Гао Кунлун (GAO Kunlun), China Electric Power Research Institute,
Ванг (WANG Yufei), China Electric Power Research Institute,
Ксу Руши (XU Ruzhi), North China Electric Power University

Исследование и применение методов ситуационного анализа кибербезопасности в интеллектуальных сетях

Когда информационно-коммуникационные технологии (ИКТ) стали всесторонне применяться во всех аспектах производства, передачи, преобразования и распределения электроэнергии, потоки электричества, технической и бизнес-информации достигли высокой степени интеграции в интеллектуальных сетях (smart grid). Поскольку интеллектуальные сети включают в себя большое количество информационных систем и оборудования, может возникнуть множество угроз, связанных с обеспечением кибербезопасности. Чтобы с этим справиться, должна быть построена система активной защиты интеллектуальной сети. Одна из ключевых технологий для построения такой системы – ситуационный анализ кибербезопасности (cybersecurity situation evaluation, CSSE).

На основании анализа большого числа микросостояний (событий) и мониторинга результатов технология CSSE позволяет спрогнозировать и оценить общую кибербезопасность интеллектуальной сети. Оценка методов защиты от кибератак сосредоточена в основном на информировании (cybersecurity situation awareness, CSSAw), оценке (cybersecurity situation assessment, CSSAs) и прогнозировании (cybersecurity situation forecast, CSSF).

Был предложен и реализован новый метод ситуационного анализа с применением алгоритма AdaBoost (Адаптивного усиления):

a. С помощью тщательного анализа процессов CSSAw и CSSF была описана аппроксимационной функцией их общая математическая модель. Кроме того, с учётом процессов CSSAw, CSSAs и CSSF была разработана интегральная модель CSSE, которая описывает как CSSAw, так и CSSF функциями аппроксимации и решает эти задачи по отдельности с помощью многократного применения алгоритма AdaBoost. Интегральная модель значительно упростила сложность модели CSSE.

b. В целях повышения надёжности метода CSSE были полностью учтены требования к точности, оперативности и интеллектуальности: для точности в качестве ключевого алгоритма аппроксимирующей функции использовался алгоритм AdaBoost, особенность которого заключается в непрерывном обучении, что значительно улучшает точность функции аппроксимации; для оперативности в качестве слабого «ученика» алгоритма AdaBoost используется метод CVM (core vector machine), что значительно уменьшает время расчётов и объём вычислений; интеллектуальность заключается в том, что все алгоритмы основаны на теории искусственного интеллекта и могут работать полностью в автоматическом режиме после предварительной настройки параметров работы.

c. На основании проекта по мониторингу кибербезопасности Государственной электросетевой корпорации Китая (State Grid Corporation of China, SGCC) модель CSSE была применена в крупномасштабной системе раннего предупреждения об угрозах кибербезопасности и её практичность была проверена в течение более трёх лет.

Введение

В последние годы интеллектуальные сети с функциями «информатизации, автоматизации, взаимодействия» переживают бурный рост. Информационные и коммуникационные технологии (ИКТ) широко используются во всех аспектах интеллектуальных сетей, таких как генерация, передача, преобразование, распределение и диспетчеризация электроэнергия и т. д., и обеспечивают высокую степень интеграции между потоками энергии, управляющей информации и данных. Интеллектуальные сети значительно расширили границы своего информационного простран-

ства и накопили большой опыт интеллектуального управления и взаимодействия их подсистем. Однако они сталкивается с беспрецедентными проблемами, связанными с кибербезопасностью. Интеллектульная сеть подвержена кибератакам, которые всерьёз ставят под угрозу её существование. Это, например, атаки на системы управления промышленными предприятиями [1, 2], крупные сетевые каскадные аварии, вызванные кибератаками [3, 4], атаки типа внедрения SQL-кода, направленные на интеллектуальную сеть [5, 6], и так далее.

Таким образом, традиционные методы обеспечения кибербезопасности, основанные на статической политике безопасности, постсобытийном тестировании и пассивной реакции, могут больше не удовлетворять потребностям текущей ситуации. Вместо этого предлагается система активной защиты от киберугроз, характеризующаяся встроенным «иммунитетом», динамическим информированием и целевым оповещением. Одной из ключевых технологий системы активной защиты является ситуационный анализ кибербезопасности (CSSE).

На основании анализа большого числа микросостояний (событий) и мониторинга результатов, CSSE позволяет провести оценку текущей ситуации и спрогнозировать общую кибербезопасность в реальном времени. Метод защиты от кибератак сосредоточен в основном на информировании о киберугрозах (cybersecurity situation awareness, CSSAw), оценке ситуации кибербезопасности (cybersecurity situation assessment, CSSAs) и прогнозировании (cybersecurity situation forecast, CSSF) [7, 8]. CSSAw используется для отображения локальной (микроскопической) ситуации с кибербезопасностью в целевой сети; CSSAs может интегрировать результаты CSSAw по всей сети, чтобы получить общую оценку кибербезопасности (cybersecurity situation value, CSSV), а CSSV отражает оценку кибербезопасности в режиме реального времени в целевой области на макроуровне; CSSF используется для получения оценки кибербезопасности в целевой сети в следующий момент.

В последние годы понятие CSSE вводится также в кибербезопасность, связанную с электроэнергией. В работах [9–12] в целях реализации информированности о ситуации с микробезопасностью для локальной области интеллектуальных сетей для разработки классификатора и решения проблем классификации использовались методы CVM (core vector machine) и BVM (ball vector machine), оптимизированные алгоритмами роевого интеллекта (PSO или QGA и т. д.), и классификатор служил системой обнаружения вторжений. В работах [13, 14] при построении системы индексов оценки кибербезопасности микрорезультаты CSSAw искусственно рассчитываются в CSSV для отражения исторической (архивной) и текущей (в реальном времени) оценки кибербезопасности сети. При построении системы индексов применены комплексные инструменты оценки, такие как метод анализа иерархий (МАИ) и «серый кластерный анализ» (gray clustering analysis). В работах [15, 16] для интеллектуальных сетей реализуется CSSF, где ключевая идея заключается в абстракции CSSF через задачу регрессии. Классификатор (SVM-классификатор, оптимизированный алгоритмами роевого интеллекта типа МРЧ (метод роя частиц) или QGA (quantum genetic algorithm) и т. п.) применяется для обучения и получения из архивных данных модели CSSF, и эта модель используется для раннего предупреждения о будущих тенденциях CSSV. Но есть определённый дефицит в результатах данных исследований. Несмотря на то, что предыдущие решения CSSAw и CSSF основаны на алгоритмах искусственного интеллекта, исследования этих двух частей независимы друг от друга и не имеют глубокого анализа их математического характера.

