Нейросетевая идентификация элементов стохастической матрицы для моделирования процессов защиты информации

И. В. Котенко[1,2], И. Б. Паращук[2]
[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)
[2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО)
[1]ivkote@comsec.spb.ru, [2]parashchuk@comsec.spb.ru

***Аннотация*. Приводится алгоритм идентификации неполных и противоречивых знаний о поведении параметров процессов защиты информации путем использования нейросетевого преобразования. Идентификации подлежат элементы стохастической матрицы переходных вероятностей – главной составляющей модели процессов защиты. Использование предложенного нейросетевого алгоритма позволяет обеспечить учет неопределенности нестохастического характера, повысить достоверность моделирования и степень обоснованности принимаемых решений.**

Ключевые слова: процесс защиты информации; идентификация; нейронная сеть; алгоритм; матрица; когнитивная карта

I. Введение

Моделирование сложных процессов, в том числе и процессов защиты информации (ЗИ), требует большого числа знаний об этих процессах, причем знаний экспериментальных и экспертных. Особенно это актуально при современных угрозах безопасности, когда возможны сложные многошаговые атаки различных категорий нарушителей [1, 2]. Для обработки этих знаний в последнее время широко используются искусственные нейронные сети (ИНС). Доказано [3], что с помощью любой многослойной ИНС с двумя промежуточными слоями возможно с любой точностью аппроксимировать любую многомерную функцию на единичном отрезке.

Модели процессов ЗИ применяют в интересах оценивания эффективности их функционирования. Благодаря своим достоинствам, применение методов теории ИНС при построении моделей процессов ЗИ целесообразно и актуально. Это позволяет: использовать эти методы для описания элементов задач моделирования и оценивания качественных и количественных субъективных оценок, которые определяются с помощью весовых коэффициентов (синаптических весов) и весовых отношений; формализовать неточные (противоречивые) описания с помощью нейросетевых алгоритмов идентификации; автоматически накапливать эмпирические знания о свойствах объекта оценивания и принимать решения, опираясь на накопленные знания. При этом качество идентификации растет по мере увеличения объема накопленных знаний [3, 4].

Это исследование было поддержано грантами РФФИ (проекты № 18-07-01369 и 18-07-01488), бюджетом (проект № АААА-А16-116033110102-5) и Правительством Российской Федерации, грантом 074-U01.

II. Релевантные работы

Потенциальные приложения ИНС просматриваются в тех задачах идентификации [3, 4], когда в силу неопределенности, например, из-за неполноты и противоречивости информации, традиционные вероятностные и нечеткие методы идентификации неэффективны, а обычные вычисления непомерно трудоемки или же неадекватны решаемой задаче. Например, в работе [4] эти методы отличаются только уровнями неопределенности.

Многослойные ИНС находят применение и как идентификаторы состояния нелинейных объектов [5, 6], успешно конкурируя с традиционными линейными и нелинейными идентификаторами. Но они не гарантируют высокой точности идентификации. В статье [7] предложен подход, основанный на адаптивной фильтрации состояний процессов с использованием рекуррентных нейронных сетей. Однако такой подход требует рассмотрения вспомогательных параметров фильтрации, что не всегда возможно. В работе [8] изложен расширенный подход к нейрокомпьютингу. Но этот подход применим для идентификации и моделирования сложных квазистатических процессов, что сужает область применения. Работа [9] посвящена методу, который позволяет моделировать сложные процессы с использованием нейро-нечетких систем с нечеткими связями. Но этот подход очень сложный для математического моделирования и трудоемкий.

В нашем случае идентификация недостоверно заданных исходных данных для моделирования случайного процесса ЗИ представляет собой традиционную задачу. Это задача классификации значений исходных данных с помощью нейросетевого алгоритма. При этом в задачах классификации выходной элемент ИНС должен выдавать сильный сигнал в случае, если данное наблюдение принадлежит к интересующему нас классу, а слабый – в противоположном случае. Такая конструкция ИНС известна как дискриминантная функция

в задачах идентификации и распознавания показателей качества сети связи [10].

