УДК 004.032.26

И.Л. Каширина, К.А. Федутинов

ПРИМЕНЕНИЕ СЕТИ FUZZY ARTMAP В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Воронежский государственный университет, Воронеж, Россия

В статье рассмотрены вопросы организации интеллектуальных систем обнаружения и диагностики вторжений. Исследования в области разработки инструментов обеспечения информационной безопасности показывают, что на сегодняшний день наиболее перспективные и гибкие решения базируются на методах машинного обучения, позволяющих предотвратить ущерб от вторжений, не замеченных стандартными средствами борьбы с компьютерными атаками. В предлагаемом подходе предлагается использовать последовательный обратный поиск с возвращением для отбора значимых признаков и нейронную сеть Fuzzy ARTMAP для обнаружения и диагностики атак. Сеть Fuzzy ARTMAP способна адаптироваться к динамике компьютерных атак и позволяет распознавать вторжения в информационные систему в режиме реального времени, при этом не нужно подгружать наборы данных пакетно. Это дает возможность автоматизировать анализ протоколов безопасности в непрерывном режиме. Широкие возможности использования сетей семейства ART в задачах обнаружения вторжений позволяют считать актуальным поиск подходов, позволяющих улучшить их эксплуатационные характеристики. В данной статье управляющие гиперпараметры для сети Fuzzy ARTMAP предлагается настраивать в автоматическом режиме с использованием генетического алгоритма. По результатам вычислительного эксперимента редуцированный набор признаков уменьшает время вычислений на 41%. Точность алгоритма классификации составила 100% и 99,89% для стадии обнаружения и стадии диагностики соответственно.

Ключевые слова: нейронная сеть, Fuzzy ARTMAP, генетический алгоритм, обнаружение вторжений, интеллектуальные системы защиты информации.

1. Введение

Сетевые компьютерные системы глубоко интегрированы во все процессы современного информационного общества. Эффективное осуществление государственных и коммерческих сделок и услуг или последовательное упрощение социальных коммуникаций между миллиардами пользователей, зависят от крупных сетевых компьютерных систем. Возрастающая зависимость компаний и государственных учреждений от компьютерных сетей усилила важность защиты этих систем от внешних атак. Однократное вторжение в компьютерную сеть организации может привести к потере, несанкционированному использованию или модификации больших объемов данных.

Вторжение — это несанкционированный доступ или использование ресурсов компьютерной системы. Системы обнаружения вторжений

(Intrusion Detection System – IDS) – это программное обеспечение, которое обнаруживает, идентифицирует и реагирует на несанкционированные или аномальные действия. Основным элементом архитектуры IDS является подсистема анализа, предназначенная для выявления атак и подозрительных действий на основе данных сенсоров. Д. Деннинг представила первую модель IDS, сформировавшую основу для большинства современных систем, еще в 1986 году. [1] Эта модель использовала статистические методы для обнаружения вторжений и называлась IDES. Большинство разработанных позднее систем обнаружения вторжений использовало подходы, основанные на правилах, но в таких системах затруднено обнаружение новых атак. В последние годы акцент был перенесен на использование алгоритмов машинного обучения, основанных на методах интеллектуального анализа данных. Анализ математических методов и алгоритмов исследования защищенности информационных систем, показывает, что интеллектуальные методы машинного обучения, базирующиеся на качественном статистическом материале, являются эффективным, прошедшим хорошую апробацию, инструментом обеспечения безопасности информационных и компьютерных систем. На сегодняшний день индустрия кибербезопасности вкладывает значительные средства в машинное обучение в надежде достичь динамичного сдерживания роста угроз. По прогнозам некоторых аналитиков машинное обучение в течение ближайших пяти лет вытеснит большую часть традиционных антивирусов и систем на основе сигнатур [2].

Широкое распространение для решения задачи обнаружения вторжений на данный момент получили нейронные сети [3]. В данной статье предлагается для решения этой задачи использовать нейронную сеть Fuzzy ARTMAP. Основным преимуществом, присущим сети Fuzzy ARTMAP, и отличающим ее от других нечетких алгоритмов распознавания образов, является то, что она анализирует данные в режиме онлайн, а не выполняет автономную оптимизацию некоторого целевого критерия.

