УДК 621.31 DOI:10.30724/1998-9903-2021-23-5-13-23

ИСПОЛЬЗОВАНИЕ МНОГОМОДЕЛЬНОЙ ПРОГНОЗНОЙ ОЦЕНКИ СОСТОЯНИЯ СИСТЕМ ЭЛЕКТРОСНАБЖЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ КИБЕР-АТАК

И.А. Лукичева, А.Л. Куликов

Нижегородский государственный технический университет им. Р.Е. Алексеева, г. Нижний Новгород, Россия
lukicheva.ir@gmail.com, inventor61@mail.ru

Резюме: *ЦЕЛЬ. Интеллектуальные электрические сети предполагают широкое использование информационной инфраструктуры. Такая совокупная киберфизическая система может подвергаться воздействию кибератак. Одним из способов противодействия кибератакам является оценка состояния, позволяющая уточнять показания установленных в сети измерителей параметров электрической сети, а также использовать избыточность измерений для фильтрации поврежденных данных. В частности, при подмене реального измерения фальшивым или сбое в функционировании каналов связи возможно обнаружение ложных данных и их восстановление. Однако существует класс кибератак с вводом неверных данных, направленный на искажение результатов оценки состояния. Целью исследования было разработать алгоритм оценки состояния, сохраняющий высокую точность в условиях кибер-атак. МЕТОДЫ. Авторами предлагается метод прогнозируемой оценки состояния, основанный на многомодельном дискретном следящем оценивании параметра фильтром Калмана. Многомодельная оценка определяется как взвешенная сумма одномодельных оценок, полученных с использованием различных переходных моделей. Обнаружение кибератаки реализуется с помощью инновационного анализа и анализа невязки измерения и оценки. Анализ работы предложенного алгоритма производился с помощью имитационного моделирования на примере 30-ти узловой схемы IEEE в программном комплексе MatLab. РЕЗУЛЬТАТЫ. В статье описана кибер-атака с вводом неверных данных и ее специфика воздействия на оценку состояния. Разработан алгоритм многомодельной прогнозируемой оценки состояния, позволяющий обнаруживать кибер-атаку и восстанавливать искаженные данные. Выполнено моделирование работы алгоритма и доказана его эффективность. ЗАКЛЮЧЕНИЕ. Результаты показали точность обнаружения кибератаки 100% в случае больших внесенных искажений параметров. Использование многомодельной прогнозируемой оценки состояния является эффективным методом защиты от воздействия кибер-атак на энергосистему.*

Ключевые слова: *авторегрессия; векторная авторегрессия; кибератака, оценка состояния; фильтрация Калмана; экспоненциальное сглаживание Хольта; электроэнергетическая система.*

Для цитирования: Лукичева И.А., Куликов А.Л. Использование многомодельной прогнозной оценки состояния систем электроснабжения для обнаружения кибер-атак // Известия высших учебных заведений. ПРОБЛЕМЫ ЭНЕРГЕТИКИ. 2021. Т. 23. № 5. С.13-23. doi:10.30724/1998-9903-2021-23-5-13-23.

THE USAGE OF POWER SYSTEM MULTI-MODEL FORECASTING AIDED STATE ESTIMATION FOR CYBER ATTACK DETECTION

IA. Lukicheva, AL. Kulikov

Nizhny Novgorod State Technical University R.E. Alekseeva, Nizhny Novgorod, Russia
lukicheva.ir@gmail.com, inventor61@mail.ru

Abstract: *THE PURPOSE. Smart electrical grids involve extensive use of information infrastructure. Such an aggregate cyber-physical system can be subject to cyber attacks. One of*

the ways to counter cyberattacks is state estimation. State Estimation is used to identify the present power system operating state and eliminating metering errors and corrupted data. In particular, when a real measurement is replaced by a false one by a malefactor or a failure in the functioning of communication channels occurs, it is possible to detect false data and restore them. However, there is a class of cyberattacks, so-called False Data Injection Attack, aimed at distorting the results of the state estimation. The aim of the research was to develop a state estimation algorithm, which is able to work in the presence of cyber-attack with high accuracy. METHODS. The authors propose a Multi-Model Forecasting-Aided State Estimation method based on multi-model discrete tracking parameter estimation by the Kalman filter. The multimodal state estimator consisted of three single state estimators, which produced single estimates using different forecasting models. In this paper only linear forecasting models were considered, such as autoregression model, vector autoregression model and Holt's exponential smoothing. When we obtained the multi-model estimate as the weighted sum of the single-model estimates. Cyberattack detection was implemented through innovative and residual analysis. The analysis of the proposed algorithm performance was carried out by simulation modeling using the example of a IEEE 30-bus system in Matlab. RESULTS. The paper describes an false data injection cyber attack and its specific impact on power system state estimation. A Multi-Model Forecasting-Aided State Estimation algorithm has been developed, which allows detecting cyber attacks and recovering corrupted data. Simulation of the algorithm has been carried out and its efficiency has been proved. CONCLUSION. The results showed the cyber attack detection rate of 100%. The Multi-Model Forecasting-Aided State Estimation is an protective measure against the impact of cyber attacks on power system.