III. Теоретическая часть

Рассмотрим процедуру нейросетевой идентификации на примере определения значений элементов стохастической матрицы или матрицы переходных вероятностей (МПВ) для различных состояний параметра процесса ЗИ. Значения вероятностей переходов для неточно (противоречиво) заданных (сформулированных) состояний параметра ЗИ $\tilde{\Pi}(k, k+1, u)$ являются исходными данными для аналитического моделирования динамики смены состояний (ДСС) этого процесса. Описанию параметров процесса ЗИ присущ именно этот тип неопределенности [10]. Существуют работы [11, 12], посвященные синтезу математических моделей для дискретных по состоянию, но непрерывных по времени случайных процессов. Модели формулируются в виде разрывных марковских последовательностей в форме стохастических дифференциалов. Это позволяет выдвинуть гипотезу о том, что существует принципиальная возможность введения унифицированных моделей процесса ЗИ на основе управляемых цепей Маркова в форме разностных стохастических уравнений. За основу берем общую методологию моделирования ДСС *i*-го неточно (противоречиво) заданного параметра процесса ЗИ (например, для шести состояний). Тогда модель может быть представлена в виде уравнений состояния и наблюдения следующим образом:

$$\vec{Y}_i(k+1) = C^{\mathrm{T}}_{\vec{Y}_i}(k+1)\,\vec{\Theta}_{\vec{Y}_i}(k+1); \qquad (1)$$

$$\vec{\Theta}_{\vec{Y}_i}(k+1) = \tilde{\Pi}^{\mathrm{T}}_{\vec{Y}_i}(k, k+1, u)\,\vec{\Theta}_{\vec{Y}_i}(k) + \Delta\vec{\Theta}_{\vec{Y}_i}(k+1); \qquad (2)$$

$$\vec{Z}_{\vec{Y}_i}(k+1) = H_{\vec{Y}_i}(\vec{Y}_i(k+1))\,\vec{\Theta}_{\vec{Y}_i}(k+1) + \vec{\eta}_{\vec{Y}_i}(k+1), \qquad (3)$$

где $\vec{Y}_i(k+1)$ – вектор дискретных по времени и по состояниям неточно (противоречиво) заданных значений *i*-го параметра процесса ЗИ; $C_{\vec{Y}_i}(k+1)$ – *M*-мерная (в нашем случае $M = 6$) матрица-строка возможных неточно (противоречиво) сформулированных состояний *i*-го параметра процесса ЗИ; $\vec{\Theta}_{\vec{Y}_i}(k+1)$ – вспомогательный вектор-индикатор состояния *i*-го неточно (противоречиво) заданного параметра процесса защиты; $H_{\vec{Y}_i}(\vec{Y}_i(k+1))$ – шестимерная матрица неточных наблюдений за ДСС процесса ЗИ $\vec{Y}_i(k)$; $\Delta\vec{\Theta}_{\vec{Y}_i}(k+1)$ – вектор значений приращения индикаторов состояния параметра процесса ЗИ, $\vec{\Theta}_{\vec{Y}_i}(k)$ – значение вектора вспомогательных индикаторов состояния *i*-го неточно (противоречиво) заданного параметра на предыдущем шаге; $\vec{Z}_{\vec{Y}_i}(k+1)$ – вектор наблюдения за состоянием *i*-го неточно (противоречиво) заданного параметра процесса ЗИ; $\vec{\eta}_{\vec{Y}_i}(k+1)$ – вектор шумов наблюдения за ДСС *i*-го неточно (противоречиво) заданного параметра ЗИ; $\tilde{\Pi}_{\vec{Y}_i}(k, k+1, u)$ – матрица неточно (противоречиво) заданных одношаговых вероятностей перехода *i*-го неточно (противоречиво) заданного параметра из *k*-го в $(k+1)$ состояние, учитывающая внешние и управляющие воздействия $u(k)$.