Современные системы обнаружения вторжений используют большое число различных входных признаков. Однако некоторые из признаков могут быть избыточными или незначительно влиять на эффективность обнаружения. Поэтому важной задачей является выявление значимых входных признаков при построении системы обнаружения вторжений, эффективной с вычислительной точки зрения. Для отыскания оптимального подмножества признаков в данной статье предлагается использовать алгоритм последовательного обратного поиска с

возвращением.

2. Материалы и методы

2.1. Отбор признаков.

В сложных алгоритмах классификации некоторые признаки могут быть избыточными, поскольку информация, которую они добавляют, уже содержится в других признаках. Избыточные признаки увеличивают время вычислений и могут повлиять на точность алгоритма. Методы отбора признаков улучшают классификацию путем поиска такого подмножества признаков, которое обеспечивает наиболее высокую точность классификации. В данной статье для отыскания подмножества наиболее значимых признаков используется алгоритм последовательного обратного поиска с возвращением.

При реализации данного алгоритма точность метода классификации на основе сети Fuzzy ARTMAP определяется как $W = R_{acc}(S_w)$, где S_w является рассматриваемым подмножеством признаков, а R_{acc} определяется как:

$$R_{acc}(S_w) = \frac{1}{C}\sum_{j=1}^{C}[y_i = \bar{y}_i], \qquad (1)$$

где C - количество примеров в обучающей выборке,

y_i – класс, предсказанный Fuzzy ARTMAP при использовании входного набора S_w, $\bar{y}_i$ – правильный класс. При этом выражение $[y_i = \bar{y}_i] = 1$, если $y_i = \bar{y}_i$ и $[y_i = \bar{y}_i] = 0$, если $y_i \neq \bar{y}_i$.

Подмножество признаков, которому соответствует максимальное значение W, является наиболее значимым. Последовательный обратный поиск с возвращением основан на двух известных алгоритмах отбора признаков: последовательном обратном поиске (SBS) и последовательном прямом поиске (SFS), где SBS исключает наименее важные признаки по одному, а SFS добавляет наиболее важные признаки по одному.

Наименее важным для рассматриваемого подмножества признаков S_w называют такой признак f_x , что

$$R_{acc}(S_w - f_x) > R_{acc}(S_w - f_i), \quad (f_i \in S_w, f_i \neq f_x) \qquad (2)$$

Алгоритм SBS удаляет наименее важные признаки из исходного множества признаков S до тех пор, пока количество признаков не достигнет изначально заданного числа $к$.

Наиболее важным для рассматриваемого подмножества признаков S_w называют такой признак $f_x \in S_u$, где $S_u = S - S_w$, и при этом

$$R_{acc}(S_w + f_x) > R_{acc}(S_w + f_i),\ (f_i \in S_u, f_i \neq f_x) \qquad (3)$$

Здесь $S_w \pm f_x$ означает, что f_x удаляется или добавляется в S_w.

Алгоритм SFS добавляет (начиная с пустого множества) наиболее важные признаки до тех пор, пока количество признаков не достигнет изначально заданного числа *k*.

Алгоритмы SBS и SFS относятся к классу так называемых “жадных алгоритмов”. Как известно, жадные алгоритмы иногда могут находить решения, далекие от оптимальных. Например, это может произойти, если есть два признака, каждый из которых по отдельности не показывает высокого прироста точности классификации Fuzzy ARTMAP (и они не будут отобраны), но их комбинация максимизирует величину W. Поэтому более перспективным представляется использование алгоритма последовательного обратного поиска с возвращением, который можно описать следующим образом.

Шаг 1. Инициализация.
Задается максимально допустимое количество признаков *k*.
Шаг 2. Исключение.
Используется базовый метод SBS для удаления признаков.
Шаг 3. Условное включение.
Ищется наиболее значимый признак среди исключенных признаков, и добавляется к текущему подмножеству. Процедура условного включения продолжается до тех пор, пока R_{acc} с включением очередного признака монотонно увеличивается.
Шаг 4: Отображение.
Если количество признаков в текущем подмножестве больше *k*, переход к шагу 2; в противном случае подмножество признаков найдено.

2.2. Сеть Fuzzy ARTMAP.

