УДК 004.056
DOI: 10.31673/2409-7292.2021.021516

Самандрула В.В., Луценко М.М.

ЗАСТОСУВАННЯ МЕТОДІВ ВНУТРІШНІХ ТОЧОК В ЗАДАЧАХ КІБЕРБЕЗПЕКИ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ЕНЕРГЕТИКИ

В роботі розглянуто підходи до створення інтелектуальних систем енергетики, які базуються на системах моніторингу режимів WAMS, з використанням інформаційних технологій в метрології, в засобах прийому, обробки та передачі інформації та визначенні параметрів в задачах керування. В роботі проведено аналіз існуючих кібератак на систему SCADA та WAMS та розглянуті можливі шляхи розв'язування задач керування в умовах порушення інформаційної безпеки інтелектуальних систем енергетики. Більш детально розглянуто DoS-атаки, які приводять до відмови приладів, які здійснюють вимірювання струмів, напруг та потужностей, а також до порушення роботи засобів обробки інформації. В роботі запропоновано алгоритм оцінювання стану кіберзахисту інтелектуальної системи енергетики на основі математичного моделювання внутрішніх станів системи, яке дає можливість отримувати необхідну точність розрахунків в умовах не повної інформації, причиною чого є неможливість доступу до даних вимірювання.

Ключові слова: Кібератаки, повнота, внутрішні точки, доступність, цілісність.

Вступ

В останній час спостерігається велика кількість аварій в електромережах для українських споживачів. Середня тривалість планових відключень для споживачів за 2020 рік в Україні становила приблизно 8 годин. Це втричі більше, ніж в Євросоюзі. А середня тривалість позапланових відключень в Україні становила приблизно 11 годин 20 хвилин, що в 7 разів більше, ніж в країнах Євросоюзу. Було досліджено, що технологічні втрати електроенергії на її передачу та розподіл в електромережах України становить приблизно 12% від загального відпуску, що в півтора рази перевищує середньоєвропейський рівень та більше ніж вдвічі за рівень втрат у розвинутих країнах [2]. Щоб уникнути описані негативні явища в електроенергетиці, необхідно створювати новий клас електромереж. Таким новим класом є так звані «розумні мережі» які отримали назву Smart Grid. Для надійного функціонування розумних мереж, задачі, пов'язані з керуванням даними процесами інтеграції повинні розв'язуватись з урахуванням кіберзагроз, які впливають на якість режимів інформатизації.

Постановка проблеми

Для оперативного керування розумними мережами необхідно використовувати параметри поточного режиму, які визначаються за рахунок їх вимірювання. Значення цих параметрів отримуються від систем SCADA та WAMS (Wide Area Measurement Systems). При успішній реалізації кібератак на системи SCADA та WAMS може відбутись знищення даних, які отримуються від засобів вимірювання. При цьому, результати вимірювання можуть мати похибки, які неможливо виявити існуючими підходами та методами, які здійснюють оцінку станів. Отже, задача виявлення тих станів розумних мереж, які характеризують їх уразливість є актуальною задачею сьогодення.

Аналіз публікацій

В роботі [1] розглянуто гібридні системи електротеплозабезпечення. Зауважено, що керування інтелектуальними електромережами за наявності гібридних систем електротеплопостачання суттєво ускладнюється. Однак, при викладенні матеріалу не враховуються вразливості від кібератак таких інтелектуальних систем, а лише пояснюється необхідність децентралізованого керування. В роботі [2] запропоновано математичну модель оцінки станів на основі методу внутрішніх точок Проведено аналіз кібератак на системи SCADA та WAMS. Однак, алгоритм, який запропоновано не дає повної картини щодо успішної реалізації кібератак, особливо Dos – атак. В роботі [3] для запобігання успішній реалізації кібератак запропоновано принцип децентралізації. До аналізу та захищеності інтелектуальних систем запропоновано системний підхід, який полягає в постійній підтримці цілісності системи розумні мережі, в підтримці їх швидкості і ефективності системи. Атаки реалізація яких направлені на пошук вразливостей у практичній реалізації криптосистеми

