УДК 04.056

ВИКОРИСТАННЯ PMU ДЛЯ ВИЯВЛЕННЯ АТАКИ НА ЕНЕРГЕТИЧНУ ІНФРАСТРУКТУРУ

Р. Ю. Слєпий[1,a], Л. Ю. Гальчинський [1]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

Робота присвячена методу виявлення атаки на енергетичну інфраструктуру, що спирається на використання PMU(Phasor Measurement Unit). У цій роботі описані основні принципи роботи PSS (Power System Stabilizer) та типи атак, що його стосуються. Результати проведеного аналізу можливо застосувати для програмної або апаратної реалізації аналізу стану енергосистеми, підвищення її стійкості до кібератак, а також прискорення виявлення аномалій поведінки генератора.

Ключові слова: виявлення атак, PSS, PMU, Time-delay attack.

Вступ

Останніми роками інформаційні технології стрімко впроваджуються в усі сфери життя, зокрема в енергетику. Це веде до зростання використання апаратного та програмного забезпечення у виробництві електроенергії й, відповідно, розширює потенційну площу для кібератак. На тлі геополітичного протистояння кібератаки, спонсоровані державними структурами, стали звичним явищем. Починаючи з атаки на енергосистему України у 2015 році, російські угруповання систематично здійснюють кібератаки, спрямовані на дестабілізацію енергетичної інфраструктури. Раннє виявлення таких атак є ключовим для підвищення стійкості та запобігання негативному впливу на економіку і суспільство [1].

1. Постановка задачі

Мета роботи полягає у визначенні методу виявлення кібератак на PSS, здатного ефективно виявляти аномалії поведінки в системі на основі аналізу векторів атак на енергосистеми. Робоча гіпотеза про наявність такого методу грунтується на використанні крос-кореляції між двома незалежними PMU-сигналами з нормальним профілем, що дозволяє виявити спотворення викликані часозатримними атаками. Визначений метод окрім стійкості до кібератак допоможе підвищити час виявлення відхилень, що впливають на енергосистему і вироблення електроенергії.

2. Основні типи атак на PSS

2.1. Основні принципи роботи PSS (Power System Stabilizer)

Power System Stabilizer (PSS) – це пристрій, який використовується в енергетичних системах для підвищення стабільності електричної мережі.Він призначений для демпфування електромеханічних коливань синхронного генератора.

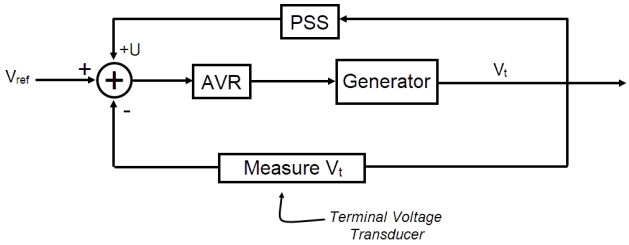

Рис. 1. Загальний вигляд взаємодії PSS і генератора.

За Кундуром, PSS слугує для підвищення динамічної стійкості системи шляхом додавання демпфувального електромагнітного моменту, синхронного з коливаннями ротора, та складається з набору структурних блоків: вхідного фільтра (washout), фазових коректораів (lead-lag), підсилювача (gain) і лімітерів.

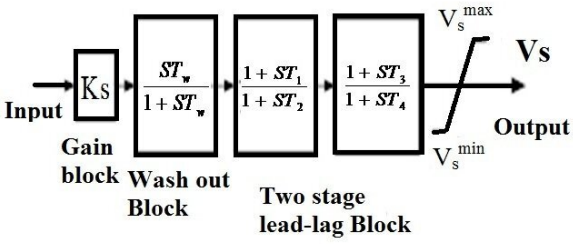

Рис. 2. Блоковий вигляд PSS.

Вхідний сигнал у PSS проходить через washout-фільтр (високочастотний фільтр першого порядку з часовою константою T_w), який пропускає лише коливальні компоненти та блокує сталі зсуви. Для компенсації фазового відставання між збудженням і моментом генератора застосовуються одна-дві секції

[a] romslye-ipt25@lll.kpi.ua

lead-lag компенсаторів (до $\sim 60^\circ$ кожна) у діапазоні 0.2–3 Гц. Часові константи (T_1, T_2, ...) добираються так, щоб забезпечити максимальне демпфування на частотах власних коливань системи. Після фазової компенсації сигнал підсилюється із загальним коефіцієнтом K, що визначає амплітуду демпфувального моменту, і проходить через обмежувач (limiter), який запобігає надмірним коливанням вихідної напруги збудження. Отриманий сигнал $Vstab$ подається на вхід AVR генератора, коригуючи напругу збудження саме в ті моменти, коли відхилення швидкості ротора спричиняють погасання коливань.