Определение (идентификация) элементов матрицы переходных вероятностей (МПВ) $\tilde{\Pi}_{\vec{Y}_i}(k, k+1, u)$ составляет главную особенность разработки модели процесса ЗИ с неточно (противоречиво) заданными параметрами. Идентификация осуществляется с помощью нейросетевого алгоритма. Данный алгоритм предназначен для преобразования неточно (противоречиво) заданных исходных данных к виду, пригодному для использования в рамках процедур моделирования и фильтрации (экстраполяции). Он может быть реализован на основе комплексированной нейронной сети (КНС) – ИНС, в состав которой входят различные сети двух и более топологий. Теоретические аспекты процесса определения значений элементов МПВ с помощью нейросетевого алгоритма идентификации, например, для шести состояний *i*-го параметра ЗИ, имеют следующие особенности. В нейросетях типа КНС используются когнитивные карты для каждого из возможных состояний. Состояния задаются матрицами связей, имеющими (для шести состояний параметра процесса ЗИ) вид

$$V(k) = \begin{vmatrix} v_{11}(k) & v_{12}(k) & \dots & v_{16}(k) \\ v_{21}(k) & v_{22}(k) & \dots & v_{26}(k) \\ \vdots & \vdots & \ddots & \vdots \\ v_{61}(k) & v_{62}(k) & \dots & v_{66}(k) \end{vmatrix}. \qquad (4)$$

Матрицы формируются по входным векторам, характеризующим зависимость переходных вероятностей в строке МПВ. Они формируются в ходе первого этапа обучения КНС на основе мнений эксперта, поступающих на распределительный (входной) слой нейронной сети. При этом КНС имеет тип «СОКП-ДАП». Это тип двухслойной ИНС с прямым распространением информации – самоорганизующаяся карта признаков (СОКП), а также сеть с двунаправленной ассоциативной памятью (ДАП). В рамках нейросетевой идентификации элементов МПВ, каждый элемент $v_{ij}(k)$ данной матрицы характеризует одну строку МПВ (одно стартовое состояние). Он описывает взаимосвязь, корреляционную зависимость вероятностей перехода из данного состояния в другие, зависимость *i*-ой вероятности перехода и *j*-ой вероятности перехода на *k*-ом шаге процесса ЗИ.

IV. Экпериментальная часть

Рассмотрим формирование матрицы связей (весов) на конкретном примере. Для шести возможных состояний неточно (противоречиво) заданного параметра процесса ЗИ должны быть заданы шесть матриц весов. Если говорят о первой строке МПВ – идентифицируются вероятности перехода из первого состояния во второе, третье, четвертое, пятое, шестое и вероятность остаться в первом состоянии. Тогда вектор, характеризующий зависимость

переходных вероятностей в первой строке МПВ, по мнению 1 эксперта, может иметь вид

$$\vec{U}_1 = (1, 0, 1, -1, -1, 0).$$

Этот вектор является символьной записью выражения: «рост вероятности нахождения в первом состоянии и остаться в нем $\pi_{11}(k)$ приводит к повышению (доминированию) вероятности перехода из первого в третье состояние $\pi_{13}(k)$. По отношению к вероятности перехода из первого в четвертое и из первого в пятое состояния $\pi_{14}(k)$ и $\pi_{15}(k)$, по влиянию изменений вероятности перехода из первого во второе и из первого в шестое состояния $\pi_{12}(k)$ и $\pi_{16}(k)$ мнение эксперта отсутствует». Причем, если положительному значению элемента вектора $\vec{U}_1$, характеризующему повышение вероятности перехода соответствует положительное значение другого элемента вектора $\vec{U}_1$, то эту корреляционную связь между ними принимают положительной. Отрицательная связь существует, если положительному значению элемента вектора $\vec{U}_1$ соответствует отрицательное значение другого элемента вектора $\vec{U}_1$. Числовая характеристика взаимосвязи представляет собой сумму по модулю значений, характеризующих взаимосвязь переходных вероятностей в МПВ. В результате работы СОКП, в соответствии с вектором $\vec{U}_1$, получается когнитивная карта и соответствующая ей матрица связей (5).