віднесені до атак аналітичного типу. В роботі [4] розроблено предикатну модель процесних знань про об'єкти, що спостерігаються в багатоканальних інтелектуальних системах моніторингу. Приведені основні особливості та структурні елементи цих моделей процесних знань. Недоліком даного підходу є те, що дані моделі не враховують випадковість. В роботі [5] узагальнено та проаналізовано загрози для користувачів інтернет – банкінгу, які пов'язані з використанням телекомунікаційних мереж та засобів зв'язку. Недоліком є те, що було застосовано метод експертних оцінок для підвищення рівня захисту користувачів інтернет – банкінгу від загроз, які пов'язані з використанням телекомунікаційних мереж та засобів зв'язку.

Мета статті

Метою даної статті є розробка математичного апарату, який дає можливість отримати точні оцінки параметрів режиму роботи розумних мереж, які визначають як нормальні режими, так і критичні, які виникають в результаті успішної реалізації кібератак.

Викладення основного матеріалу

Для дослідження кіберзахисту «розумних мереж», які ще мають назву інтелектуальні енергетичні системи (IEC) слід розділити дану систему на дві складові: керуюча складова та керована складова. ***Керуюча складова*** уявляє собою інформаційно-комунікаційну систему, яка виконує запрограмовані команди та команди, які задає оператор. До даних складових відносяться системи SCADA та WAMS. ***Керована складова*** – це технологічний процес, який забезпечує енергопостачання. Даними складовими є електричні станції та підстанції, мережі які розподіляють та передають електроенергію. На рисунку 1 представлено ієрархічну структуру керування «розумними мережами».

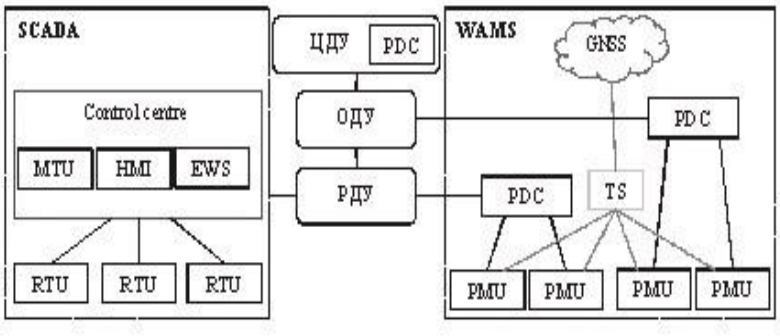

Рис. 1. Ієрархічна структура керування «розумними мережами».

Система SCADA здійснює підтримку роботи диспетчерів в процесі оперативного та анти аварійного керування IEC. Ця система складається з:

1. RTU (remote terminal unit) – віддалені засоби телемеханіки, які сканують телесигнал для отримання інформації про стан комутаційного обладнання та каналів зв'язку та здійснюють телевізійне вимірювання параметрів режиму.
2. MTU (master terminal unit) – диспетчерський пункт керування, який забезпечує інтерфейс між оператором HMI (human machine interface) та системою EWS (engineering work station).

Система моніторингу перехідних режимів Wams уявляє собою об'єднання реєстраторів синхронних направлених вимірювань (PMU), концентраторів направлених даних (PDC) на всіх рівнях керування з боку диспетчерів, каналів передачі інформативних сигналів між реєстраторами, концентраторами та диспетчерськими центрами, включаючи засоби обробки отриманої інформації.

В роботах [6-7] було проаналізована можливі кібератаки на системи SCADA та WAMS, основними з яких є наступні:

1. ***Розвідувальні атаки*** – атаки, направлені на виявлення вразливих місць в даних системах та визначення цілей, на які будуть в подальшому визначатись вид атак. В першу

чергу – це визначення IP – адресів PMU, RTU, PDC, MTU. Володіння даною інформацією дає можливість здійснювати атаки, які забезпечують введення хибних даних та атаки, які забезпечують відмову в обслуговуванні. При цьому в системах передачі даних можливо сканувати мережу, протоколи передачі даних та здійснювати аналіз мережевого трафіку.