***Keywords**: autoregression; cyberattack; electric power system; Holt exponential smoothing; Kalman filtering; state estimation; vector autoregression.*

For citation: Lukicheva IA, Kulikov AL. The usage of power system multi-model forecasting aided state estimation for cyber attack detection. *Power engineering: research, equipment, technology*. 2021; 23(5):13-23. doi:10.30724/1998-9903-2021-23-5-13-23.

Введение

Интеллектуальные электрические сети предполагают широкое использование информационной инфраструктуры. Такая совокупная киберфизическая система может подвергаться воздействию кибератак. Искажения данных от систем *SCADA* и СМПР, нарушение работы каналов связи, потеря измерений, вызванные кибератаками, могут привести к нарушениям и отказам функционирования ЭЭС. Поэтому важно сохранить достоверность и полноту информации информационно-коммуникационной и технологической систем под воздействием кибератак.

Встречаются следующие кибератаки с воздействием на функционирование энергосистемы: атаки внедрения ложных данных, переполнение буфера, *spoofing*, атаки повторного произведения, подделка устройства, *DOS*-атаки, атака «человек посередине», компрометация маршрутизаторов связи, а так же [1]. Одним из способов противодействия кибератакам является статистическая обработка измерительной информации, например, оценка состояния (ОС). ОС позволяет уточнять показания установленных в сети измерителей параметров электрической сети, а также использовать избыточность измерений для фильтрации поврежденных данных. В частности, при подмене реального измерения фальшивым или сбое в функционировании каналов связи возможно обнаружение искаженных данных и их восстановление. Специфичной кибератакой для энергосистемы атака внедрения ложных данных *(false data injection attack - FDIA*), которая позволяет снизить точность результатов оценки состояния, оставаясь незамеченным [2]. Искаженные данные могут привести к неправильным управляющим воздействиям, и, следовательно, к неэффективной работе ЭЭС и даже аварии.

В литературе представлены различные меры защиты от кибераттак. Бобба и другие в [3] предложили защищать определённый набор критически важных измерений вместо того, чтобы разрабатывать новые алгоритмы обнаружения кибервторжений. При альтернативном подходе авторами [4] после каждой операции оценки состояния вводится проверка полученных результатов на принадлежность к модели марковской цепи. Если оцененное значение не удовлетворяет требованиям принадлежности к марковской цепи, указывается большая вероятность присутствия кибератаки. Новая схема обнаружения была предложена в [5] с использованием графа марковской цепи для фазовых углов. В [6] метод Кульбака-Лейблера был использован для определения расстояния между

распределениями вероятностей, сформированных для наблюдаемых отклонений. Метод следящего оценивания на основе калмановской фильтрации был предложен в [7]. Следует отметить, что указанные выше подходы не используют возможность повышения вероятности обнаружения кибератаки за счет использования пространственного подхода в дополнение к временному. В [8] предлагается применение медианной фильтрации с использованием информации с соседних узлов. При этом для эффективности определения кибератак необходимо точное знание параметров электрической сети, что не всегда бывает возможным. Алгоритм, основанный на сопоставлении реальных и модельных данных, предложенный в [9] позволяет реализовать эффективную фиксацию факта кибератаки, однако требует предварительного расчет нормальных и аварийных режимов электрической сети с получением токов по ветвям для различных сценариев.

Авторами предлагается использование метода многомодельной прогнозируемой оценки состояния для обнаружения кибератак с помощью комбинации инновационного анализа и анализа невязки измерения и оценки. Отличиями предложенного метода по сравнению с существующими является большая точность оценки по сравнению с одномодельными методами оценки энергосистем, обладающими быстроизменяющимися динамичными режимами, одновременное использование пространственного и временного подходов для оценки параметров за счет использования нескольких одномодельных оценивателей параллельно, прогнозирование изменения параметра для проведения инновационного анализа и замены результата искаженной оценки до проверки на кибератаку на прогнозное значение оценки в случае наличия кибератаки, что делает процесс ОС непрерывным и предотвращает потерю наблюдаемости сети, а так же вычислительная простота.

Материалы и методы

Алгоритм внедрения ложных данных

Атака *внедрения ложных данных* (*FDIA*) направлена на искажение результатов ОС [2]. Основная идея такой атаки заключается в том, чтобы ввести ложные данные в массив измерений таким образом, чтобы невозможно было их определить с помощью традиционной процедуры обнаружения плохих данных (ОПД), и в следствии этого сделать результаты оценки состояния некорректными. Данный подход основывается на том, что большинство техник определения плохих данных базируется на предположении, что квадрат разницы между значениями измерений и соответствующих им оценок становится выше порогового значения в случае присутствия плохих данных в массиве измерений. Однако, существует возможность определить такой вектор ложных измерений, что это предположение будет неверным, и ложные измерения не будут обнаружены и использованы в оценке состояния.

