементи економіки та безпеки держави, які включають енергетичні, транспортні, комунікаційні, фінансові, медичні та інші системи, від яких залежить нормальне функціонування суспільства. В умовах швидкого розвитку цифрових технологій та глобалізації зростають ризики для безпеки цих об'єктів, зокрема, через кіберзагрози. Реалізувати кіберзагрози можна через кібератаки на різні рівні системи автоматизації процесів об'єктів критичної інфраструктури. Наслідками таких атак можуть бути вихід з ладу обладнання, шкода навколишньому середовищу, втрата довіри до систем автоматизації і механізмів безпеки. Атаки спрямовані на програмовані логічні контролери (PLC) відносяться до нижнього рівня.

Деякі з найпоширеніших атак включають атаки типу відмова в обслуговуванні, метою яких є виведення з ладу PLC шляхом перевантаження його каналу зв'язку або процесора. Атаки повторного відтворення передбачають повторну відправку раніше перехоплених сигналів, щоб змусити PLC виконати несанкціоновані або шкідливі дії. Атаки введення неправдивих даних вводять в систему неправдиві дані, щоб ввести в оману операторів або автоматизовані алгоритми прийняття рішень. Інші пов'язані з цим загрози включають атаки нульової динаміки, які маніпулюють сигналами управління таким чином, щоб уникнути зміни видимих результатів роботи системи; приховані атаки, які залишаються прихованими від стандартних інструментів моніторингу; і непомітні атаки, які вносять незначні зміни, які не викликають тривоги або попередження в системах моніторингу [1, 2, 3, 4].

Непомітна атака (Stealthy attack) та її модель

Непомітна атака на автоматизовану систему керування – це тип кібератаки, спеціально розроблений для того, щоб залишатися непоміченим у середовищі операційних технологій об'єктів критичної інфраструктури. Метою атаки є непомітні маніпуляції, контроль або руйнація промислових процесів (наприклад, на електростанціях, системах водопостачання, нафтопереробних заводах або виробничих об'єктах) не викликаючи тривоги ні у фізичних системах, ні в їхньому програмному забезпеченні для моніторингу. Непомітні атаки в ІКС особливо небезпечні, оскільки вони зливаються зі звичайними операціями, що ускладнює їх виявлення за допомогою традиційних інструментів безпеки.

Під час непомітної атаки прихований вплив може невидимо змінювати дані датчиків, команди управління або задані значення. Таким чином непомітна атака може бути спрямована на сам об'єкт керування, на систему моніторингу та на систему керування об'єктом.

Розглянемо атаку спрямовану на систему керування об'єктом (рис. 1).

Одною з основних характеристик є поступове внесення змін, для того, щоб уникнути детектування. З однієї сторони ці зміни мають бути достатньо малими, щоб не спричинити їх виявлення, а з іншої такими, щоб суттєво порушувати роботу об'єкта керування.

Запишемо модель досліджуваної системи:

$$\begin{aligned}\frac{dx(t)}{dt} &= Ax(t) + Bu(t) \\ x(0) &= x_0 \\ y(t) &= Cx(t)\end{aligned}$$

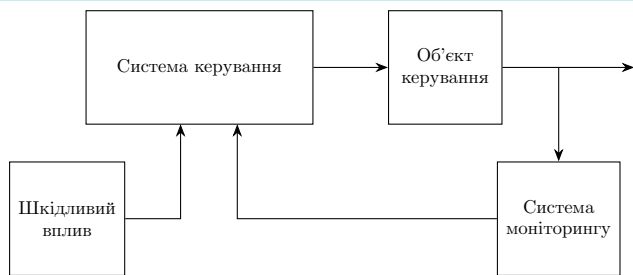


Рис. 1. Непомітна атака на систему керування об'єктом

Тоді функціонал якості (оптимальне керування) має наступний вигляд:

$$J = \int_0^k [x^T(t)Qx(t) + u^T(t)Ru(t)] dt$$

а граничні умови оптимального керування такі [5]:

$$u(t) = -K(t)x(t), K(t) = R^{-1}B^T P(t)$$

де матриця $P(t)$ є рішенням нелінійного рівняння Рікатті:

