УДК 004.891.3

ИММУННЫЙ АЛГОРИТМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ УПРАВЛЕНИИ СЛОЖНЫМИ СИСТЕМАМИ

В.И. Васильев
Уфимский государственный авиационный технический университет
Россия, 450008, Уфа, Карла Маркса ул., 12
E-mail: vasilyev@ugatu.ac.ru

А.Е. Сулавко
Омский государственный технический университет
Россия, 644050, Омск, Пр. Мира, д. 11
E-mail: sulavich@mail.ru

Е.В. Шалина
Омский государственный университет путей сообщения
Россия, 644050, Омск, Пр. Мира, д. 11
E-mail: burka-777@yandex.ru

Ключевые слова: искусственные иммунные системы, система поддержки принятия решений, детектор, коррелирующие данные.

Аннотация: В данной работе рассматривается система поддержки принятия решений для обеспечения информационной безопасности автоматизированных систем управления. Предложен вариант ее построения на основе аппарата искусственных иммунных систем. Интеллектуальный анализ данных производится системой детекторов, которые ориентированы на обработку сильно или слабо коррелирующих данных. Рассмотрены ключевые параметры искусственной иммунной системы и связь между ними.

1. Введение

Сегодня автоматизированные системы управления получили широкое применение в различных областях, выйдя за рамки крупного производства. Для любого предприятия или организации повышение эффективности зависит от выполнения требований надежности систем автоматизации, поскольку современные автоматизированные системы управляют сложными и опасными технологическими процессами, сбой в которых может привести к авариям на производстве или техногенным катастрофам [1].

Задачи обеспечения информационной безопасности для вышеописанных систем управления обладают следующими свойствами: разнотипные переменные (вещественные, целочисленные, булевы), наличие многих моделей для описания управляемых объектов, многокритериальность [2] и т.п. Модели решения таких задач являются довольно сложными с точки зрения их алгоритмического описания. Они содержат в себе алгоритмы обработки нечеткой информации, алгоритмы, которые «отсеивают» заведомо «плохие» варианты решения.

В качестве технологического исполнения вышеупомянутых алгоритмов обычно предлагается использовать аппарат искусственных нейронных сетей, как например в [1]. Но последние обладают рядом недостатков. Например, искусственные нейронные сети, обучаемые с помощью алгоритма обратного распространения ошибки, теряют устойчивость при усложнении своей структуры, и объем обучающей выборки возрастает. Появляются «ложные» локальные максимумы качества [3]. Многослойные нейронные сети (в том числе, сети «глубокого обучения», сверточные нейронные сети) требуют огромный объем обучающей выборки, что затрудняет их использование в тех приложениях, где объем обучающей выборки ограничен [4]. В отличие от вышеперечисленных методов, искусственные иммунные системы (ИИС) способны обучаться на выборках небольшого объема. Вычислительные элементы ИИС направлены на поддержание разнообразия, а сеть, построенная на базе ИИС, не теряет своей устойчивости даже при значительном наращивании своей структуры.

Поэтому для решения задач обеспечения ИБ в данной работе предлагается использование системы поддержки принятия решений (СППР) на базе аппарата искусственных иммунных систем.

2. Иммунный алгоритм поддержки принятия решений

2.1. Система поддержки принятия решений

Система поддержки принятия решений (Decision Support System, DSS) – это компьютерная автоматизированная система, целью которой является помощь лицам, принимающим решение (ЛПР), в сложных условиях для полного и объективного анализа предметной деятельности [1]. Архитектура СППР напрямую зависит от данных и знаний, используемых системой для принятия решений, от вида решаемых задач, а также от квалификации пользователя системы.

После поступления входных данных СППР вырабатывает сценарий реагирования, соответствующий ситуации. В конечном счете ЛПР решает использовать этот сценарий или нет.

В результате анализа процессов обеспечения ИБ можно выделить следующие основные задачи по обеспечению ИБ, решаемые с помощью СППР:

– накопление и систематизация информации об ИБ процесса;

– оценка риска при реализации угрозы ИБ;

– помощь в выработке рекомендаций для минимизации возможных рисков ИБ.

На вход СППР могут поступать как количественные, так и качественные показатели, то есть появляется неопределенность в принятии решений по оценке рисков. В данной статье для определения уровня риска ИБ предлагается использовать технологию интеллектуального анализа данных, а именно искусственные иммунные алгоритмы. Общая архитектура СППР по обеспечению ИБ представлена на рис. 1.