В данной статье представлена интегрированная модель CSSE. Практически она была развёрнута в информационной сети Государственной электросетевой корпорации Китая (SGCC). Этапы заключались в следующем:

a. Был проведён углублённый анализ рабочих процедур CSSAw и CSSF и выяснены математические характеристики для нахождения связей с их математическими моделями.

b. На основе алгоритма AdaBoost была разработана модель CSSE, последовательно выполняющая функции CSSAw, CSSAs и CSSF. Здесь алгоритм AdaBoost применяется несколько раз, чтобы упростить структуру модели CSSE, и использование характера самообучения алгоритма AdaBoost эффективно улучшает точность CSSE.

c. На основе проекта «системы обеспечения безопасности информационной сети (ISS)», модель CSSE была развёрнута в крупномасштабной системе мониторинга кибербезопасности.

Краткие сведения о CSSE

Области исследования CSSE

Для аккуратного описания ситуации с кибербезопасностью современной масштабной сети сегодня недостаточно полагаться только на простые сетевые эксплуатационные характеристики, такие как сетевая топология, рабочее состоянии каждого узла, сетевые соединения и сетевые потоки и т. д., требуются более сложные технические средства.

В 1988 году концепция оценки кибербезопасности была предложена при изучении технологии управления воздушным движением: «Оценка кибербезопасно-

сти сети – это текущее и прогнозное состояние всей целевой сети, содержащей различное функционирующее оборудование, а также поведение пользователей и других факторов в определённый период времени» [17]. Таким образом, CSSE должна включать в себя микро- и макропонимание текущего состояния кибербезопасности в целевой сети – CSSAw и CSSAs, а также прогноз кибербезопасности в целевой сети – CSSF.

Рис. 1. Процесс расчёта CSSV

CSSAw является эффективным средством для получения в режиме реального времени информации о микроситуации с кибербезопасностью для сети, по которой можно судить о существовании кибератак на основе всеобщего сбора данных в режиме реального времени с конкретных узлов в целевой сети. Данные содержат информацию о сетевых сообщениях, распределении сетевых потоков, состоянии системных процессов и функционировании сервисов. Обычно в качестве CSSAw для малых и средних сетей может быть использована технология обнаружения вторжений.

CSSAs может отвечать за использование системы индексов оценки кибербезопасности для расчёта текущей CSSV с помощью микрорезультатов CSSAw и за отображение в реальном времени макроситуации кибербезопасности целевой сети. CSSV – численное описание ситуации кибербезопасности. Это значение непосредственно отражает макроситуацию кибербезопасности в целом. Расчёт процесса CSSV показан на рис. 1.

CSSF предсказывает тенденции развития ситуации макрокибербезопасности прогнозированием будущего CSSV целевой сети.

Таким образом, существует явная причинная связь между тремя рабочими процессами: CSSAw – первый процесс, который должен быть запущен при оценке CSSE, затем процесс CSSAs использует CSSV для описания ситуации макрокибербезопасности посредством всеобъемлющего расчёта результатов CSSAw, и наконец CSSF использует CSSV в качестве источника данных. Полный цикл работы CSSE показан на рис. 2.

Анализ математических характеристик CSSE

Математические характеристики CSSAw

Процесс CSSAw представляет собой следующее: на основе текущего сетевого трафика производится запись мониторинга, которая состоит из n полей данных, затем они используются, чтобы различными аналитическими методами определить, принадлежит ли трафик к некоторым видам кибератак (при условии, что имеется m видов кибератак). Этот процесс аналогичен функции аппроксимации: целевая задача (CSSAw) с n-мерным входом (запись со структурой n полей данных) и 1-мерным выходом (выходное значение представлено m + 1 значениями скаляра, где m это виды кибератак, а 1 – нормальное функционирование сети). Так CSSAw можно абстрагировать в функцию проблемы с фиксированным выходным диапазоном.

Функция аппроксимации, соответствующая CSSAw, имеет фиксированный выходной диапазон (потому что виды кибератак ограничены), поэтому нелинейной функцией аппроксимации типа «S» можно добиться точной классификации данных мониторинга, как показано на рис. 3(а).

Математические характеристики CSSF

Процесс CSSF представляет собой следующее: CSSV v_1, v_2, ...,v_m – известные точки непрерывного мониторинга архивных данных, по которым с помощью различных методов прогнозируются CSSV v_{m+1}, v_{m+2}.

Теперь CSSF можно объяснить с помощью функции аппроксимации: CSSF имеет типичные характеристики одномерного временного ряда. В CSSF выходные значения (будущий CSSV) могут быть спрогнозированы