Базовый принцип создания атаки с вводом неверных данных заключается в следующем. Пусть вектор оценки состояния содержит n переменных состояния $x_1, \ldots, x_n$ и m измерений $y_1, \ldots, y_m$. Взаимосвязь между состоянием и измерениями описывается матрицей H размерностью mxn в случае линейной оценки состояния

$$x = Hy\,. \tag{1}$$

Предположим, что y_a – вектор измерений, содержащий плохие данные, введенные злоумышленником:

$$y_a = y + a\,, \tag{2}$$

где $y = (y_1, ..., y_m)$ – первоначальный вектор измерений (до действий злоумышленника), $a = (a_1, ..., a_m)$ – вектор атаки, где $a_i = 0$, если i-ое измерение не атаковано.

Чтобы измерения с ошибкой y_a успешно прошли процедуру ОПД, должны выполнятся условия:

$$a = Hc\,, \tag{3}$$

$$\hat{x}_a = x + c\,, \tag{4}$$

где $c = [c_1, ..., c_m]$ – любой случайный вектор, $\hat{x}_a$ – вектор оценки состояния, полученный с использованием атакованных измерений y_a.

В статье рассматривается вариант случайной атаки *FDIA*, когда вектор c может принимать произвольные значения. Вектор атаки $a' = (a_1, ..., a_k)^{\mathrm{T}}$, состоящий из ненулевых элементов:

$$a' = (I - B'^{-}B)d\,, \tag{5}$$

где B – матрица размерностью mxm, I –единичная матрица, d –произвольный ненулевой вектор

$$B = H(H^{\mathrm{T}}H)^{-1}H^{\mathrm{T}} - I \,. \tag{6}$$

При выполнении условий (6)-(10) невязка между измеренными значениями параметров и оценкой состояния в случае будет равной невязке, если бы измерения не были изменены измерениями:

$$r_a = z_a - H\hat{x}_a = z + a - H(\hat{x} + c) = (z - H\hat{x}) + (a - Hc) = r \,. \tag{7}$$

Следовательно, процедура ОПД на основе значения невязки не позволяет определить наличие атаки *FDI* и атакованные измерения используются для ОС, внося ошибки в ее результаты.

Многомодельная прогнозируемая оценка состояния

Эффективной мерой защиты от кибератак является прогнозируемая оценка состояния (ПОС). ПОС является частным случаем динамической оценки состояния, получаемой в результате упрощения математической модели динамической системы [11]:

$$x_k = f(x_k, u_k, w_k, k) \,, \tag{8}$$

где k - номер отсчета, x - вектор состояния, u – управляющее воздействие, w – параметр, характеризующий точность модели, f – нелинейная функция. В ПОС принимаются допущения, что время дискретизации достаточно мало, так что нелинейную модель изменения параметра можно представить линейной, и погрешность модели описывается Гауссовским законом распределения с математическим ожиданием равным нулю, и постоянной ковариационной матрицей.

Принимая во внимание данные допущения, получаем линейную модель прогнозируемой оценки:

$$x_k = F_{k-1}x_{k-1} + G_{k-1} + w_{k-1}, \tag{9}$$

$$y_k = h(x_k) + v_k \tag{10}$$

где F_k - функция, описывающая переходную матрицу состояния, G_k - параметр отражающий тренд изменения состояния, w_k – ошибка прогнозирования, распределенная по Гауссовскому закону распределения с математическим ожиданием равным нулю, и ковариационной матрицей Q, $h(x_k)$ – функция взаимосвязи состояния x_k и измерения y_k

ПОС имеет несколько преимуществ перед СОС:

– В СОС используется один снимок измерений. Избыточность измерений имеет решающее значение, т.к. система должна быть наблюдаемой. Поэтому требуется более или менее централизованный подход для сбора всех измерений, охватывающих анализируемую область. Однако возможны потери или задержки связи, которые могут затруднить расчет состояния. В ПОС измерения различных узлов могут обрабатываться независимо, поэтому оценка состояния может выполняться децентрализованно.

– СОС чувствителен к неверным данным, а, следовательно, и кибератакам, которые имеют размытый эффект искажения на результаты оценки. ПОС использует информацию о предыдущих состояниях, что позволяет проводить инновационный анализ. Анализ инноваций может помочь обнаружить аномалии. Тогда ошибочные или потерянные измерения можно заменить прогнозом состояния.

– Результаты ПОС могут быть использованы в качестве псевдоизмерений для повышения наблюдаемости сети и избыточности измерений для увеличения точности СОС

– Комбинация инновационного анализа и анализа невязки измерений и оценки теста позволяет различать внезапные изменения в системе, неверные данные или кибератаки, ошибку конфигурации сети, ошибку сетевых параметров [12].

– ПОС позволяет нам наблюдать динамику состояния квазистатической энергосистемы, что очень важно в электрических сетях с стохастическим характером нагрузки и генерации.

– Прогнозирование оценок состояния позволяет предотвратить развитие аварийных событий, определить неверные данные и кибератаки, а также выявить внезапные изменения в системе, топологические ошибки и другие аномалии.