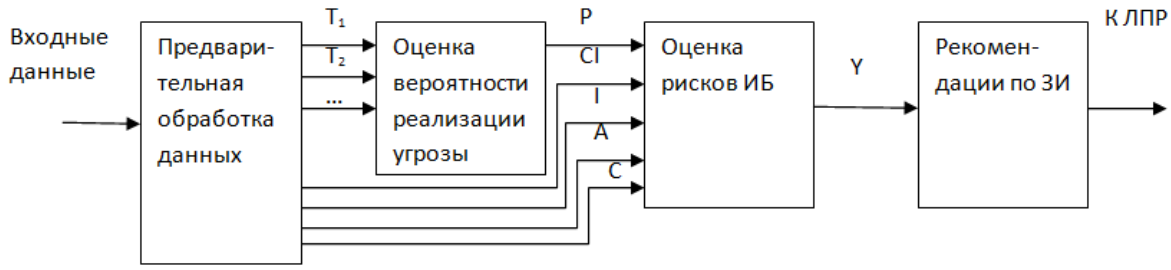

Рис. 1. Архитектура СППР.

Модуль предварительной обработки данных приводит входные величины к единому масштабу. На входы блока, реализующего искусственный иммунный алгоритм, подаются показатели выявленных уязвимостей ИБ (T_1,T_2, т.д.), с помощью которых определяется вероятность реализации угрозы P. Далее, для расчета оценки рисков(Y) используется формула:

$$Y = P * (C + I + A) * CI,$$

где CI – показатель ценности информации, содержащейся в системе, C,I,A – степень возможного ущерба при нарушении конфиденциальности, целостности и доступности, соответственно. Далее, на основе полученного значения Y, формируются рекомендации для ЛПР по достижению желаемого уровнем безопасности системы.

2.2. Алгоритм искусственной иммунной системы

Для понимания работы блока СППР, реализующего искусственный иммунный алгоритм, необходимо обратиться к принципам работы естественной иммунной системы.

В вышеупомянутой системе выявляемые чужеродные клетки служат сигналом для активации защитного механизма. Обнаружение антигена (вещества, которое организм рассматривает как чужеродное или потенциально опасное) в организме влечет за собой размножение лимфоцитов, которое приводит к образованию клонов идентичных клеток (антител, обеспечивающих иммунный ответ). В ИИС каждое антитело и антиген представлены набором атрибутов, в виде двоичного кода или точки в многомерном пространстве. Аналогом антигена будет являться значение определенного показателя системы (характеризующего тот или иной процесс), либо совокупность значений нескольких признаков (в зависимости от подхода). В иммунной системе за обнаружение антигенов отвечают Т-лимфоциты. Т-клетки проходят отрицательный отбор: клетки, вступившие в реакцию с собственными белками, уничтожаются, а остальные (не образующие с ними связей) пополняют иммунную систему: циркулируют по всему организму и выполняют функцию защиты от чужеродных антигенов. Аналоги данных клетки в ИИС называют детекторами (или узлами), для формирования совокупности эффективных детекторов ИИС необходимо обучить.

На этапе обучения ИИС, ЛПР вводит несколько обучающих примеров нормальной работы системы (шаблонов). Также на этом этапе требуется выборка примеров работы системы при возникновении угроз и уязвимостей ИБ. Далее каждый из вышеперечисленных примеров преобразуется в вектор значений показателей работы системы (далее, показателей) [1]. Алгоритм создания и обучения ИИС– это цикл из некоторого количества итераций. Количество итераций I может быть задано явно, также могут быть предусмотрены условия досрочного завершения цикла обучения. Каждая итерация алгоритма состоит из следующих шагов [5]:

a) Расчет матрицы [R] парных коэффициентов корреляции $r_{j,t}$ между показателями шаблонов, j и t – номера показателей.

b) Генерируется N различных детекторов $D_i=\{m,A_i,R_i,y=f_i(\bar{a}_i)\}$,где A_i и R_i – множества показателей, обрабатываемых детектором, и коэффициентов корреляции между ними, y – аффинность (мера схожести) между детектором и антигеном $\bar{a}_i$, представляющим собой вектор из m показателей, извлеченных из шаблона. По сути A_i и R_i образуют граф, определяющий интерфейс взаимодействия детектора и антигенов (каждый i-й детектор анализирует только определенные сочетания m показателей из n имеющихся в векторе). Для каждого детектора случайным образом выбирается функционал $y=f(\bar{a}_i)$. Число m и сами показатели, которые анализирует детектор, тоже выбираются случайно (m>1), но со следующими граничными условиями: парные коэффициенты корреляции между показателями должны быть локализованы в некотором интервале$[r_{i,min};r_{i,max}]$. Границы интервала задаются, исходя из типа функционала детектора(подходит ли он для обработки сильно или слабо коррелирующих данных). Также вводится параметр r_{border}, который определяет граничный уровень корреляции по модулю, отделяющий условно независимые признаки($r<r_{border},r\epsilon R_i$) от явно коррелированных между собой($r>r_{border},r\epsilon R_i$). Известно множество функционалов, например, для обработки зависимых данных($r_{border}<r_{i,min},r_{border}<r_{i,max},r_{border}\geq 0.3$) подходят многомерный разностный функционал Байеса [6] или гравитационная мера [7], для слабозависимых ($r_{border}>r_{i,min},r_{border}>r_{i,max},r_{border}\leq 0.7$) – мера Пирсона [8]. Граница r_{border} может меняться от итерации к итерации цикла для большего разброса вариаций генерируемых детекторов, но ее целесообразно держать в пределе $0.3\leq r_{border}\leq 0.7$.