$$V(k) = \begin{vmatrix} 0 & 0 & 2 & -2 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & -2 & -2 & 0 \\ -2 & 0 & -2 & 0 & 2 & 0 \\ -2 & 0 & -2 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{vmatrix}. \qquad (5)$$

Аналогичным образом формируются когнитивные карты и матрицы связей (весов) V_2, V_3, V_4, V_5, V_6 для пяти оставшихся строк МПВ. При этом когнитивные карты каждого эксперта могут быть естественным образом объединены в итоговую когнитивную карту. Она учитывает коллективное мнение всех привлекаемых экспертов о корреляционных зависимостях вероятностей перехода параметра ЗИ. Вычисляется в соответствии с выражением (6)

$$W_1(k) = \sum_{i=1}^{E} V_i(k), \qquad (6)$$

где $E = 6$ – количество экспертов (матриц связей), принимающих участие в установлении множества элементов МПВ и характера связей между ними. Так как эта матрица отражает противоречивые мнения всех экспертов о корреляционных зависимостях вероятностей перехода параметра ЗИ из состояния в состояние, то она содержит не только элементы 1 и –1, но и 0. Это позволяет более полно отражать причинно-следственные зависимости между концептами (состояниями параметра ЗИ). Аналогичным образом могут быть сформированы итоговые когнитивные карты и итоговые матрицы весов для остальных строк МПВ $\tilde{\Pi}(k, k+1, u)$.

Рассмотрим подробно алгоритм идентификации значений вероятностей перехода неточно (противоречиво) заданного параметра процесса ЗИ из состояния в состояние. Данный нейросетевой алгоритм идентификации предназначен для определения значений параметров моделирования и фильтрации (экстраполяции) в интересах оценивания эффективности, причем в условиях недостоверности информации, неполноты и противоречивости знаний о требованиях и состоянии ЗИ.

Нейросетевая идентификации на основе КНС происходит в следующей последовательности. Выполняется активизация входного слоя КНС входным образом, т.е. приведение нейронов входного слоя в начальные состояния. Происходит начальная инициализация нейронов второго слоя, затем приведение нейронов входного слоя КНС к состоянию нейронов второго слоя: $a_i = b_i$, $\forall i = \overline{1, 6}$. Потом вычисление новых состояний нейронов второго слоя для всех $i \in [1, \ldots, 6]$ по формуле:

$$b_i(k+1) = f\left(\sum_{j=1}^{5} b_i(k)\, w_{ij}(k)\right), \forall i = \overline{1, 6}, \qquad (7)$$

где f – ступенчатая функция активации. Затем повторение шагов 3 и 4 до тех пор, пока КНС не достигнет стабильного состояния. Проверка, достигла или не достигла КНС стабильного состояния осуществляется путем сравнения состояний нейронов второго слоя на предшествующем k-ом и очередном $(k + 1)$-ом шаге. При достижении КНС стабильного состояния, осуществляется суммирование значений весовых коэффициентов.

$$\vec{B}_{\Sigma}^{n} = \sum_{i=1}^{6} \vec{B}_i(f[b_i]). \qquad (8)$$

Элементы данного суммарного вектора характеризуют идентифицированные весовые коэффициенты корреляционной связи значений вероятностей переходов параметра ЗИ для одной n-ой строки МПВ. На их основе получается корреляционная суммарная матрица весов.