Теория адаптивного резонанса (*ART)* описывает семейство нейронных сетей, способных генерировать устойчивые кластеры путем самоорганизации в ответ на произвольные последовательности входных образов. Создавая кластеры динамически при обработке различных входных сигналов, сети семейства ART способны регулировать их размер и количество в зависимости от сложности и комплексности поступающего набора данных. В данной статье предлагается общий подход к решению

задач обнаружения вторжений с помощью сетей *Fuzzy ARTMAP*[6].

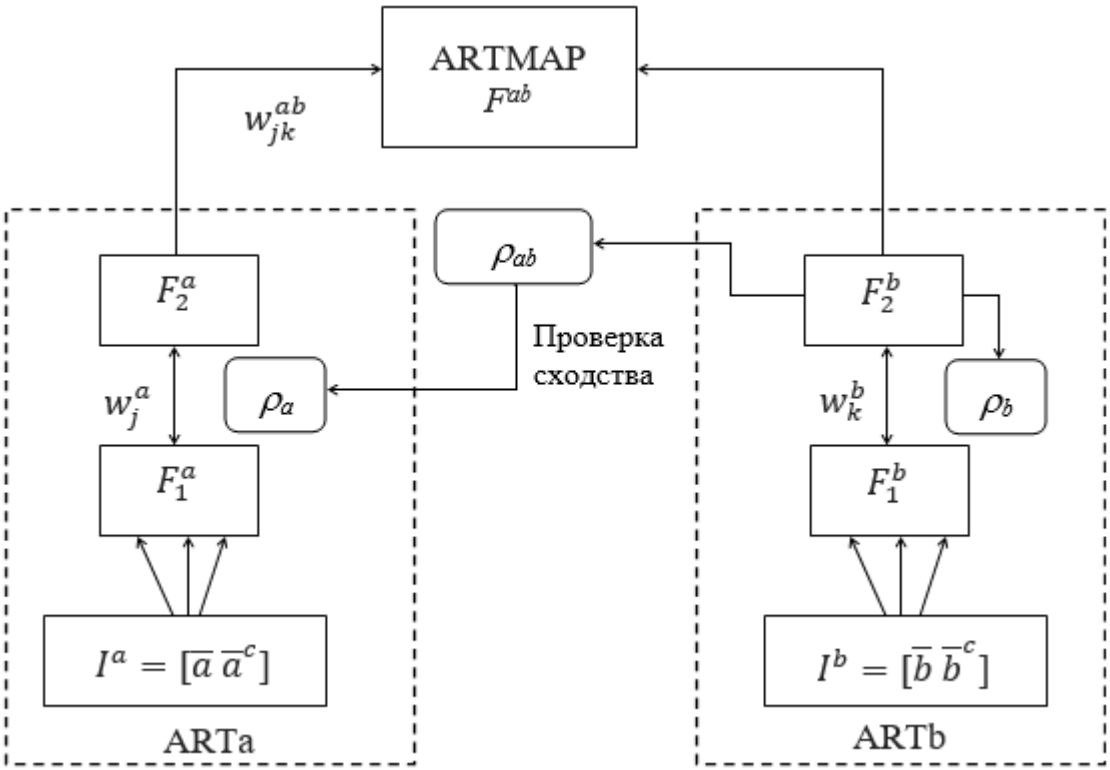

Рисунок 1 - Архитектура сети Fuzzy ARTMAP

Fuzzy ARTMAP опирается на архитектуру сети Fuzzy APT, использующей вычисления на основе нечеткой логики, однако, в отличие от Fuzzy APT, Fuzzy ARTMAP обучается с учителем. Fuzzy ARTMAP состоит из двух модулей Fuzzy APT: ARTa и ARTb, объединенных с использованием модуля ассоциативной памяти, как показано на Рисунке 1.

Fuzzy ARTMAP имеет внутренний контроллер, который обеспечивает автономную работу системы в режиме реального времени. Модуль F^{ab} представляет собой механизм саморегулирования с проверкой сходства, целью которого является максимизация обобщения и минимизация ошибки сети. Размер слоя F_1^a совпадает с размерностью входного вектора. Число нейронов в слое F_2^a совпадает с числом имеющихся на данный момент категорий (кластеров) и может увеличиваться в процессе обучения. Слои F_1^a и F_2^a связаны между собой весовой матрицей $W^a = (w_{ij}^a)$, при этом вектор $w_j^a,\ j = 1..l,$ представляет собой