Якщо вхідний сигнал спотворений або затриманий, PSS може генерувати хибний стабілізуючий сигнал, або вводити сигнал в протифазі, що призводить до неефективного або навіть шкідливого впливу на стабільність системи. Як результат генератор енергосистеми може вийти з ладу або працювати не стабільно, що призведе до зниження ефективності генерації чи ризиків аварійної зупинки усієї електростанції [2, 3].

2.2. Основні види атак на PSS

Для здійснення впливу на PSS характерні нижче перераховані типи атак.

1. Bias Injection Attack.
   Атака з ін'єкцією зміщення полягає у впровадженні атакувальником постійного або синусоїдального збурення до вхідного сигналу PSS. Формально, сигнал, що надходить до стабілізатора, змінюється за формулою:
   $$\tilde{u}(t) = u(t) + d(t) \tag{1}$$
   де $u(t)$ – нормальний сигнал, а $d(t)$ – додаткове збурення (зміщення). У довгостроковій перспективі це призводить до того, що,через неправильну оцінку стану системи, PSS дає неадекватну компенсацію коливань, або ж може викликати перекомпенсацію. Це призводить до нестабільності енергосистеми. Малопомітна атака, яка може не викликати миттєвої аварії, але призводить до довгострокового погіршення стабільності системи [4, 5].
2. Time-delay attack. Атаки даного типу мають на меті порушити часову синхронізацію PMU, вносячи похибку в мітку часу або фазу вимірювань. Основним способом реалізації є зміна часової мітки так, що усі фази сигналів зсуваються на деяку величину Δt. Як приклад: якщо оригінальна фаза напруги чи струму у PMU дорівнює $\varphi(t)$, то після здійснення даної атаки вона стає
   $$\tilde{\varphi}(t) = \varphi(t - \Delta t) \tag{2}$$
   де Δt – стала затримка, введені атакуючим. Система із атакою затримки описується таким чином:
   $$\dot{x}(t) = Ax(t) + Bu(t + \tau) \tag{3}$$
   де τ – часова затримка [6]. Варто зазначити, що атака цього типу не змінює сигнал, та не виводить з ладу PSS методом Denial-of-Service, а передає реальний сигнал зі сталою затримкою в часі, або зсувом, що були підібрані атакуючим [5].
3. Delay Replay Attack. Атаки даного типу мають на меті ввести в оману стабілізатор введенням записаного раніше сигналу стабільної системи, під виглядом поточного. Для реалізації атакуючий спочатку повинен записати справжні вхідні сигнали u(τ) за час $\tau \in [t_0, t_1]$, а потім підмінити ними поточні вимірювання відтворюючи їх з деякою затримкою T.
   Таким чином оригінальний сигнал $u(\tau)$ замінюється на
   $$\tilde{u}(t) = u(t_0 + t - T). \tag{4}$$
   Отже у формулу керування потрапляє заздалегідь записане значення сигналу u, зсунуте на інтервал часу T. Це також дозволяє проводити атаку у стелс-режимі: до початку відтворення злоякісного сигналу монітор нічого не помітить. А у разі утворення будь-якої аномалії (осциляція наприклад) зміни не будуть відображені в сигналі. Як результат про вихід обладнання з ладу дізнаються після критичної зупинки, а не з попередніх змін поведінки [5].
4. False Data Injection Attack (FDIA). Атака введення шкідливих даних має на меті ввести шкідливу, але близьку до правдоподібної (легітимної) інформацію у PSS. Необхідність введення правдоподібних даних полягає у тому, щоб не викликати підозр з боку механізмів виявлення. Нехай z – вектор реальних вимірювань у системі, який пов'язаний зі станом системи x через рівняння:
   $$z = Hx + ez \tag{5}$$
   де H – матриця спостереження, що описує залежність між станом системи та вимірюваннями, а e – вектор похибок вимірювань. Атакувальник створює вектор фальшивих даних a і додає його до реальних вимірювань, отримуючи змінений вектор вимірювань z':
   $$z' = z + a = Hx + e + a \tag{6}$$
   Якщо вектор a сконструйований таким чином, що він належить до простору стовпців матриці H (тобто $a = Hc$, де c – довільний вектор),то спотворення залишиться непоміченим стандартними методами виявлення помилок,оскільки:
   $$z' = Hx + e + Hc = H(x + c) + e \tag{7}$$
   У цьому випадку змінений стан $x' = x + c$ призводить до тих самих залишків при оцінці стану, що й у випадку без атаки, ускладнюючи виявлення втручання. На противагу типам атак 2 і 3 , атака FDIA вносить абсолютно неправдивий сигнал від самого початку реалізації, але може бути виявлення із запізненням через наближення фальсифікованого сигналу до еталонного [4, 5].