Следующим шагом идентификации является вычисление значений вероятностей перехода неточно (противоречиво) заданного параметра ЗИ из первого состояния во второе, третье, четвертое, пятое, шестое и вероятности остаться в первом состоянии. Данная процедура реализуется на основе квадратичной метрики, применяемой к смещенным значениям суммарных весовых коэффициентов. Заключительный шаг – повторение выполнения шагов алгоритма до тех пор, пока не будут идентифицированы элементы во всех остальных i-х строках МПВ. В соответствии с рассмотренным алгоритмом выходной вектор второго слоя на каждом k-ом шаге работы КНС последовательно принимает ряд значений состояний. Они определяются на основе выражения (7) и для нашего примера будут равны:

$$\vec{B}_1(1) = f([0,\ 0,\ 2,\ -6,\ 2,\ 0]) = [1,\ 0,\ 1,\ -1,\ 1,\ 0];$$

$$\vec{B}_1(2) = f([10,\ -4,\ 2,\ -4,\ -4,\ 4]) = [1,\ -1,\ 1,\ -1,\ -1,\ 1];$$

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

$$\vec{B}_1(5) = f([6,\ 10,\ 6,\ -20,\ -12,\ 10]) = [1,\ 1,\ 1,\ -1,\ -1,\ 1].$$

Видно, что КНС достигла стабильного состояния на четвертом шаге. Аналогичным образом получаем выходные векторы второго слоя КНС для входных образов: $\vec{C}(k) = [0,\ 1,\ 0,\ 0,\ 0,\ 0];\ \vec{C}(k) = [0,\ 0,\ 1,\ 0,\ 0,\ 0];\ \ldots$ $\vec{C}(k) = [0,\ 0,\ 0,\ 0,\ 0,\ 1].$ Данные входные образы характеризуют соответственно необходимость изменения корреляционных зависимостей между вероятностью нахождения в первом состоянии, и остаться в нем и вероятностями перехода из первого в третье, в четвертое, в пятое и в шестое состояния Выходные векторы второго слоя КНС для этих входных образов соответственно равны:

$$\vec{B}_2(4) = f([6,\ 10,\ 6,\ -20,\ -12,\ -10]) = [1,\ 1,\ 1,\ -1,\ -1,\ 1];$$

$$\vec{B}_3(5) = f([6,\ 10,\ 6,\ -20,\ -12,\ -10]) = [1,\ 1,\ 1,\ -1,\ -1,\ 1];$$

$$\vec{B}_4(3) = f([-6,\ -10,\ -6,\ 20,\ 12,\ -10]) = [-1,\ -1,\ -1,\ 1,\ 1,\ -1];$$

$$\vec{B}_5(4) = f([-6,\ -10,\ -6,\ 20,\ 12,\ -10]) = [-1,\ -1,\ -1,\ 1,\ 1,\ -1];$$

$$\vec{B}_6(4) = f([6,\ 10,\ 6,\ -20,\ -12,\ 10]) = [1,\ 1,\ 1,\ -1,\ -1,\ 1].$$

Полученные результаты характеризуют суммарную предпочтительность преобладания значений одной вероятности перехода параметра ЗИ из состояния в состояние, по отношению к другой. Суммарный вектор весовых коэффициентов имеет значения элементов

$$B_{\Sigma}^{1} = ([12,\ 20,\ 12,\ -40,\ -24,\ 20]).$$

Нормировка позволяет избавиться от отрицательных значений весов, но сохранить их пропорциональную зависимость. В итоге получим значения вероятностей перехода неточно (противоречиво) заданного параметра процесса ЗИ. Вероятности перехода из первого состояния во второе, третье, четвертое, пятое, шестое и вероятность остаться в первом состоянии, т.е. элементы первой строки МПВ $\widetilde{\Pi}(k,\ k+1,\ u)$:

$$\pi_{11}(k) = b_{11}^2 / (b_{11}^2 + b_{21}^2 + b_{31}^2 + b_{41}^2 + b_{51}^2 + b_{61}^2) = 0{,}211;$$

$$\pi_{12}(k) = b_{22}^2 / (b_{12}^2 + b_{22}^2 + b_{32}^2 + b_{42}^2 + b_{52}^2 + b_{62}^2) = 0{,}275;$$

$$\pi_{13}(k) = b_{33}^2 / (b_{13}^2 + b_{23}^2 + b_{33}^2 + b_{43}^2 + b_{53}^2 + b_{63}^2) = 0{,}211;$$