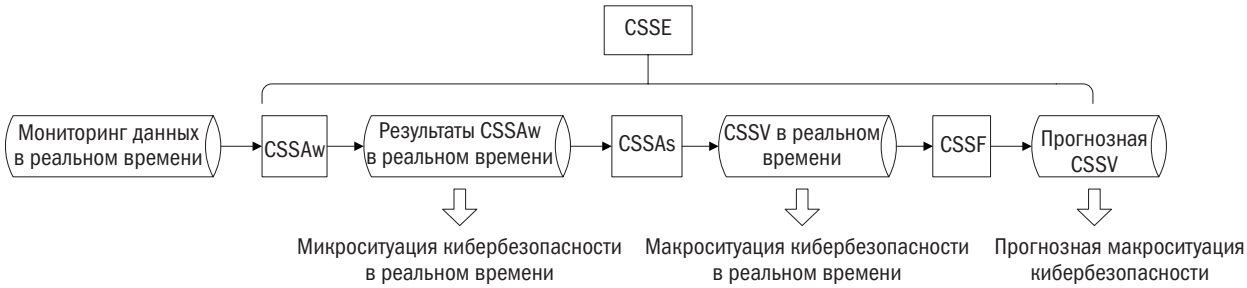

Рис. 2. Цикл работы CSSE

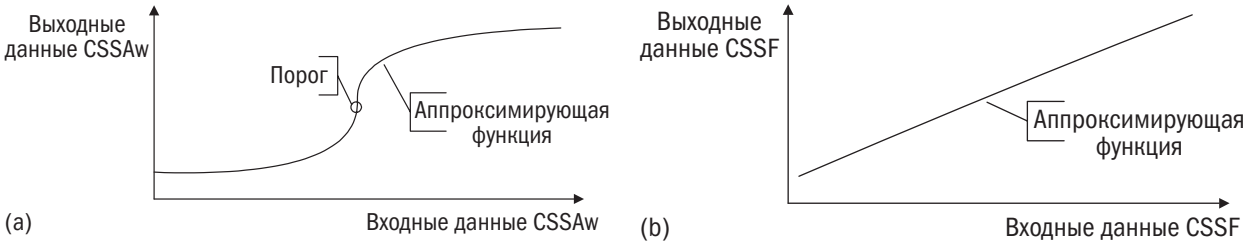

Рис. 3 Функция аппроксимации CSSAw (a) и функция аппроксимации CSSF (b)

через множество непрерывных входных значений (архивные значения CSSV). Необходимым условием решения проблемы временных рядов с помощью аппроксимирующей функции является построение нескольких дуальных групп «вход-выход».

Дуальная группа генерируется динамическим скользящим окном [18]. Если установить размер «скользящего» окна равным m, а длину шага равной 1, то первый вход «v_1, v_2, ..., v_m», даст на выходе v_{m+1}; аналогичным образом, второй вход «v_2, v_3, ...,v_{m+1}», даст на выходе v_{m+2} и так далее. Поскольку диапазон значений CSSV непредсказуем, линейная функция аппроксимации должна быть использована для описания CSSF, как показано на рис. 3(b).

Математическая составляющая между CSSAw и CSSF

Теперь мы видим, что, хотя CSSAw и CSSF находятся на разных стадиях CSSE, они имеют высокую согласованность математической составляющей. У них один и тот же рабочий механизм, который может оценивать один выход через множество входных факторов, и они оба могут быть описаны с помощью аппроксимирующей функции «многомерной вход – одномерный выход». Единственное различие между ними заключается в том, что формы аппроксимирующих функций различны, что обусловлено разными физическими смыслами CSSAw и CSSF. Процесс аппроксимации CSSAw и CSSF показан на рис. 4.

Оценка кибербезобасности модели Смартгрид

Интегральная структура модели оценки кибер–безопасности

CSSE может контролировать микро- и макроситуацию с кибербезопасностью всей целевой сети непрерывно и направить предупреждающий сигнал на ранней стадии для возможных ситуаций угроз кибер-

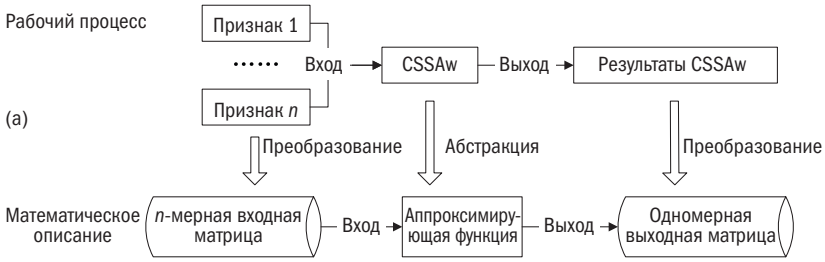

Рис. 4 (a) Процессы аппроксимации CSSAw

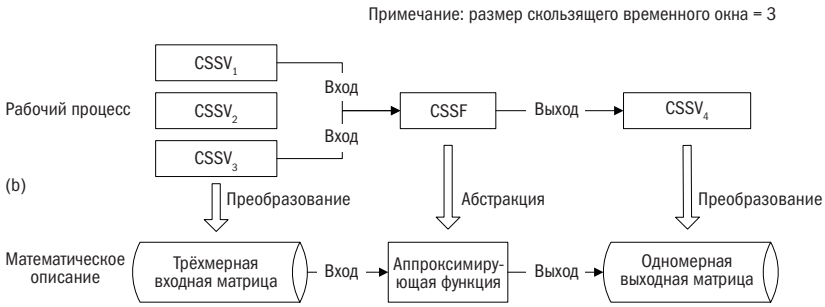

Рис. 4 (b) Процессы аппроксимации CSSF

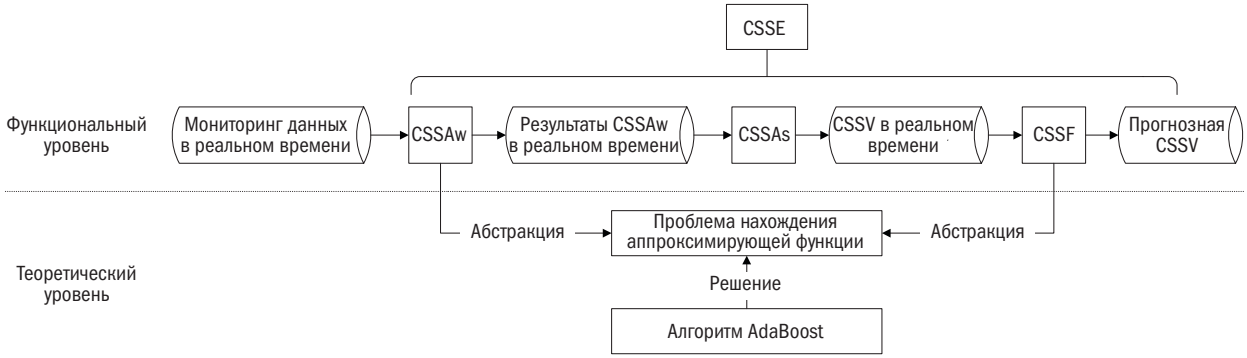

Рис. 5. Механизм работы модели CSSE

безопасности на макро уровне, так что модель CSSE может в полной мере реализовать CSSAw, CSSAs и CSSF. Как мы знаем, CSSAw и CSSF имеют один и тот же математический механизм, а алгоритм AdaBoost используется для решения проблемы аппроксимации в модели CSSE. В модели CSSE алгоритм AdaBoost используется в обоих процессах (как в CSSAw, так и в CSSF), что эффективно снижает сложность модели CSSE. Механизм работы модели CSSE показан на рис. 5. В дополнение, подмодель CSSAs модели CSSE, которая фиксирует индекс системы оценки кибербезопасности, разработана эталонным методом [13]. Полная модель CSSE показана на рис. 6.