2. ***Атаки, направлені на введення хибних даних***- метою цих атак є порушення цілісності, доступності та достовірності даних, що в свою чергу порушує роботу системи. Реалізація цих атак здійснюється за рахунок введення хибних даних, які є результатом вимірювання або результатом введення команд. Об'єктами реалізації таких атак є RTU, PMU, та PDC, який є приймачем синхронізованих даних від декількох PMU, та формує єдиний потік виводів. Метою даних атак є маніпулювання великою кількістю синхронізованих даних [8–9].

3. ***Dos-атаки*** – метою даних атак є неможливість отримати доступ до даних в наслідок чого виникає відмова в обслуговувані. Це призводить до зупинці передачі вимірювань від PMU або RTU в центри, які здійснюють керування. Також виникає загроза неможливості здійснювати спостерігання системи. Існують три види DOS-атак на вимірювальні пристрої, а саме:

- витрати трафіка (таблиця 1).
-

Таблиця 1.

Витрати трафіка

<table>
<tr><td>Приєднання до мережі</td><td>Аналіз портів</td><td>Використання власних портів</td><td rowspan="5">Витрати трафіка</td></tr>
<tr><td rowspan="3">Аналіз трафіка</td><td>Знання структурних пакетів даних</td><td>Заповнення мережі</td></tr>
<tr><td colspan="2">Безпечний міжмережевий захист</td></tr>
<tr><td colspan="2">Знаходження уразливостей в протоколах</td></tr>
<tr><td colspan="3">Заповнення мережі випадковими даними</td></tr>
</table>

- не достатня кількість ресурсів, або їх надмірна кількість (Таблиця 2).

Таблиця 2.

Недостатня кількість ресурсів

<table>
<tr><td>Знання операційної системи</td><td colspan="2">Намір пошкодження операційної системи</td><td rowspan="2">Не достатня кількість ресурсів</td></tr>
<tr><td>Отримання доступу до мережі</td><td>Аналіз трафіка</td><td>Синхронна атака</td></tr>
</table>

- помилки роботи програмного забезпечення (таблиця 3).

Таблиця 3.

Помилка роботи програмного забезпечення.

Приєднання до мережі	Неможливість виявлення атаки системою захисту	Модифікація знань ключів	Помилка роботи програмного забезпечення

Наслідки DOS-атак призводять до затримки надходження інформативних сигналів від вимірювальних приладів, знищення даних або RTU(PMU) можуть не відповідати на запити MTU(PDC). Для запобігання неможливості успішної реалізації Dos-атак на системи керування здійснюють шифрування даних, обмежують доступ до мережі за допомогою міжмережевих екранів, здійснюється захист операційної системи, тощо.

4. ***Атаки повторного відтворення*** – метою цих атак є перехоплення та запис потоків даних для дублювання ретрансляції та маніпуляції ними, а також направлені для введення хибних сигналів, які здійснюють керування системою. Успішна реалізація таких атак призводить до аварійних ситуацій в технологічній складовій.

5. ***Атаки, пов'язані зі створенням перешкод*** – направлені на зашумлення каналів передачі інформативних сигналів за рахунок сигналів перешкод. Метою даних атак є порушення зв'язку зі складовими SCADA та WAMS.

Для виявлення атак на ІЕС в першу чергу необхідно здійснювати оцінку стану електроенергетичної системи. Задача оцінки стану полягає в визначенні розрахункових значень напруг, струмів, потужностей, та порівняння їх з робочими, при яких ІЕС функціонує в нормальному режимі, при якому відсутні аварійні стани та своєчасно відбувається передача, отримання та обробка інформативних сигналів.