– Эти преимущества в сочетании с довольно точными и быстрыми методами прогнозирования и фильтрации делают ПОС важной процедурой в системе управления и мониторинга электрической сети.

Для решения задач ПОС на практике наибольшее распространение получил фильтр Калмана. Фильтр Калмана – рекурсивный фильтр, оценивающий вектор

состояния динамической системы с использованием ряда неполных и искаженных («зашумленных») измерений [13]. Задача калмановской фильтрации состоит в определении математического ожидания и дисперсии оцениваемого параметра x_k, изменяющегося по определенному закону, на основе измерений y_k.

Оценка производится в соответствии с уравнениями (11)-(15).

$$\tilde{x}_k = F_{k-1}\hat{x}_{k-1} + u_{k-1}, \tag{11}$$

$$\tilde{P}_k = F_{k-1}\hat{P}_{k-1}F_{k-1}^T + Q_{k-1}, \tag{12}$$

$$\hat{x}_k = \tilde{x}_k + K_k(y_k - H_k\tilde{x}_k), \tag{13}$$

$$P_k = \left(I - K_k H_k\right)\tilde{P}_k, \tag{14}$$

$$K_k = \tilde{P}_k H_k^T \left(H_k\tilde{P}_k H_k^T + R_k\right)^{-1}, \tag{15}$$

где $\tilde{x}_k$ - априорная оценки состояния, $\hat{x}_k$ – апостериорная оценка состояния, $\tilde{P}_k$ – ковариация априорной оценки состояния, $\hat{P}_k$ – ковариация апостериорной оценки состояния, K_k – коэффициент усиления Калмана.

Фильтр Калмана эффективен с учетом следующих допущений:

1. Ошибки оценки параметров и измерений распределены по нормальному закону с математическим ожиданием равным нулю;

2. Ковариации ошибок оценки параметров и измерений известны;

3. Известна точная математическая модель пересчета параметров от шага к шагу.

Авторами предлагается многомодельная прогнозируемая оценка состояния (ММПОС), позволяющая реализовать одновременно несколько процедур фильтрации Калмана (13)-(17) с использованием различных переходных моделей F_k, так как:

1. В реальности в электроэнергетических системах, для которых характерны быстроизменяющиеся динамичные режимы, например, в микросетях с возобновляемыми источниками энергии, вышеуказанные допущения не соблюдаются полностью. Из-за случайного поведения нагрузок и режимов возобновляемых источников энергии не существует единой универсальной модели перехода, с помощью которой можно было бы точно прогнозировать изменения оцениваемого параметра во времени. На разных временных отрезках различные переходные модели могут показывать лучшие результаты. Поэтому ММПОС имеет меньшую ошибку, чем одномодельная оценка.

2. Для обнаружения кибератаки эффективно использовать несколько оценок, чтобы избежать вероятности искажения результирующей оценки в случае выбора модели с чувствительностью к неверным данным.

Общее схематическое изображение алгоритма многомодельной оценки представлено на рисунке 1.

В данной работе анализировалась ММПОС на примере многомодельного оценивателя, состоящего из трех одномодельных фильтра Калмана с авторегрессионной переходной моделью первого порядка, векторной авторегрессионной моделью первого порядка и моделью экспоненциальное сглаживание Хольта.

1) Экспоненциальное сглаживание Хольта.

Прогнозное значение параметра определяется как сумма экспоненциально-сглаженного значения параметра a_k и тренда его изменения b_k

$$\tilde{x}_{k+1} = a_k + b_k. \tag{16}$$

Экспоненциально-сглаженное значение параметра и тренд так же оцениваются на каждом шаге:

$$a_k = \alpha\tilde{x}_k + (\alpha - 1)\tilde{x}_{k-1}, \tag{17}$$

$$b_k = \beta[a_k - a_{k-1}] + (1-\beta)b_{k-1}, \tag{18}$$

где α и β – сглаживающие коэффициенты, принимающие значения от 0 до 1.

Параметры сглаживания Холта были выбраны равными: $\alpha = 0,5$ и $\beta = 0,8$ [13].