Таким образом, у интегральной модели CSSE есть две примечательные особенности: 1) в реализации проекта одинаковый механизм CSSAw и CSSF, используемый в модели CSSE, может упростить модель структуры и улучшить эффективность алгоритма; 2) может быть построена законченная структура из последовательностей CSSAw, CSSAs и CSSF.

Теоретические основы модели оценки кибербезобасности

В целях соответствия модели CSSE требованиям по «точности», «работе в реальном времени» и «интеллектуальности», для аппроксимирующей функции используется алгоритм AdaBoost, являющийся ключевым моментом работы модели CSSE.

***a.* Точность**

Модель CSSE может определить, есть ли угрозы кибербезопасности в текущей области мониторинга, и спрогнозировать тенденцию возникновения угрозы кибербезопасности в будущем. Преимущество алгоритма AdaBoost состоит в непрерывном обучении на ошибках больших выборок, которое улучшает точность аппроксимирующей функции.

***b.* Работа в реальном времени**

Модель CSSE может завершить анализ данных и обработки данных в течение короткого времени. В качестве самообучающейся машины слабого уровня алгоритма AdaBoost выбран метод CVM (Core Vector Mashine), который может значительно снизить трудоёмкость и сложность вычислений.

***c.* Интеллектуальность**

Все задействованные алгоритмы в модели CSSE имеют теоретическое обоснование искусственного интеллекта и позволяют полностью автоматизировать работу после предварительной настройки рабочих параметров.

Алгоритм AdaBoost описывается следующим образом. Во-первых, слабая обучающаяся машина проводит многократную последовательную прогонку данных для получения последовательности базовых классификаторов. Во-вторых, после получения своих «весов» все базовые классификаторы представляют собой сильную обучающуюся машину. В-третьих, сильная обучающаяся машина используется для завершения всех расчётов [19, 20]. Наиболее важной особенностью алгоритма AdaBoost является то, что в процессе обучения подготовка каждой следующей выборки производится в соответствии с ошибками классификации предыдущих выборок. Рис. 7 представляет собой схему алгоритма AdaBoost.

В алгоритме AdaBoost сильная конечная обучающаяся машина получается обучением слабой машины. Поэтому выбор самой слабой обучающейся машины напрямую повлияет на производительность алгоритма AdaBoost. В модели CSSE слабой обучающейся машиной является CVM. Метод CVM – это улучшение метода опорных векторов (support vector mashine, SVM). Улучшение состоит в том, что вместо квадратичного программирования в SVM [21, 22], применяется минимальная ограничивающая сфера (minimum en-