Нехай I_i, U_i - струм і напруга в i - му вузлі електромережі, при значенні яких забезпечується нормальний режим роботи всієї системи; I_{ij} - струм в мережі, яка з'єднує i та j вузли, значення якого забезпечує нормальний режим роботи всієї системи; P_i, Q_i - активна та реактивна потужності в i - му вузлі електромережі, значення яких забезпечує нормальний режим роботи всієї системи.

Відповідна енергетична система визначається деяким рівнянням

$$W(I_i, U_i, I_{ij}, P_i, Q_i) = 0. \tag{1}$$

В загальному випадку рівняння (1) нелінійне. Однак завжди існує можливість перетворити це рівняння в систему лінійних рівнянь

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \end{pmatrix} \begin{pmatrix} I_i \\ U_i \\ I_{ij} \\ P_i \\ Q_i \end{pmatrix} = \begin{pmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \\ \eta_4 \\ \eta_5 \end{pmatrix}. \tag{2}$$

Права частина рівності (2) визначає помилку лінеарізації, причому кожний елемент цього вектора-стовпчика відмінний від 0.

При розв'язуванні задачі оцінки стану системи необхідно враховувати наступні обмеження, а саме діапазон параметрів, які вимірюються, при якому буде нормальне функціонування всієї системи:

$$I_{i\min} \le I_i \le I_{i\max},\ U_{i\min} \le U_i \le U_{i\max},\ I_{ij\min} \le I_{ij} \le I_{ij\max},\ P_{i\min} \le P_i \le P_{i\max},\ Q_{i\min} \le Q_i \le Q_{i\max}. \tag{3}$$

В якості критерія для оцінки стану системи мінімізується вираз

$$J = \sigma_{I_i}^2 \left(\overline{I_i} - I_i\right)^2 + \sigma_{U_i}^2 \left(\overline{U_i} - U_i\right)^2 + \sigma_{I_{ij}}^2 \left(\overline{I_{ij}} - I_{ij}\right)^2 + \sigma_{P_i}^2 \left(\overline{P_i} - P_i\right)^2 + \sigma_{Q_i}^2 \left(\overline{Q_i} - Q_i\right)^2, \tag{4}$$

де $\sigma_{I_i}^2$, $\sigma_{U_i}^2$, $\sigma_{I_{ij}}^2$, $\sigma_{P_i}^2$, $\sigma_{Q_i}^2$ - дисперсії результатів вимірювання струму в i-му вузлі, напруги в i-му вузлі, струму в мережі, яка з'єднує i-й вузол з i-м, активної потужності в i-му вузлі та реактивної потужності в i-му вузлі відповідно.

$\overline{I_i}$, $\overline{U_i}$, $\overline{I_{ij}}$, $\overline{P_i}$, $\overline{Q_i}$ - середні допустимі значення відповідних параметрів вимірювання. Варто відмітити, що визначення обмежень (3), (4) дає можливість визначати помилки в вимірюваннях параметрів, а граничні значення активних та реактивних потужностей дають можливість отримувати достовірну інформацію про технологічні можливості устаткування, що в свою чергу підвищує якість оцінок параметрів, які визначають фізичний стан

енергетичної системи. Ця інформація важлива при наявності кіберзагроз, так як при успішній реалізації їх значення цих параметрів виходять за межі допустимих, а іноді і до неможливості їх визначення.

Метод внутрішніх точок оцінки стану системи полягає в мінімізації виразу (3) при обмеженнях (1), (2). Алгоритм складається з двох кроків:

Крок 1. Визначення області допустимих розв'язків рівняння (1).