прототип кластера с номером j. Слои F_1^b и F_2^b имеют аналогичный смысл, но при этом используются для кластеризации выходов. Слой F_2^a соединен с модулем F^{ab} бинарной весовой матрицей $W^{ab} = (w_{jk}^{ab}), j = 1..l;\ k = 1..n$. Здесь l – количество входных, n – количество выходных кластеров. Элемент $w_{jk}^{ab} = 1$, если входной кластер j соответствует выходному кластеру k. Таким образом, в сети Fuzzy ARTMAP может быть несколько выходных нейронов, соответствующих одному и тому же входному кластеру и наоборот. Это сделано для того, чтобы можно было хранить несколько вариаций входных и выходных образов одного класса, что повышает способность сети к обобщению. Упрощенно работу сети Fuzzy ARTMAP можно описать следующим образом: в процессе обучения сеть кластеризует не только входные, но и выходные векторы. При этом обучение проводится с учителем, но в процессе этого обучения устанавливается соответствие не только между определенными входными и выходными векторами, но и между кластерами входов и выходов. Таким образом, несмотря на механизм обучения с учителем, сети Fuzzy ARTMAP удается решать проблему стабильности – пластичности: с одной стороны, сеть сохраняет накопленные знания, с другой стороны, позволяет корректировать знания в процессе обучения, аккумулируя опыт экспертов в сфере информационной безопасности в структуре сформированных кластеров.

Работу сети Fuzzy ARTMAP можно описать в терминах обобщенной модели функционирования сетей семейства ART, представленной в [8]. Кратко общие этапы работы сетей этого семейства имеют следующий вид.

Этап 1. Инициализация сети и её параметров**.**

Этап 2. Препроцессинг (педобработка) входных векторов.

Этап 3. Выбор категории кластеризации (с использованием функции выбора) - первичная оценка входного вектора при помощи некоторой функции сходства и активизация наиболее схожего с ним нейрона из слоя прототипов.

Этап 4. Проверка сходства (с использованием функции соответствия) – более детальный анализ схожести, с возможным возвратом на этап 3 и рассмотрением оставшихся прототипов.

Этап 5. Обучение (с использованием функции обучения) - подстройка весов прототипа кластера, вызвавшего реакцию функции выбора. Если ни один из существующих прототипов не прошёл проверку функцией соответствия, то активируется новый нейрон и создается новый кластер на базе нераспознанного вектора.

Этап 6. Постпроцессинг нейронного слоя - например, объединение или разъединение некоторых кластеров в соответствии с требуемыми

условиями.

Далее рассмотрим реализацию этапов предложенной модели для сети Fuzzy ARTMAP.

Этап 1. Входные образы подсети ARTa представлены векторами вида $a = [a_1. , , a_{Ma}]$, а входные образы подсети ARTb имеют вид $b = [b_1. , , b_{Mb}]$, где $a_i , b_j \in [0,1]$. При этом существуют семь основных гиперпараметров, оказывающих влияние на производительность Fuzzy ARTMAP [3].

- параметры выбора (α_a, α_b >0): влияют на выбор категории и препятствует вырождению прототипов кластеров.
- параметры скорости обучения (β_a, $\beta_b \in [0, 1]$) Значения β_a, β_b, близкие к 1 позволяют системе быстрее адаптироваться к новым данным, а β_a, β_b, близкие к 0 используются, как правило, при необходимости выявления долговременных тенденций в данных.
- параметры сходства (ρ_a, ρ_b, $\rho_{ab} \in [0, 1]$): управляют сетевым резонансом. Параметры сходства отвечают за количество сформированных кластеров и представляют собой условную оценку требуемой однородности векторов в кластере. Если параметр сходства очень велик, он создает хорошую классификацию, но при этом возникает большое число кластеров, а это означает, что сеть имеет мало ошибок на обучающей выборке, но у нее меньше возможностей для обобщения. Если параметр сходства очень мал, будет сгенерировано мало кластеров, и сеть будет иметь больше возможностей для обобщения, но при этом больше возможностей совершать ошибки [7].