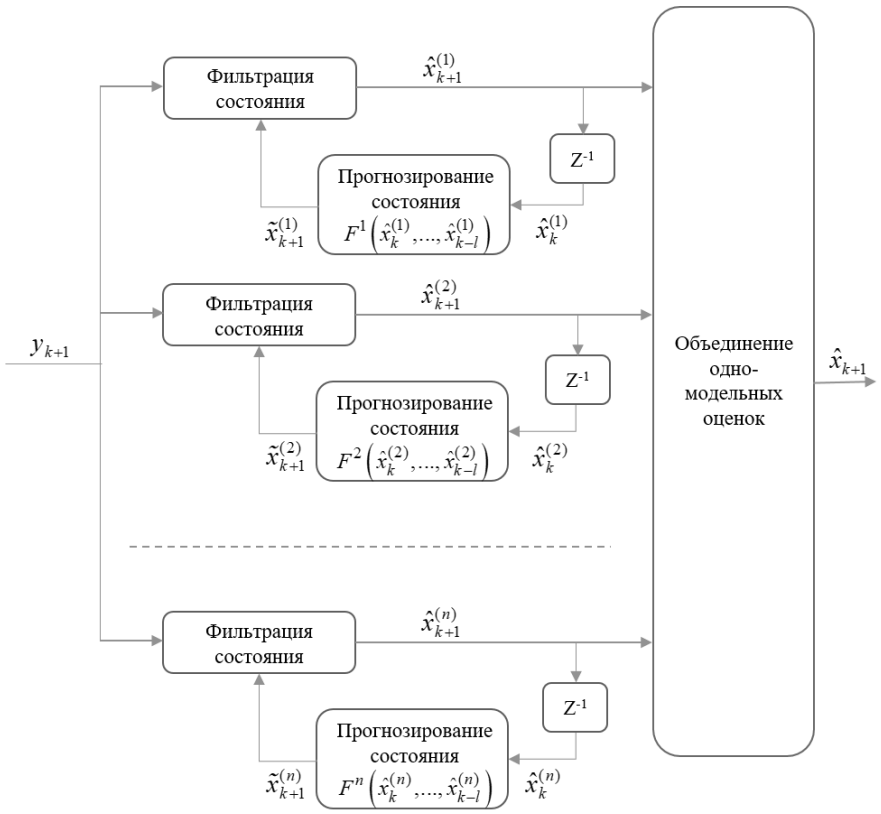

Рис. 1. Структура многомодельной прогнозируемой оценки состояния

Fig.1. The structure of Multi-Model Forecasting State Estimation

Переходные модели используемые в ММПОС

2) Модель авторегрессии первого порядка *AR.*

Использование авторегрессионного анализа эффективно, с точки зрения вычислительной нагрузки, поэтому этот метод широко используется в алгоритмах ПОС.

Модель *AR*(*p*) – это модель, в которой значения временного ряда в текущий момент линейно зависят от предшествующих значений того же ряда. Параметр *p* соответствует количеству используемых предшествующих наблюдений.

$$x_{k+1} = \sum_{i=1}^{p} \varphi_i x_{k+1-i} + \varepsilon_{k+1}\,, \tag{19}$$

где φ_i – авторегрессионнный коэффициент *i*-го порядка, ε_{k+1} – белый шум с нулевым средним и инвариантной во времени ковариационной матрицей.

3) Модель векторной авторегрессии первого порядка *VAR*

VAR модель порядка (*p*) вычисляется согласно выражению

$$x_{k+1} = \Phi_1 x_k + \Phi_2 x_{k-1} + \cdots + \Phi_n x_{k-n+1} + \varepsilon_{k+1}, \tag{20}$$

где Φ_i – матрица коэффициентов $n \times n$.

Результирующая оценка ММПОС формируется как взвешенной суммы одномодельных оценок по критерию оптимальности равному минимуму ковариации результирующей многомодельной оценки [15].

В итоге результирующая оценка формируется на основе равенства:

$$\hat{x} = \sum_{i=1}^{n}\left(\sum_{j=1}^{n}\left(\Sigma^{(j)}\right)^{-1}\right)^{-1} \cdot \left(\Sigma^{(i)}\right)^{-1} \hat{x}^{(i)}, \tag{21}$$

где $\Sigma^{(i)}$ – ковариационная матрица *i*-й оценки $\hat{x}^{(i)}$

Обнаружение кибератаки

Обнаружение кибератаки реализуется с помощью инновационного анализа и анализа невязки измерения и оценки [16].

В момент времени *t*, соответствующему отсчету *k*, нормализованный вектор невязки равен:

$$\varsigma^{n}{}_{k}(i) = \frac{y(i)_k - \hat{x}(i)_k}{\sqrt{E_k(i,i)}}, \tag{22}$$

где $y(i)_k$ – измерение *i*-ого параметра в момент времени k, $\hat{x}(i)_k$ – апостериорная оценка *i*-ого параметра в момент времени *k*, $E_k(i,i)$ – дисперсия невязки *i*-ого параметра в момент времени *k*.

Нормализованный инновационный вектор:

$$\nu^{n}{}_{k}(i) = \frac{y(i)_k - \tilde{x}(i)_k}{\sqrt{Y_k(i,i)}}, \tag{23}$$

где $\tilde{x}(i)_k$ – априорная оценка *i*-ого параметра в момент времени *k*, $Y_k(i,i)$ – дисперсия инновации *i*-ого параметра в момент времени *k*.

Для определения кибератаки задаются пороговые значения $\nu_k^{n,\max}$ и $\varsigma_k^{n,\max}$, при превышении значения которых, соответствующее измерение маркируется подозрительным и заменяется на прогнозное значение оценки.