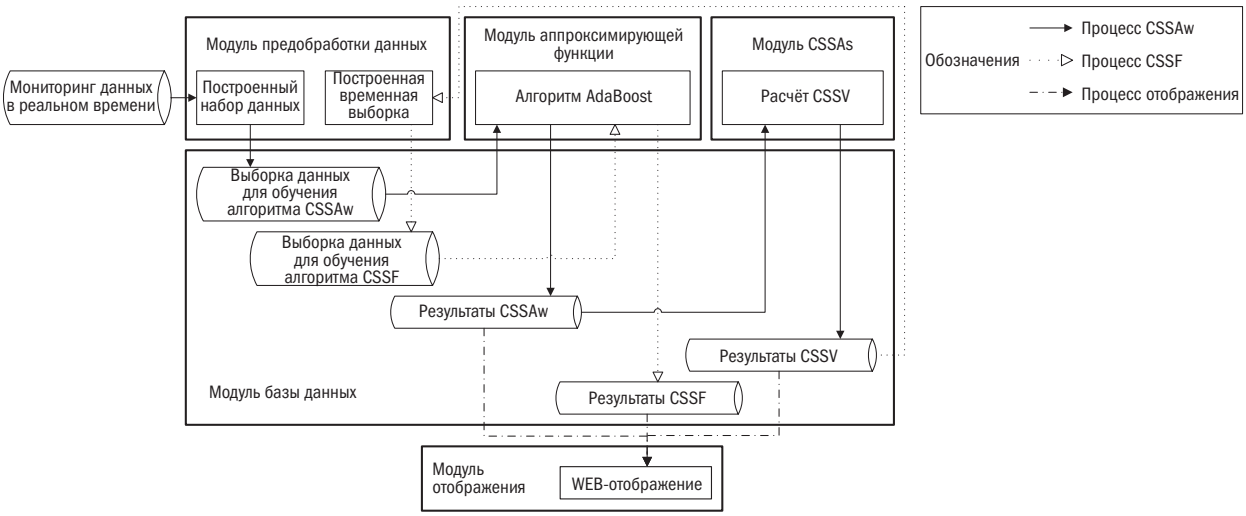

Рис. 6. Интегральная структура модели CSSE

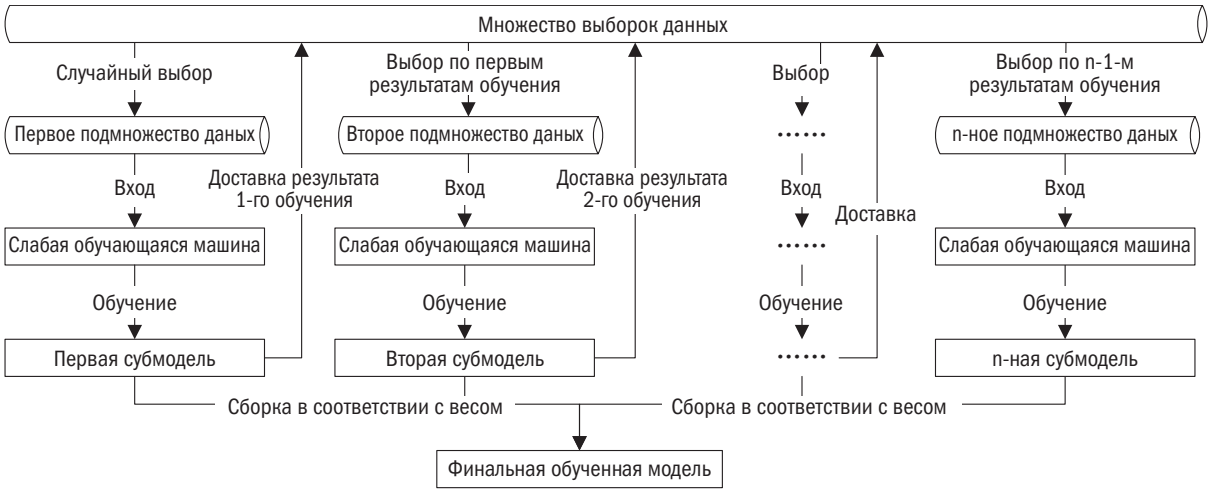

Рис. 7. Рабочий процесс алгоритма Ada–boosting

closing ball, MEB). Если в выборке есть n образцов, то временная сложность метода CVM составляет O(n), а пространственная сложность CVM не зависит от n. Тем не менее временная сложность SVM составляет O(n^3), а пространственная сложность CVM составляет O(n^2). Метод CVM, очевидно, имеет большое преимущество в скорости для данных CSSE.

Рабочий процесс модели CSSE, основанный на алгоритме AdaBoost

Рабочий процесс CSSAw

Модель CSSAw, основанная на алгоритме AdaBoost, включает в себя три фазы: «предварительная обработка данных», «автономное обучение» и «онлайн-работа».

Фаза I: «Предварительная обработка данных».

a. Сбор данных. Собираются все данные в режиме реального времени в области мониторинга с датчиков, которые будут служить в качестве источников данных CSSAw.

b. Построение набора данных. Объединяются данные $x^i_1, x^i_2, ..., x^i_n$ для параметров $x_1, x_2, ..., x_n$ с результатом CSSAw y^i в каждой точке времени i для построения набора данных D для CVM.

Фаза II: «автономное обучение».

Для того чтобы получить подмодель CSSAw с высокой точностью, набор данных D обучается по алгоритму AdaBoost.

c. Устанавливается максимальное число интеграций T для алгоритма AdaBoost и параметры обучения по умолчанию для CVM.

d. Стандартизируется набор данных D и устанавливается ω_1 (l) в качестве начального значения каждой выборки D, $\omega_1(l) = 1/m$, $l \in [1, ..., m]$, где m – общее количество выборок в D.

e. Строится подвыборка D_f из первых 50 % максимальных ω_f (l) в распределении D. Получается базовый классификатор h_f из подвыборки D_f от CVM, $f \in [1, ..., T]$.

На шаге e выбирается условие ω_f (l), при котором результат CSSAw (полученный h_f) не соответствует действительности. Если условие выполняется, ω_f (l) является результатом; в противном случае ω_f (l) =0.

f. Рассчитывается ошибка классификации ε_f для классификатора h_f по формуле (1), $f \in [1, ..., m]$, ω_f (l) есть выбор вероятности:

$$\varepsilon_f = \sum_{l=1}^{m} \omega_f(l) \qquad (1)$$

g. Рассчитывается вес α_f для h_f, по формуле (2).

$$\alpha_f = \frac{1}{2}\ln\frac{1-\varepsilon_f}{\varepsilon_f} \qquad (2)$$

h. Обновляется вес выборки D, по формуле (3).

$$\omega_{f+1}(l) = \frac{\omega_f(l)e^{-\alpha_f h_f(x_l)}}{M_f} \qquad (3)$$

В формуле (3) $\omega_{f+1}(l)$ – новый вес, $\omega_f(l)$ – старое значение веса выборки, h_f (x_l) – результат CSSAw для входных данных x_l от CVM, M_f – коэффициент нормализации, который приводится в формуле (4).

$$\sum_{l=1}^{m} \omega_{f+1}(l) = 1 \qquad (4)$$

i. После выполнения любого из следующих условий происходит переход к шагу j, в обратном случае – возвращение к шагу e:

Условие 1: Алгоритм AdaBoost достигает максимального числа итераций T.

Условие 2: Значение показателя $\omega_f(l)$ не изменяется.

j. Выходной результат (сильный классификатор) H рассчитывается по формуле (5), где *sign* – кусочно-линейная-функция.

$$H = sign\left[\sum_{f=1}^{T} \alpha_f h_f(x)\right] \qquad (5)$$

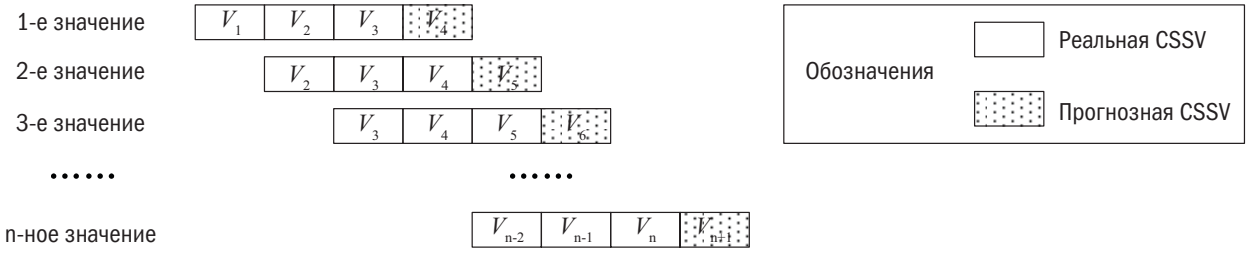

Рис. 8. Сборка обучающей выборки при помощи скользящего временного окна

Фаза III: «онлайн работа».

k. Ввод данных мониторинга в реальном времени $x_1, x_2, ... x_n$ для сильного классификатора *H*.

l. Использование сильного классификатора *H* для CSSAw в режиме реального времени.