c) Детекторы настраиваются так, чтобы не реагировать на шаблоны. Для каждого из них выставляется порог τ_i, равный максимальному $y=f_i(\bar{a}_i)$ среди множества вычисленных значений $Yc_i=\{y_{i,1},y_{i,2},\ldots,y_{i,k},\ldots,y_{i,Kc}\}$ функционала i-го детектора для всех шаблонов(k–номер обучающего примера). Далее на вход детекторов поступают векторы, описывающие появления угрозы/уязвимости в системе, для них рассчитываются аналогичные величины $Yч_i=\{y_{i,1},y_{i,2},\ldots,y_{i,k},\ldots,y_{i,Kч}\}$. Детектор реагирует на k-й вектор, если преодолевается порог его функционала ($u_{i,k}$=1,если$y_{i,k}>y_{i,max}$,иначе$u_{i,k}$=0). По данным $u_{i,k}$ строится табл.1. Из данной таблицы можно понять, какие детекторы являются слабыми (малоэффективными, по минимуму $\hat{u}_i$) и какие векторы имеют наивысшую близость к шаблонам(по максимуму $\hat{y}_k$). Иммунная стратегия преследует цели поддержания разнообразия, поэтому нужно избавляться от детекторов, которые дают схожие результаты, начиная с самых слабых. В качестве меры аффинности между детекторами можно использовать операцию XOR по отношению к парам векторов $\bar{u}_i=\{u_{i,1},u_{i,2},\ldots,u_{i,k},\ldots,u_{i,Kч}\}$. Если аффинность между парой детекторов превышает порог $Tcor$, они считаются схожими, и детектор с меньшим значением $\hat{u}$ удаляется.

d) Проверяется условие завершения обучения (например, наличие заданного остаточного числа детекторов или прохождение определенного количества итераций). Если условие не выполнено производится случайное изменение («мутация») параметра r_{border} и переход на шаг2. Если условие выполнено, цикл обучения может быть завершен либо продолжен, но с условием повышения u_{min} или снижения $Tcor$ для достижения более высокого качества обучения. В первом случае ИИС будет стремиться выработать более сильную популяцию при аналогичном разнообразии детекторов, во втором –достигнуть большего разнообразия детекторов при схожих показателях их силы.

Таблица 1. Определение эффективности детекторов.

$u_{1,1}$	$u_{2,1}$	$u_{i,1}$	$u_{N,1}$	$\hat{y}_1=\Sigma_{i=1}^{N}u_{i,1}$
…	…	…	…	…
$u_{1,k}$	$u_{2,k}$	$u_{i,k}$	$u_{N,k}$	$\hat{y}_k=\Sigma_{i=1}^{N}u_{i,k}$
…	…	…	…	…
$u_{1,Kч}$	$u_{2,Kч}$	$u_{i,Kч}$	$u_{N,Kч}$	$\hat{y}_{Kч}=\Sigma_{i=1}^{N}u_{i,Kч}$
$\hat{u}_1=\Sigma_{k=1}^{Kч}u_{1,k}$	$\hat{u}_2=\Sigma_{k=1}^{Kч}u_{2,k}$	$\hat{u}_i=\Sigma_{k=1}^{Kч}u_{i,k}$	$\hat{u}_N=\Sigma_{k=1}^{Kч}u_{N,k}$	

Можно запоминать неудачные конфигурации детекторов и учитывать их при генерации новых (чтобы не тратить время на обучение заведомо слабых детекторов).

Процесс распознавания шаблонов заключается в голосовании детекторов –«за» и «против». В простейшем случае решения детекторов можно усреднить и получить аналог вероятности. Однако алгоритм можно модифицировать, отказавшись от бинарных выходов детекторов и используя непрерывную шкалу реагирования в интервале [0; 1]. Тогда в качестве меры аффинности между детекторами необходимо использовать коэффициент корреляции Пирсона. Непрерывные выходы можно воспринимать как условные вероятности, которые легко преобразуются в апостериорную вероятность с помощью формулы гипотез Байеса [9].Апостериорная вероятность характеризует наличие (или отсутствие) угрозы (всего предусматривается 2 гипотезы).