Моделирование

Моделировалась 30-ти узловая схема *IEEE* (рис. 2) [17], в которой дополнительно имитировалась установка ветрогенераторов на шинах *14, 16, 27*. Ветровая генерация составила около 5% от общей генерируемой мощности в системе. Данные о паттерне изменения ветрогенерации и нагрузки были взяты из открытых отчетов администрации энергокомпании Боневил *(Bonneville Power Administration* (*BPA*)) [18]. Потребление и производство электроэнергии в системе были распределены между узлами пропорционально исходным значениям схемы [17]. Для увеличения частоты дискретизации измерительных сигналов пятиминутные интервалы были линейно экстраполированны, таким образом шаг между измерениями составил 30 секунд. В некоторые моменты времени различные узлы соответствовали разному паттерну изменения нагрузки/генерации. Так же были добавлены случайные флуктуации, характерные для ветрогенерации.

Вектор состояния, включающий комплексные значения напряжений всех узлов, был получен путем расчета оптимального потокораспределения в пакете *PowerModels* программного комплекса *Julia.* Измерения моделировались путем добавления к значениям углов и амплитуды напряжения шума с Гауссовским распределением. Стандартное отклонение по углам составило 0.02 градуса, по амплитудам – 0.5%, что соответствует требованиям по точности устройств векторных синхронизированных измерений [19].

Для имитации кибератаки было произведено 300 расчетов, где в момент времени t_{attack} определялись случайный вектор атаки a и искаженные измерения y_a по выражениям (3)-(6). Задавалось, что атакованы 30% измерений комплексных значений напряжений и токов. Вектор измерений y_a подавался на вход ММПОС, где производилась оценка состояния. Затем выполнялась проверка на наличие кибератаки и в случае обнаружения кибератаки результат оценки заменялся взвешенным прогнозируемым значением

$$\tilde{x} = \sum_{i=1}^{n}\left(\sum_{j=1}^{n}\left(\Sigma^{(j)}\right)^{-1}\right)^{-1} \cdot \left(\Sigma^{(i)}\right)^{-1} \tilde{x}^{(i)} \tag{24}$$

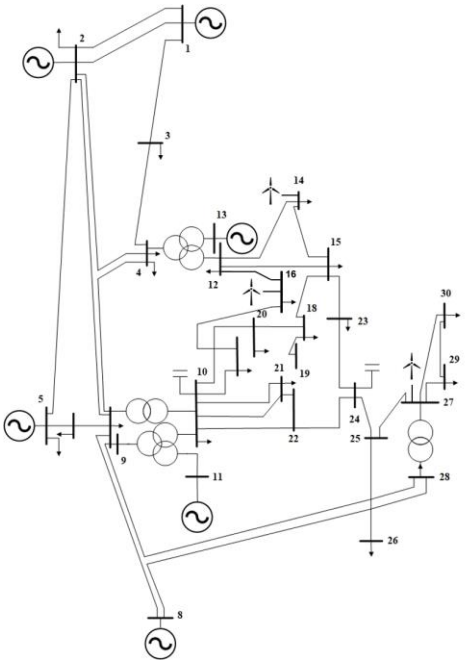

Рис. 2. Схема 30-ти узловой энерогосистемы IEEE

Fig. 2. Scheme of a 30-bus IEEE power system

Результаты

Результаты предложенного алгоритма представлены на рисунке 3 и в таблице.

На рисунке 3 изображен измерения фазного угла напряжения в узле 13 за период времени. В момент отсчета k=500 происходит атака, которая искажает измерение. Алгоритм обнаружения атаки ММПОС определил подозрительное измерение, которое было заменено прогнозной оценкой. Таким образом процесс оценки остался непрерывным с сохранением требуемой точности.

Доля обнаруженных атак составила 100%. Стоит отметить, что такая высокая точность возникает в случае больших значений вектора атаки a. При искажениях злоумышленниками измерений в рамках их погрешности атака может быть не обнаружена, однако в этом случае она и не может нанести ущерба. Предложенный метод также характеризуется малым числом ложных определений кибератак. При этом ложное срабатывание не приводит к потере наблюдаемости энергосистемы, так как исключенное измерение заменяется прогнозной оценкой состояния.

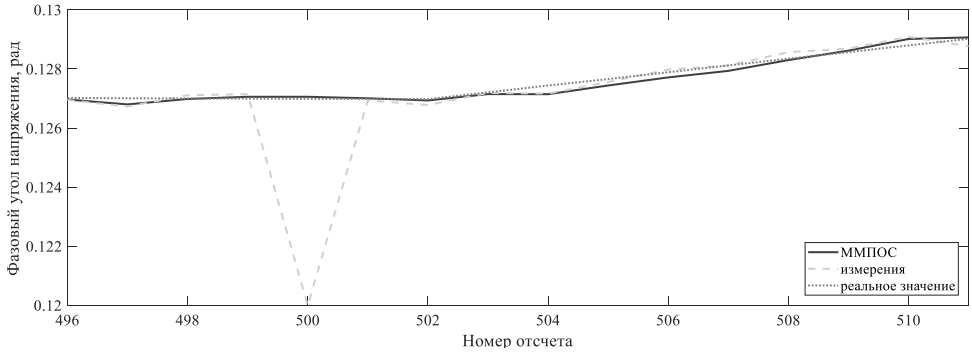

Рис. 3. Результаты предложенного метода обнаружения кибератаки на примере фазового угла напряжения в узле 13.