Рабочий процесс CSSF

Модель CSSF, основанная на алгоритме AdaBoost, включает в себя те же три фазы – «предварительная обработка данных», «автономное обучение» и «онлайн-работа», но между CSSF и CSSAw существуют различия в «предварительной обработке данных».

Фаза I: «предварительная обработка данных».

Все значения дискретных точек времени CSSV V_i объединяются во временные ряды $S=\{V_1, V_2, ..., V_i\}$ с применением скользящего окна. Устанавливается размер скользящего окна, равный 4, и шаг, равный 1, как показано на рис. 8. Для каждой выборки CSSF выходным является последнее значение, а остальные значения являются входом.

Фаза II: «автономное обучение».

Поскольку алгоритм AdaBoost вызывается последовательно, как и в модели CSSE, все шаги данной фазы (за исключением шага *e*) согласуются с шагом в CSSAw. За исключением шага *e* CSSF, $\omega_f(l)$ определяется по формуле (6).

(a) Домашняя страница ISS

(b) Сеть филиалов

(c) Пограничные угрозы

(d) Страница «глубокого» анализа

Рис. 9. Графический интерфейс ISS

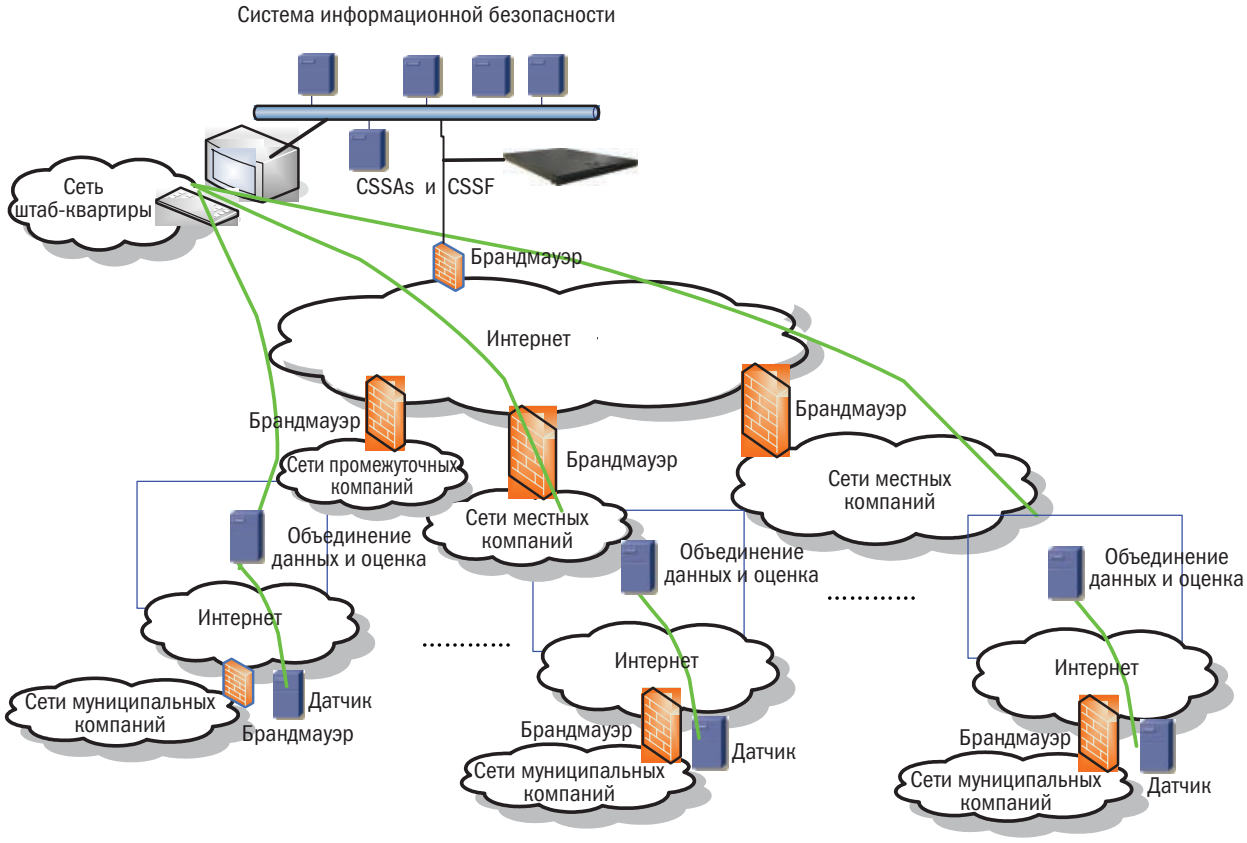

Рис. 10. Структура ISS

$$\frac{\left|\hat{V}_{i+4} - V_{i+4}\right|}{V_{i+4}} \geq 15\% \qquad (6)$$

Если данное условие выполняется, то $\omega_f(l)$ является его результатом, в противном случае $\omega_f(l) = 0$. В формуле (6) V_{i+4} является прогнозным значением CSSV, 15% – это текущий порог ошибок CSSF.

Фаза III: «онлайн-работа/обработка».

Для получения прогноза CSSV архивные данные CSSV служат входными данными для модели CSSF.

Практическое применение метода оценки кибербезопасности в интеллектуальных сетях

Обзор информационной системы мониторинга сетевой безопасности

На основе технологического проекта 2010 «Изучение системы мониторинга кибербезопасности» (The Study of cybersecurity monitoring system) была разработана Система мониторинга информационной безопасности сети (ISS) Государственной электросетевой корпорации Китая (SGCC). Система может в режиме реального времени опознавать киберугрозы Интернет-границам SGCC и более 40 её дочерних компаний, и эффективно улучшать их устойчивость против кибератак. В ISS была развёрнута модель CSSE, основанная на вышеупомянутом алгоритме AdaBoost,.

ISS стала одним из самых важных технических средств защиты SGCC. Основные графические интерфейсы показаны на рис. 9.