Многомерный функционал наибольшего правдоподобия Байеса (МФНПБ) для случая 2-х гипотез (отсутствие и наличие угрозы в данный момент) можно представить в виде:

$$P_h(\bar{a}) = \frac{0{,}5\prod_{j=1}^{N} p_h(a_j)}{\sum_{i=1}^{\Gamma}(0{,}5\prod_{j=1}^{N} p_i(a_j))} = \frac{\prod_{j=1}^{N} p_h(a_j)}{\sum_{i=1}^{\Gamma}\prod_{j=1}^{N} p_i(a_j)},$$

где $p_h(a_j)$ – условная вероятность h-й гипотезы, равная выходу j-го детектора, Г – количество гипотез, в данном случае Г=2. Решение в пользу h-й гипотезы принимается по максимальной апостериорной вероятности $P_h(\bar{a})$. Априорные вероятности можно считать равными (по 0,5), если нет статистических данных относительно частоты появления угроз.

Параметры N (количество детекторов), $Tcor$ (допустимая схожесть детекторов) и u_{min} (минимальная сила детекторов) связаны между собой и являются ключевыми для ИИС. Каждый параметр в той или иной степени влияет на качество обучения ИИС. Надежность решений ИИС становится выше, при увеличении N и u_{min}, а также при уменьшении $Tcor$.

3. Заключение

Предлагаемый вариант построения СППР на базе аппарата ИИС обладает рядом существенных отличий:

а) Алгоритм циклического обучения ИИС с каждой итерацией может работать все лучше, но не хуже. Если недостаточно данных для того, чтобы сделать достоверный вывод о состоянии автоматизированной системы управления, ИИС привлекает новые вычислительные ресурсы и начинает искать другие пути решения. Новые сгенерированные детекторы при этом остаются в базе ИИС, что является элементом обучения в процессе работы, не смотря на то, что исходная обучающая выборка остается неизменной.

b) ИИС обладает свойством двойной пластичности, позволяющим относительно легко изменять в процессе функционирования не только собственные параметры, но и структуру. Это выгодно выделяет ИИС на фоне других методов искусственного интеллекта (в частности ИНС, которые сложно масштабировать) и определяет перспективы их использования в таких сложных системах как автоматизированные системы управления на производстве.

Список литературы

1. Васильев В.И., Гвоздев В.Е., Гузаиров М.Б., Кириллова А.Д. Система поддержки принятия решений по обеспечению информационной безопасности автоматизированной системы управления технологическими процессами // Информация и безопасность. 2017. Т. 20. № 4 (4). С. 618-623.
2. Семенкина М.Е. Самоадаптивные эволюционные алгоритмы проектирования информационных технологий интеллектуального анализа данных // Искусственный интеллект и принятие решений. 2013. № 1. С. 13-23.
3. Ложников П.С. Биометрическая защита гибридного документооборота. Новосибирск: СО РАН, 2017. 130 с.
4. Иванов А.И., Ложников П.С., Сулавко А.Е. Оценка надежности верификации автографа на основе искусственных нейронных сетей, сетей многомерных функционалов Байеса и сетей квадратичных форм // Компьютерная оптика. 2017. Т. 41, № 5. С. 765-774.
5. Сулавко А.Е., ШалинаЕ.В., Стадников Д.Г. Биометрическая аутентификация по клавиатурному почерку на основе иммунного алгоритма распознавания образов // II Всероссийская научно-практическая конференция с международным участием им. В.В. Губарева. Интеллектуальный анализ сигналов, данных и знаний: методы и средства. 11-13 декабря 2018, Новосибирск.
6. Ivanov A.I., Lozhnikov P.S., Vyatchanin S.E.. Comparable Estimation of Network Power for Chisquared Pearson Functional Networks and Bayes Hyperbolic Functional Networks while Processing Biometric Data// Control and Communications (SIBCON). 29-30 June 2017, Astana, Kazakhstan. P. 1-3.
7. Sulavko A E, Zhumazhanova S S. Biometric pattern recognition using wide networks of gravity proximity measures // IOP Conf. Series: Journal of Physics: Conf. Series. II International scientific conference "Mechanical Science and Technology Update", 27-28 February 2018. Omsk, Russia. P. 1-13.
8. Lozhnikov P.S., Sulavko A.E. Usage of quadratic form networks for users' recognition by dynamic biometric images // XI International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines" (Dynamics). 14-16 November, 2017, Omsk, Russia. P. 1-6.
9. Vasilyev V.I., Sulavko A.E., Eremenko A.V., Zhumazhanova S.S. Identification potential capacity of typical hardware or the purpose of hidden recognition of computer network users // X International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines" (Dynamics). 15-17 November, 2016, Omsk, Russia. P. 1-5. DOI: 10.1109/Dynamics.2016.