Fig. 3. Results of detection of the cyberattack on voltage phase angle at node 13 by the proposed method

Таблица

Результаты определения кибератак с вводом неверных данных методом ММПОС

Доля обнаруженных кибератак	Доля необнаруженных кибератак	Доля определений отсутствия кибератак	Доля ложных определений наличия кибератак
100%	0%	99,66%	0,34%

Выводы

Специфической кибератакой для энергосистемы является атаки внедрения ложных данных, мерой защиты от которой выступает статистическая обработка измерительной информации, а именно - оценка состояния параметров режима энергосистемы.

Предлагаемый метод показывает высокую точность определения кибератак при низком уровне ложных срабатываний.

Предлагаемый метод обнаружения кибератак не требует централизованного подхода и может быть реализован в отдельных устройствах защиты и управления электрической сети.

При наличии кибератаки искаженные измерения удаляются и производится замена на значения прогнозируемой ОС для исключения влияния атакованных измерений на результаты ОС. Таким образом, сохраняется непрерывность ОС и предотвращается потеря наблюдаемости энергосистемы.

Литература

1. Колосок И.Н., Гурина Л.А. Оценка качества данных SCADA и WAMS при кибератаках на информационно-коммуникационную инфраструктуру ЭЭС // Информационные и математические технологии в науке и управлении. 2020. № 1(17). С. 69-78.

2. Liu Y., Ning P., and K. Reiter M. False data injection attacks against state estimation in electric power grids. ACM Transactions on Information and System Security (TISSEC). 2011. V. 14. № 1. p. 13.

3. Bobba R.B., Rogers K., Wang Q., et al. Detecting false data injection attacks on DC state estimation. In: Proceedings of First Workshop on Secure Control Systems (SCS 2010), Stockholm, Sweden (April 2010).

4. Karimipour H and Dinavahi V. On false data injection attack against dynamic state estimation on smart power grids. In 2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE). 2017. pp. 388-393.

5. Moslemi R., Mesbahi A., and Velni J. M. A fast, decentralized covariance selection-based approach to detect cyber attacks in smart grids. IEEE Transactions on Smart Grid, 2017.

6. Li S., lmaz Y.Y., Wang X. D. Quickest detection of false data injection attack in wide-area smart grids. IEEE Trans. Smart Grid. 2015. V. 6. № 6. pp. 27252735.

7. Esmalifalak M., Shi G., Han Z and Song L.Y. Bad data injection attack and defense in electricity market using game theory study. IEEE Trans. Smart Grid. 2013. V. 4. №. 1. pp. 160-169.

8. Куликов А.Л., Шарафеев Т.Р., Осокин В.Ю. Методы обнаружения кибератак и анализа сценариев кибернападений на электроэнергетические системы. Вестник НГИЭИ. 2017. Т.10. № 77.

9. Лукичева И.А., Куликов А.Л. 2019. Повышение точности оценки состояния электрической сети в условиях кибератак с использованием медианной фильтрации. Вестник Иркутского государственного технического университета. 2019. Т.23. № 2 (145).

10. Гамм А.З. Статистические методы оценивания состояния электроэнергетических систем. М.: Наука, 1976. 220 с.

11. Zhao J., Comer-Exposito A., Netto M et al. Power System Dynamic State Estimation: Motivations, Definitions, Methodologies, and Future Work // IEEE Transactions on Power Systems. 2019. V. 34, №. 4. pp. 3188–3198.

12. Do Coutto Filho, Milton Brown, and Julio Cesar Stacchini de Souza. Forecasting-aided state estimation. Pt I: Panorama. IEEE Transactions on Power Systems. 2009. pp.1667-1677.

13. Радиоэлектронные системы: Основы построения и теория. Справочник. 2-е изд. пе-рераб. и доп. / под ред. Я.Д. Ширмана. М.: Радиотехника, 2007. 512 с.

14. Da Silva A.L, Do Coutto Filho M., Cantera J. An efficient dynamic state estimation

algorithm including bad data processing // IEEE transactions on Power Systems. 1987. V. 2, no. 4. pp. 1050–1058.

15. An elementary introduction to Kalman filtering / Y. Pel, S. Biswas, D.S. Fussell, K. Pingali // Communications of the ACM 62.11. 2019. pp. 122–133.

16. Geetha SJ, Chakrabarti S, Rajawat K, et al. An asynchronous decentralized forecasting-aided state estimator for power systems. IEEE Transactions on Power Systems. 2019. V. 34(4). pp. 3059-3068.

17. Liao Yizheng, Yang Weng, Guangyi Liu, Ram Rajagopal Urban mv and lv distribution grid topology estimation via group lasso // IEEE Transactions on Power Systems 34.1. 2018. V. 34(1). pp. 12–27.

18. Administration B. P. (2012) Wind generation total load in the bpabalancing authority. Available at http://transmission.bpa.gov/business/operations/wind.