Крок 2. Здійснюється оптимізація в області допустимих розв'язків наступним чином

$$\begin{aligned}
I_i^{(k+1)} &= (1+h_{I_i}^{(k)})I_i^{(k)} - h_{I_i}^{(k)}\overline{I_i},\ h_{I_i}^{(k)} \text{ - значення кроку,}\\
U_i^{(k+1)} &= (1+h_{U_i}^{(k)})U_i^{(k)} - h_{U_i}^{(k)}\overline{U_i},\ h_{I_i}^{(k)} \text{ - значення кроку,}\\
I_{ij}^{(k+1)} &= (1+h_{I_{ij}}^{(k)})I_{ij}^{(k)} - h_{I_{ij}}^{(k)}\overline{I_{ij}},\ h_{I_{ij}}^{(k)} \text{ - значення кроку,}\\
P_i^{(k+1)} &= (1+h_{P_i}^{(k)})P_i^{(k)} - h_{P_i}^{(k)}\overline{P_i},\ h_{P_i}^{(k)} \text{ - значення кроку,}\\
Q_i^{(k+1)} &= (1+h_{Q_i}^{(k)})Q_i^{(k)} - h_{Q_i}^{(k)}\overline{Q_i},\ h_{Q_i}^{(k)} \text{ - значення кроку.}
\end{aligned} \tag{5}$$

Значення кроку може приймати як додатнє так і від'ємне значення. Знак кроку визначається наступним чином

$$\begin{aligned}
L^{(k+1)} = &\frac{\left(I_i^{(k+1)} - \overline{I_i}\right)^2}{\left(\min\left\{I_{i\max} - I_i^{(k+1)}; I_i^{(k+1)} - I_{i\min}\right\}\right)^2} + \frac{\left(U_i^{(k+1)} - \overline{U_i}\right)^2}{\left(\min\left\{U_{i\max} - U_i^{(k+1)}; U_i^{(k+1)} - U_{i\min}\right\}\right)^2} +\\
&+\frac{\left(I_{ij}^{(k+1)} - \overline{I_{ij}}\right)^2}{\left(\min\left\{I_{ij\max} - I_{ij}^{(k+1)}; I_{ij}^{(k+1)} - I_{ij\min}\right\}\right)^2} + \frac{\left(P_i^{(k+1)} - \overline{P_i}\right)^2}{\left(\min\left\{P_{i\max} - P_i^{(k+1)}; P_i^{(k+1)} - P_{i\min}\right\}\right)^2} +\\
&+\frac{\left(Q_i^{(k+1)} - \overline{Q_i}\right)^2}{\left(\min\left\{Q_{i\max} - Q_i^{(k+1)}; Q_i^{(k+1)} - Q_{i\min}\right\}\right)^2} \to \min,
\end{aligned} \tag{6}$$

при наступних обмеженнях

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15}\\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25}\\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35}\\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45}\\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \end{pmatrix} \begin{pmatrix} I_i^{(k+1)} - I_i^{(k)}\\ U_i^{(k+1)} - U_i^{(k)}\\ I_{ij}^{(k+1)} - I_{ij}^{(k)}\\ P_i^{(k+1)} - P_i^{(k)}\\ Q_i^{(k+1)} - Q_i^{(k)} \end{pmatrix} - \begin{pmatrix} \eta_1\\ \eta_2\\ \eta_3\\ \eta_4\\ \eta_5 \end{pmatrix} = \begin{pmatrix} r_1^{(k)}\\ r_2^{(k)}\\ r_3^{(k)}\\ r_4^{(k)}\\ r_5^{(k)} \end{pmatrix}, \tag{7}$$

де права частина рівності (7) уявляє собою вектор напрямку вибору значення кроку при умові (6). Зупинка ітераційного процесу відбувається за умови

$$J < L^{(k+1)}. \tag{8}$$

В якості прикладу було взято схема IEC, яка складається з 14 вузлів (рисунок 2).

Припустимо, що в результаті Dos-атак на систему SCADA було порушено роботу RTUта виникли проблеми з вимірюванням параметрів P_2, Q_2. Згідно технологічним умовам режиму функціонування енергетичної системи ці значення цих параметрів повинно знаходитись в межах

$$0 \le P_2 \le 60(MBm),\ 0 \le Q_2 \le 60(MBap).$$

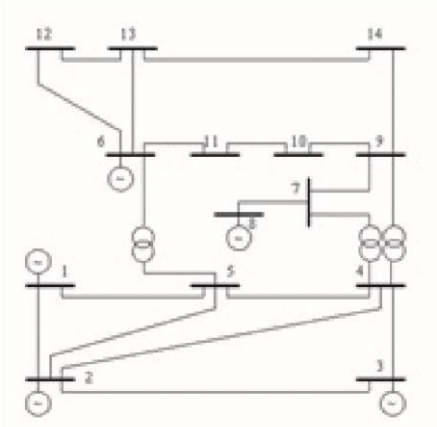

Рис. 2. Схема IEC, яка складається з 14 вузлів.