$$\frac{dP(t)}{dt} = -P(t)A - A^T P(t) + P(t)BR^{-1}B^T P(t) - Q$$

$$P(t_k) = P_k$$

Модель системи керування, яку атакували, матиме вигляд:

$$\tilde{u}(t) = u(t) + u_a(t), \quad u_a(t) \in \mathcal{U}_{\text{доп}}$$

Критерій детектора несправностей (WLS):

$$J[u_a] = \int_0^k (C\tilde{x}(t) - y(t))^T S (C\tilde{x}(t) - y(t)) dt$$

Система під атакою:

$$\frac{d\tilde{x}(t)}{dt} = A\tilde{x}(t) + B(-K(t)\tilde{x}(t) + u_a(t))$$

$$\tilde{x}(0) = x_0$$

Спряжене рівняння Лагранжа:

$$\frac{d\lambda(t)}{dt} = -(A - BK(t))^T \lambda(t) - 2C^T S (C\tilde{x}(t) - y(t))$$

$$\lambda(t_k) = 0$$

Гradientна процедура [6, 7, 8]:

$$u_a^{i+1}(t) = \text{Pr} \left\{ u_a^i(t) - \alpha \frac{dL}{du_a} \right\}$$

Знаходження параметрів непомітної атаки, з максимізацією впливу на систему керування

У класичних підходах атака моделюється як гра між атакуючим і захисником, де атакуючий обмежений умовою детектованості. Проте такі постановки

потребують складних процедур оптимізації (ККТ, варіаційна нерівність). М'який підхід дозволяє спростити задачу, інтегруючи обмеження в цільову функцію через штраф за виявлення, що дозволяє застосовувати класичні оптимізаційні методи (градієнтні, варіаційні). Таким чином, завдання зводиться до пошуку непомітного керування з м'яким обмеженням виявлення.

Отже, атакуючий максимізує відхилення стану системи:

$$\Phi(u_a) = \int_{t_0}^{t_k} \|\tilde{x}(t)\|^2 dt$$

де $\tilde{x}(t)$ – відхилення стану об'єкта під дією шкідливого керування $u_a(t)$, та мінімізує детектованість (використовується функціонал типу WLS):

$$J(u_a) = \int_{t_0}^{t_k} (C\tilde{x}(t) - y(t))^T S^{-1} (C\tilde{x}(t) - y(t)) dt$$

де S – матриця ваг, яка характеризує чутливість детектора несправностей, $y(t)$ – еталонні вимірювання без атаки.

Замість жорсткого обмеження $J(u_a) \leq \delta$ вводимо згладжений функціонал:

$$\mathcal{L}(u_a) = \Phi(u_a) - \beta \cdot J(u_a)$$

де Φ – ціль атаки (максимум впливу), J – міра детектованості, $\beta > 0$ – коефіцієнт штрафу за виявлення (параметр, що визначає баланс між агресивністю та непомітністю атаки). Якщо β велике – атака буде дуже прихована, але ефект слабкий. Якщо ж β мале – зростає ризик детекції [9, 5].

Для розв'язання задачі потрібно:

1. Провести ініціалізацію

- Задати початкове шкідливе керування $u_a^{(0)}(t)$
- Вибрати крок градієнтного методу α , параметр штрафу β

2. Здійснити чисельне інтегрування моделі

- Обчислити $\tilde{x}^{(i)}(t)$ за поточним $u_a^{(i)}(t)$

3. Обчислити градієнт $\frac{d\mathcal{L}}{du_a}$

- Сформулювати Лагранжіан:

$$\mathcal{L} = \int_{t_0}^{t_k} [\|\tilde{x}(t)\|^2 - \beta(C\tilde{x}(t) - y(t))^T S^{-1} (C\tilde{x}(t) - y(t))] dt$$

- Вивести спряжене рівняння для $\lambda(t)$
- Знайти градієнт:

$$\frac{d\mathcal{L}}{du_a} = \int_{t_0}^{t_k} K^T(t)\lambda(t) dt$$

4. Оновити шкідливе керування

$$u_a^{(i+1)}(t) = u_a^{(i)}(t) + \alpha \cdot \frac{d\mathcal{L}}{du_a}$$

5. Перевірити умови зупинки

- виконується

$$|\mathcal{L}^{(i+1)} - \mathcal{L}^{(i)}| \leq \epsilon$$

- або досягнута максимальна кількість ітерацій.