Структура развёрнутой ISS

Компоненты ISS развёрнуты на двух уровнях: в штаб-квартире SGCC и её филиалах. Подсистема CSSAw внедрена в каждом филиале, результаты CSSAw передаются в модель углублённого анализа головного сервера в штаб-квартиру SGCC для получения макро-CSSAs и CSSF, как показано на рис. 10.

1. Датчики установлены на Интернет-границах каждого филиала в виде зеркалирующего байпаса и выполняют следующую работу в режиме реального времени:
   - *a.* Объединяют события нарушения границ Интернет-пространства.
   - *b.* Анализируют и определяют сетевой трафик, а также генерируют предупреждения.
2. Узлы аггрегации и подсистемы CSSAw установлены в филиалах и выполняют следующие задачи:
   - *a.* Суммирование и передача всех видов событий кибератак, обнаруженных датчиками;
   - *b.* Выполнение процедуры CSSAw каждого филиала.
3. Установленный в филиалах SGCC серверный кластер анализирует в режиме реального времени результаты CSSAw и события возникновения угроз во всех филиалах, путём выполнения следующих функций:

a. Анализ возникновения угроз нарушения границ Интернет-пространства в режиме реального времени.

b. Анализ сетевого трафика.

c. Анализ и отображение данных отчётов о киберугрозах.

d. Оценка и отображение состояния кибербезопасности в режиме реального времени для всей GSCC.

e. Прогноз возникновения киберугроз в будущем.

Архитектура ПО ISS

Иерархически (снизу вверх) архитектура программного обеспечения ISS состоит из трёх уровней – сбора, анализа и представления, как это показано на рис. 11. Уровень сбора отвечает за сбор данных с датчиков. После фильтрации на этом уровне собранные данные передаются на уровень анализа, где они централизованно хранятся и анализируются, чтобы извлечь максимум полезной информации. Кроме того, на уровне анализа завершаются процессы CSSAw, CSSAs и CSSF. Уровень представления обеспечивает человеко-машинный интерфейс взаимодействия, отображает результаты анализа администраторам и принимает команды от администраторов кибербезопасности.

Выводы

Для решения проблем кибербезопасности, с которыми сталкиваются при построении интеллектуальных сетей, предложен и реализован новый метод оценки кибербезопасности на основе алгоритма AdaBoost, используемый в активной системе защиты от киберугроз.

CSSE может показывать в режиме реального времени угрозы кибербезопасности всех типов сетевых атак на микроуровне, информировать об атаках на макроуровне и прогнозировать будущие угрозы на глобальном уровне. В документе в первую очередь анализируется математическая составляющая процессов CSSAw и CSSF, и показывается, что они оба могут быть интерпретированы аппроксимирующими функциями, с дальнейшей разработкой интегральной модели CSSE. По сравнению с другими существующими моделями CSSE, метод имеет очевидные преимущества: во-первых, CSSAw и CSSF реализованы с помощью функций аппроксимации, что эффективно упрощает структуру модели; во-вторых, CSSAw и CSSF связаны последовательно с системой оценки кибербезопасности, которая основана на кластерном анализе для построения полного процесса CSSE.

Кроме того, для обеспечения точности и быстродействия CSSE, а также для увеличения интеллектуальности модели CSSE и сокращения участия человека модель CSSE использует в качестве аппроксимирующей функции алгоритм AdaBoost, использующий CVM в качестве слабой обучающейся машины. С одной стороны, алгоритм AdaBoost может улучшить точность аппроксимирующей функции путём расчёта ошибки для выборки, повышающей качество обучения; а с другой стороны, слабый алгоритм обучения CVM может значительно снизить трудоёмкость и сложность расчётов, а также повысить эффективность и быстроту вычисления модели CSSE. Все виды интеллектуальных

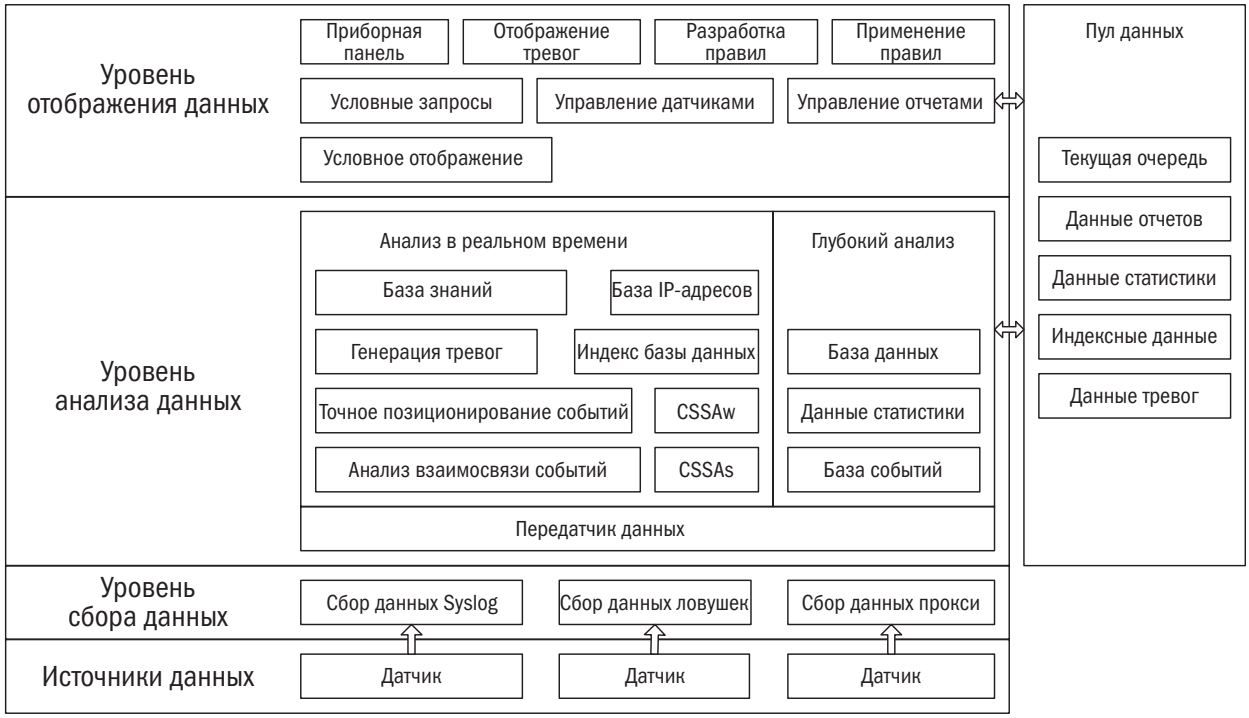

Рис. 11. Архитектура ПО ISS

алгоритмов, применяемых в модели CSSE, основаны на теории искусственного интеллекта, и можно добиться полной автоматической работы после предварительной настройки рабочих параметров.