$$\pi_{14}(k) = b_{44}^2 / (b_{14}^2 + b_{24}^2 + b_{34}^2 + b_{44}^2 + b_{54}^2 + b_{64}^2) = 0{,}001;$$

$$\pi_{15}(k) = b_{55}^2 / (b_{15}^2 + b_{25}^2 + b_{35}^2 + b_{45}^2 + b_{55}^2 + b_{65}^2) = 0{,}027;$$

$$\pi_{16}(k) = b_{66}^2 / (b_{16}^2 + b_{26}^2 + b_{36}^2 + b_{46}^2 + b_{56}^2 + b_{66}^2) = 0{,}275.$$

Аналогичным образом могут быть идентифицированы остальные значения вероятностей перехода неточно (противоречиво) заданного параметра процесса ЗИ, т.е. элементы второй, третьей, четвертой, пятой и шестой строк МПВ $\widetilde{\Pi}(k,\ k+1,\ u)$.

V. Выводы

Таким образом, сформулирован подход к моделированию случайного процесса ЗИ с недостоверно (неточно и противоречиво) заданными параметрами. Подход основан на использовании систем модифицированных разностных уравнений состояния. При этом неточные, неполные и противоречивые знания о поведении некоторых параметров ЗИ путем использования нейросетевого алгоритма трансформируются в количественные значения элементов МПВ – одной из ключевых составляющих модели. Использование предложенного нейросетевого алгоритма позволяет учесть неопределенности нестохастического характера, присущие исходным данным процессов ЗИ. Это позволяет в интересах процедуры оценивания эффективности ЗИ повысить достоверность анализа и обоснованность принимаемых решений.

Список литературы

[1] Kotenko I.V. Active Vulnerability Assessment of Computer Networks by Simulation of Complex Remote Attacks // Proceedings of the International Conference on Computer Networks and Mobile Computing. ICCNMC-03 (IEEE Computer Society), 2003. pp. 40-47.

[2] Kotenko I.V., Chechulin A.A. Common Framework for Attack Modeling and Security Evaluation in SIEM Systems // Proceedings of the 2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing (California: IEEE Computer Society), 2012. pp. 94-101.

[3] Kosko B. Neural Networks and Fuzzy Systems. A Dynamical Systems Approach to Machine Intelligence. Englewood Cliffs: Prentice-Hall, 1992. 346 p.

[4] Kriesel D. A Brief Introduction to Neural Networks. Cambridge: Cambridge Press, 2010. 226 p.

[5] Rojas R. Neural Networks. Berlin: Springer-Verlag, 1996. 453 p.

[6] Muller B., Reinhardt J., Strickland M.T. Neural networks: an introduction. Springer, 1995. 306 p.

[7] Parlos A.G., Menon S.K., Atiya A.F. An algorithmic approach to adaptive state filtering using recurrent neural networks // IEEE Trans. Neural Networks. 2001. Vol.12. No 6. pp. 1411-1432.

[8] Anderson J.A., Rosenfeld E. Neurocomputing: Foundation of Research, Cambridge, Mass: MIT Press, 1988. 267 p.

[9] Nesteruk G.Ph., Kupriyanov M.C. Neural-fuzzy systems with fuzzy links // Proc. of the VI-th Int. Conference SCM'2003. St.Pb: StPSETU «LETI», 2003. v. 1. pp. 341-344.

[10] Parashchuk I.B. System Formation Algorithm of Communication Network Quality Factors using Artificial Neural Networks // 1st IEEE International Conference on Circuits and System for Communications (ICCSC'02). St. Pb: SPbGTU, 2002. pp. 263-266.

[11] Stewart N.E., Thomas G.K. Markov processes // Probability and Mathematical Statistics. John Wiley & Sons Inc., New York, 1986. pp. 214-234.

[12] Bini D., Latouche G., Meini B. Numerical Methods for Structured Markov Chains. Oxford University Press, New York, 2005. 215 p.