3. Метод виявлення часозатримних атак на PSS, що базується на використанні PMU

Часозатримні атаки навмисно вводять затримку у сигнали, що надходять до або від PSS. Навіть невелика затримка в системі стабілізації частоти може викликати недемпфовані коливання або навіть втрату синхронізму генераторів, що в підсумку загрожує відключенням цілих енергоблоків чи навіть системними аваріями. Атаки такого типу належать до стелс-атак і прихованість робить їх небезпечними, а раннє виявлення – критично необхідним.

- Підготовчий етап.
  Для фазового кута напруги зі «здорового» PMU на терміналі генератора надають позначення $y'(t)$, а для фазового кута струму з іншого PMU на тому ж терміналі надають позначення $s(t)$. У даному випадку сигнал $s(t)$ відіграє роль «водяного знаку» [5].
- Накопичення кореляційних показників
  Протягом роботи системи обчислюється середньозважена (часозалежна) кореляція між $s(t)$ і $y'(t)$:
  $$\psi(t) = \frac{1}{t}, \quad t > 0 \tag{8}$$
  Цей показник відображає, наскільки «узгоджено» змінюються два незалежні сигнали у нормальному режимі [5].
- Оцінка самої швидкості змін.
  Для підвищення ефективності виявлення атак у роботі використовується швидкість залежної від часу крос-кореляційної функції.[5]Хоча швидкості обчислюються за допомогою диференціальних операцій, використання диференціатора сприйнятливе до шумів.Тому замість «грубої» похідної, яка надто чутлива до шуму, в реальному часі зміна обчислюється з використанням формули:
  $$\frac{d\psi(t)}{dt} = \frac{1}{t+\varepsilon}\left(s(t)y'(t) - \psi(t)\right) \tag{9}$$
  Де ε – мала додатна константа, що використовується для уникнення ділення на нуль [5].
- Сповіщення про атаку.
  Якщо за умов оцінки кореляції швидкість зміни кореляції виходить за дозволені межі змін значення, оператору надходить сигнал про можливе виникнення атаки або змін у системі, що можуть призвести до її виходу з ладу. Далі оператор має діяти згідно із заздалегідь визначеним алгоритмом для попередження аварійних ситуацій та відновлення стабільної роботи системи.

Висновки

У даному дослідженні було розглянуто основні принципи роботи PSS, основні типи атак на PSS/PMU, було проаналізовано метод виявлення Time-delay атак на ранніх етапах з використанням крос-кореляції зміни показників PMU на терміналах генераторів. Раннє виявлення Time-delay атак на енергетичну інфраструктуру є необхідним для підвищення її стабільності та відмовостійкості. Метою впровадження цього методу є спроба використати алгоритм виявлення часозатримних атак на PSS, що виводять з ладу систему генерації електроенергії. Використання отриманих даних можливе для впровадження програмного або вбудованого апаратного засобу для виявлення аномалій поведінки або кібератак на енергетичну інфраструктуру. Загалом метод виявлення атак і аномалій, пов'язаних із часовими затримками сигналу, на ранніх етапах сприяє розвитку стійких резильєнтних енергосистем.

Перелік використаних джерел

1. *CISA*. Cyber-Attack Against Ukrainian Critical Infrastructure. — 07/20/2021.
2. IEEE Recommended Practice for Excitation System Models for Power System Stability Studies // IEEE Std 421.5-2016 (Revision of IEEE Std 421.5-2005). — 2016. — С. 1—207. — DOI: 10.1109/IEEESTD.2016.7553421.
3. *Kundur P.*, *Balu N.*, *Lauby M.* Power System Stability and Control. — McGraw-Hill Education, 1994. — 1176 с. — (EPRI power system engineering series). — ISBN 9780070359581.
4. *Liu Y.*, *Ning P.*, *Reiter M. K.* False data injection attacks against state estimation in electric power grids // ACM Transactions on Information and System Security (TISSEC). — 2011. — Т. 14, № 1. — С. 1—33.
5. *Said A.*, *Matsuo T.* Assessment of Cyber Attacks against Power System Stabilizer and Their Detection Using Phasor Measurement Units // Journal of the Institute of Industrial Applications Engineers Vol. — 2024. — Т. 12, № 3. — С. 48—57. — DOI: 10.12792/JIIAE.12.48.
6. *Косарик Д. А.*, *Гальчинський Л. Ю.* Пом'якшення наслідків атаки на нижньому рівні управління, як елемент резильєнтності об'єктів критичної інфраструктури. // XXII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених теоретичні і прикладні проблеми фізики, математики та інформатики. — 2024. — Т. 22. — С. 265—268.