На значення напруг згідно (3) накладені обмеження

$$64.8 \le U_1 \le 79.9\,,\ 62.8 \le U_5 \le 69.9\,,\ 11.89 \le U_{10} \le 14.95.$$

Дані оцінки були отримані на основі розробленого алгоритму внутрішніх точок.

Висновок

В даній роботі було проведено аналіз існуючих кібератак на системи SCADA та WAMS. Так як інтенсивність Dos-атак на ці системи достатньо велика та їх успішна реалізація може порушити систему прийому, обробки та передачі даних, то більш детальний аналіз було проведено саме цим атакам. Запропоновано алгоритм для отримання оцінки керуючих параметрів, а саме струмів, напруг та потужностей на випадок неможливості їх виміряти при успішній реалізації кібератак. Результати розрахунків дали можливість стверджувати, що даний підхід є достатньо не складним і при цьому є достатньо ефективним.

Перелік посилань

1. Фіалко Н.М., Тимченко М.П., Халатов А.А., Шеренковський Ю.В. Інтелектуальні енергетичні системи теплозабезпечення будівель. Інститут технічної теплофізики НАН України – 2016. С. 203-209.

2. Колосюк И.Н., Гурина Л.А. Повышение кибербезопасности интеллектуальных энергетических систем методами оценивания состояния. // Вопросы кибербезопасности, №3(27) – 2018. С. 63-69.

3. Горбенко Ю.І., Єсіна М.В., Мялковський Д.В., Акользіна О.С., Пономарь В.А. Сучасні проблеми централізованих технологій типу «Клієнт-сервер» та можливості їх удосконалення на основі децентралізації. Радіотехніка. 2019. Вип. 198. С. 131-145.

4. Жирнов В.В., Солонская С.В. Предикатная модель процессных знаний о наблюдаемых объектах в многоканальных интеллектуальных системах мониторинга. Радіотехніка, 2019. Вип. 199. С. 67-74.

5. Антипов И.Е., Бочаров Б.В., Найдёнова Д.Р. Оценка безопасности пользователей интернет-банкинга. Радіотехніка. 2020. Вип. 200. С. 188-194.

6. Yao Liu, Peng Ning, Michael K. Reiter. False Data Injection Attacks against State Estimation in Electric Power Grids // CCS'09 Proceedings (9-13 November 2009, Chicago, Illinois, USA). Pp. 21-32.

7. Kebina Manandhar, Xiaojun Cao, Yao Liu. Detection of Faults and Attacks Including False Data Injection Attacks in Smart Grid Using Kalman Filter // IEEE Transactions of Control of Network Systems. Vol. 1, No 4, December 2014. Pp. 370-379.

8. Liang Heng, Jonathan J. Makela, Alejandro D. Dom´ınguez-Garc´ıa, Rakesh B. Bobba, William H. Sanders, and Grace Xingxin Gao. Reliable GPS-Based Timing for Power Systems: A Multi-Layered Multi-Receiver Architecture // 2014 Power and Energy Conference at Illinois (PECI) Proceedings. Pp. 1-7.

9. Mohd Rihan, Mukhtar Ahmad, M. Salim Beg. Vulnerability Analysis of Wide Area Measurement System in the Smart Grid // Smart Grid and Renewable Energy [Online] (Sep. 2013). Pp. 1-7. Available: http://www.scirp.org/journal/sigre.

Надійшла: 18.04.2021 Рецензент: д.т.н., професор Кожухівський А.Д.