Модель CSSE была реализована в системе мониторинга безопасности информационной сети SGCC для раннего предупреждения о возможных кибератаках, система работала стабильно на протяжении более трёх лет и сыграла важную роль в управлении рисками в киберпространстве.

Литература

1. Ernest Foo, Mark Branagan, Thomas Morris, «A proposed australian industrial control system security curriculum»[A], the 46th Hawaii International Conference on System Sciences (HICSS)[C], pp.1754–1762, 2013.

2. Piggin R.S.H. «Development of industrial cyber security standards: IEC 62443 for SCADA and industrial control system security»[A], IET Conference on Control and Automation 2013: Uniting Problems and Solutions, pp. 1–6, 2013.

3. Zhao Junhua, Wen Fushuan, Xue Yu-sheng, et al. «Cyber physical power systems: architecture, implementation techniques and challenges»[J], Automation of Electric Power Systems, vol. 34, no. 15, pp.1–7, 2010 (in Chinese).

4. Yu Yong, Lin Weimin, «General frameworks for the safety protection of the information system of power systems» [J], Netinfo Security, no. 9, pp.58–60, 2005 (in Chinese).

5. R. Dharam, S.G. Shiva, «Runtime monitors to detect and prevent union query based SQL injection attacks» [A], 10th International Conference on Information Technology [C], pp. 357–362, 2013.

6. Liu Lanchao, M. Esmalifalak, Han Zhu, «Detection of false data injection in power gridexploiting low rank and sparsity» [A], IEEE International Conference on Communications (ICC), pp. 4461–4465, 2013.

7. G. Jakobson, «Mission cyber security situation assessment using impact dependency graphs» [A], Proceeding of the 14th International Conference on Information Fusion (FUSION), pp.1–8, 2011.

8. Chen Xiuzhen, Zheng Qinghua, Guan Xiaohong. «Quantitative hierarchical threat evaluation model for network security» [J], Journal of Software, vol. 17, no. 4, pp.885–897, 2006 (in Chinese).

Xu Ruzhi, WANG Yufei. «A study on electric power information network-oriented security situation awareness,» Power System Technology, vol. 37, no. 1, pp. 53–57, 2013 (in Chinese).

9. Wang Yufei, Zhao Ting, Li Shaoyu, et al. «An intrusion detection method for electric power information network based on improved minimum enclosing ball vector machine» [J], Power System Technology, vol. 37, no. 9, pp. 2675–2680, 2013 (in Chinese).

10. Wang Yufei, Zhou Liang, Wang Jing. «Intrusion Detection System of Electric Power Information Network Based on Improved Ball Vector Machine» [A], The 4th International Conference on Intelligent System Design and Engineering Applications (ISDEA 4th) [C], pp. 369–373, 2013.

Li Yuancheng, Wang Yufei. «A misuse intrusion detection model based on hybrid classifier algorithm», JDCTA: International Journal of Digital Content Technology and its Applications, vol. 6, no. 5, pp. 25–33, 2012.

11. Gao Kunlun,Xu Ruzhi,Wang Yufei. «A hierarchical network security situation evaluation system for electric power enterprise based on grey clustering analysis» [C]. IEEE Conference Computer Science and Service System (CSSS), pp. 1990–1995, 2011.

12. Wang Yufei, Wang Jing, Xu Zhibo, et al. «Assessing Cyber-threats Situation for Electric Power Information Network» [A], The 9th International Conference on Natural Computation (ICNC'13) [C], pp. 1505–1510, 2013.

13. Gao Kunlun, Liu Jianming, Xu Ruzhi, et al. «A hybrid security situation prediction model for information nerwork based on support vector machine and particle swarm optimization», Power System Technology, vol. 35, no. 4, pp. 176–182, 2011 (in Chinese).

14. Zhang Xiang, Hu Changzhen, Liu Shenghang, et al. «Research on network attack situation forecast technique based on support vector machine» [J]. Computer Engineering, vol. 11, no. 3,pp. 10–12, 2007 (in Chinese).

15. Endsley M R. «Design and evaluation for situation awareness enhancement» [A]. Paper presented at the Human Factors Society 32nd Annual Meeting [C]. Santa Monica, CA, pp. 7–11, 1988.

16. D.F Crouse, P. Willett, Y. Bar-Shalom, «A low-complexity sliding-window Kalman FIR smoother for discrete-time model» [J], IEEE Signal Processing Letters, vol. 17, no. 2, pp.1 77–180, 2010.

17. Mallapragada P-K, Jin R, Jain A-K. «Semiboost: boosting for semi-supervised learning» [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 31, no. 11, pp. 2000–2014, 2009.

18. Weiming Hu, Wei Hu, Steve Maybank. «Adaboost-based algorithm for network intrusion detection» [J]. IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, vol. 38, no. 2, pp. 577–583, 2008.

19. Tsang I W H, Kwok J T Y, Zurda J A. «Generalized core vector machines», IEEE Transactions on Neural Networks, vol.1 7, no. 5, pp. 1126–1140, 2006.

20. Chung Fulai, Deng Zhaohong, Wang Shitong. «From minimum enclosing ball to fast fuzzy inference system training on large datasets», IEEE Transactions on Fuzzy Systems, vol. 17, no. 1, pp. 173–184, 2009.

Источник: «Study and Practice of Cybersecurity Situation Evaluation Method for Smart Grid», труды CIGRE 2014, http : //www.cigre.org