Використаний вище підхід є універсальним, так як дозволяє атакуючому самостійно налаштувати рівень непомітності через параметр β , без жорстких обмежень. Його можна адаптувати за допомогою машинного навчання, наприклад, навчаючи нейронну мережу формувати $u_a(t)$, щоб максимізувати $\mathcal{L}(u_a)$.

Висновки

У ході дослідження було розглянуто модель непомітної атаки (stealthy attack), яка становить серйозну загрозу для систем керування об'єктами критичної інфраструктури через свою здатність залишатися невиявленою, водночас завдаючи суттєвого впливу на функціонування системи. Аналіз характеристик такої атаки дозволив глибше зрозуміти механізми її реалізації та впливу. Запропонований поетапний алгоритм визначення параметрів атаки може стати основою для розробки ефективніших методів виявлення та нейтралізації подібних загроз. Отримані результати підкреслюють важливість подальших досліджень у напрямку зміцнення кіберзахисту систем автоматизованого управління.

Перелік використаних джерел

1. Bibliographical review on cyber attacks from a control oriented perspective / H. Sánchez [et al.] // *Annual Reviews in Control*. — 2019. — Vol. 48. — P. 103–128. — DOI: [10.1016/j.arcontrol.2019.08.002](https://doi.org/10.1016/j.arcontrol.2019.08.002).
2. Cyber-physical systems in industrial process control / Y. Wang [et al.] // *ACM Sigbed Review*. — 2008. — Vol. 5, no. 1. — P. 1–2. — DOI: [10.1145/1366283.1366295](https://doi.org/10.1145/1366283.1366295).
3. Detecting stealthy attacks against industrial control systems based on residual skewness analysis / Y. Hu [et al.] // *EURASIP Journal on Wireless Communications and Networking*. — 2019. — No. 74. — P. 1–14. — DOI: [10.1186/s13638-019-1389-1](https://doi.org/10.1186/s13638-019-1389-1).
4. Mo Y., Sinopoli B. Secure Control Against Replay Attacks // *47th Annual Allerton Conference on Communication, Control, and Computing*. — 2009. — P. 911–918. — DOI: [10.1109/Allerton16076.2009](https://doi.org/10.1109/Allerton16076.2009).
5. Sage A., White C. I. *Optimum Systems Control*. — New Jersey : Prentice-Hall, 1977. — URL: <http://www.semanticscholar.org/paper/Optimum-systems-control%3A-by-A.-P.-Sage-and-C.-C.-Eslami/83d44a3e6cd41f834a99209a671a248dfef12634>.
6. Визначення параметрів непомітних кібератак на системи керування об'єктів критичної інфраструктури / О. Новіков, І. Стьопчкіна, М. Льїн, М. Овчарук // *Наукові вісті КНУ*. — 2024. — № 1. — С. 69–75. — DOI: [10.20535/kpissn.2025.1.322905](https://doi.org/10.20535/kpissn.2025.1.322905).
7. Cyber Security Logical and Probabilistic Model of a Critical Infrastructure Facility in the Electric Energy Industry / L. Alekseichuk [et al.] // *Theoretical and Applied Cybersecurity*. — 2023. — Vol. 5, no. 1. — P. 61–66. — DOI: [10.20535/tacs.2664-29132023.1.287365](https://doi.org/10.20535/tacs.2664-29132023.1.287365).
8. Cyber Attacks Simulation for Modern Energy Facilities / O. Novikov [et al.] // *CEUR Workshop Proceedings. Selected Papers of the XXIII International Scientific and Practical Conference "Information Technologies and Security"*. Vol. 3887. — 2023. — P. 35–49. — URL: <https://ceur-ws.org/Vol-3887/>.
9. Optimal Control Theory: An Introduction / D. Kirk [et al.]. — Mineola, New York : Dover Publications, Inc., 2004. — URL: <https://books.google.com.ua/books?id=fCh2SAtWIdwC>.