19. Meliopoulos, Madani V., Novosel D, et al. Synchrophasor measurement accuracy char-acterization // North American Synchro Phas-or Initiative Performance &Standards Task Team (Consortium for Electric Reliability Technology-Solutions). 2007. V. 10.

Авторы публикации

Лукичева Ирина Александровна – стажер-исследователь Сколковского института науки и технологий центра Энергетических наук и технологий, Москва, Россия.

Куликов Александр Леонидович – д-р техн. наук, профессор кафедры «Электроэнергетика, электроснабжение и силовая электроника», Нижегородский государственный технический университет им. Р.Е. Алексеева».

References

1. Kolosok IN, Gurina LA. Quality Assessment of SCADA and WAMS Data in the Case of Cyberattacks on Information and Communication Infrastructure of EPS . *Information and mathematical technologies in science and management.* 2020;1(17): 69-78.

2. Liu Y, Ning P and Reiter MK. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC)*. 2011;14(1):13.

3. Bobba RB, Rogers K, Wang Q, et al. Detecting false data injection attacks on DC state estimation. *Proceedings of First Workshop on Secure Control Systems (SCS 2010)*, Stockholm, Sweden (April 2010).

4. Karimipour H and Dinavahi V. *On false data injection attack against dynamic state estimation on smart power grids.* 2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE). 2017. pp. 388-393.

5. Moslemi R., Mesbahi A., and Velni J. M. *A fast, decentralized covariance selection-based approach to detect cyber attacks in smart grids.* IEEE Transactions on Smart Grid, 2017.

6. Li S, lmaz YY and Wang XD. Quickest detection of false data injection attack in wide-area smart grids. *IEEE Trans. Smart Grid*. 2015;6(6):2725-2735.

7. Esmalifalak M, Shi G, Han Z, et al. Bad data injection attack and defense in electricity market using game theory study. *IEEE Trans. Smart Grid*. 2013;4(1):160-169.

8. Kulikov AL, Sharafeev T.R, Osokin V.U. Methods of Detecting Cyber Attacks and Analysis of Scenarios of Cyber Attacks on the Power System. Bulletin NGIEI. 2017(10 (77)).

9. Lukicheva IA, Kulikov AL. Povyshenie tochnosti otsenki sostoyaniya elektricheskoi seti v usloviyakh kiberatak s ispol'zovaniem mediannoi fil'tratsii. *Vestnik Irkutskogo gosudarstvennogo tekhnicheskogo universiteta*, 2019;23:2 (145).

10. Gamm AZ. Statistical methods for the power systems state estimation. M.: Nauka, 1976, 220 p.

11. Zhao A. Comer-Exposito, Netto M, et al. *Power System Dynamic State Estimation: Motivations, Definitions, Methodologies, and Future Work*. IEEE Transactions on Power Systems. 2019;34(4):3188–3198. doi: 10.1109/TPWRS.2019.2894769.

12. Do Coutto Filho, Milton Brown, and Julio Cesar Stacchini de Souza. *Forecasting-aided state estimation-Part I: Panorama.* IEEE Transactions on Power Systems 24.4 (2009): 1667-1677.

13. Hirman S. YAD. Radioelektronnye sistemy: Osnovy postroeniya i teoriya. Spravochnik. Electronic systems: Basics of construction and theory. Izd. 2-e pererab. i dop. M.: Radiotekhnika, 2007. 512 p.

14. Da Silva A.L, Do Coutto Filho M, Cantera J. An efficient dynamic state estimation algorithm including bad data processing // IEEE transactions on Power Systems. 1987;2(4):1050–1058.

15. Pel Y, Biswas S, Fussell DS, et al. *An elementary introduction to Kalman filtering.* Communications of the ACM 62.11. 2019. pp. 122–133.

16. Geetha SJ, Chakrabarti S, Rajawat K, Terzija V. *An asynchronous decentralized forecasting-aided state estimator for power systems.* IEEE Transactions on Power Systems. 2019 Jan 31;34(4):3059-68.

17. Liao Yizheng, Yang Weng, Guangyi Liu, Ram Rajagopal. Urban mv and lv distribution grid topology esti-mation via group lasso. IEEE Transactions on Power Systems 34.1. 2018. pp. 12–27.

18. Administration BP. (2012) Wind generation total load in the bpabalancing authority. [Online]. Available at http://transmission.bpa.gov/business/operations/wind

19. Meliopoulos A, Madani V, Novosel D, et al. Synchrophasor measurement accuracy char-acterization. North American Synchro Phas-or Initiative Performance &Standards Task Team (Consortium for Electric Reliability Technology-Solutions). 2007. V. 10.

Authors of the publication

Irina A. Lukicheva – Center for Energy Science and Technology, Moscow, Russia.

Alexander L. Kulikov – Power Supply and Power Electronics, Nizhny Novgorod State Technical University R.E. Alekseeva. Nizhny Novgorod, Russia.

Получено ***15.10.2021г***

Отредактировано ***23.10.2021г***

Принято ***25.10.2021г.***