Этап 2. Специфика обучения сети Fuzzy ARTMAP приводит к постоянному уменьшению значений координат векторов. Это уменьшение может приводить к вырождению прототипов кластеров. Для решения этой проблемы к входным векторам применяется комплементарное кодирование: N-мерный вектор превращается в 2N-мерный путём дополнения его N компонентами, что сохраняет его амплитудную информацию. Таким образом, входные образы подсети ARTa принимают вид $I^a = \left[\overline{a}\ \overline{a}^c\right] = \left[a_1,..,a_{M_a},a_1^c,..,a_{M_a}^c\right]$, где $a_i^c = 1 - a_i$, а M_a длина исходного входного вектора. Аналогично, $I^b = \left[\overline{b}\ \overline{b}^c\right] = \left[b_1,..,b_{M_b},b_1^c,..,b_{M_b}^c\right]$.

Этап 3. Сеть ARTMAP выполняет одновременную обработку двух сетей Fuzzy ART: ARTa и ARTb. В качестве функции выбора используется один из возможных вариантов реализации “нечеткого И”:

$$T_J = \max_j T_j = \frac{|I^a \wedge w_j^a|}{\alpha_a + |w_j^a|}; \quad S_K = \max_k S_k = \frac{|I^b \wedge w_k^b|}{\alpha_b + |w_k^b|}, \qquad (4)$$

где оператор $\wedge$ определяется как $(p \wedge q)_i = \min_i(p_i \wedge q_i)$, а норма $|p| = \sum_i p_i$. После подтверждения резонанса J является активной категорией для сети ARTa, а K является активной категорией для сети ARTb.

Этап 4. На этом этапе проводится проверка сходства: отвечает ли активная категория ARTa желаемому вектору вывода, представленному в ARTb. Функция соответствия вычисляется по формуле:

$$M_{ab} = \frac{|y^b \wedge w_{JK}^{ab}|}{|y^b|} \qquad (5)$$

Соответствие между кластерами устанавливается при выполнении условия $M_{ab} \geq \rho_{ab}$, где ρ_{ab} – параметр сходства. В случае нарушения условия кластер помечается как неактивный для исключения этого кластера и выбора другого кластера. Процесс повторяется до тех пор, пока активный кластер не будет соответствовать желаемому результату. Если активных кластеров не осталось – создаётся новый, с весами, соответствующими входному вектору.

Этап 5. После того, как установился резонанс между входом и выходом, происходит обучение (адаптация) весовых коэффициентов. Веса прошедших проверку сходства прототипов модулей ARTa и ARTb модифицируются по формулам:

$$w_J^a \leftarrow \beta_a\left(I^a \wedge w_J^a\right) + (1 - \beta_a)w_J^a \qquad (6)$$
$$w_K^b \leftarrow \beta_b\left(I^b \wedge w_K^b\right) + (1 - \beta_b)w_K^b \qquad (7)$$

Адаптация весов для модуля F^{ab} выполняется следующим образом:

$$w_{JK}^{ab} = 1, w_{Jk}^{ab} = 0 \text{ для } k \neq K. \qquad (8)$$

Этап 6. Одним из общих недостатков сетей семейства ART является сложность подбора гиперпараметров. Результатом их неправильного выбора может стать пропуск вторжений или, наоборот, высокий процент ложных срабатываний. Как правило, подбор гиперпараметров сети осуществляется на этапе постпроцессинга в ходе большого вычислительного эксперимента. Для сети Fuzzy ARTMAP такой подход неэффективен, так как она имеет семь гиперпараметров и случайный

выбор их оптимального соотношения маловероятен. В данном исследовании предлагается использование параметрической оптимизации с использованием генетического алгоритма, направленной на повышение качества решения задачи.

2.3. Генетический алгоритм (ГА)

Как уже было отмечено, сеть Fuzzy ARTMAP требует отыскания набора гиперпараметров, которые важны в системе классификации. Рассмотрим метод автоматического выбора набора параметров с использованием ГА. Для оценки каждого набора параметров в популяции используется следующая функция приспособленности: $E = C_I / C$, где C_I количество примеров обучающей выборки, которые были правильно распознаны сетью Fuzzy ARTMAP при данном наборе параметров, а C - общее количество примеров в обучающей выборке. Применяется вещественное кодирование хромосом, поскольку оно позволяет быстрее выполнять поиск. При скрещивании используется арифметический кроссовер [9], так как в процессе вычислительного эксперимента он продемонстрировал лучшую стабильность при создании новых решений. Также используется неравномерная мутация Михалевича [9], поскольку она обеспечивала более быструю сходимость и большую точность.

Процесс выбора параметров с помощью ГА представлен на Рисунке 2.

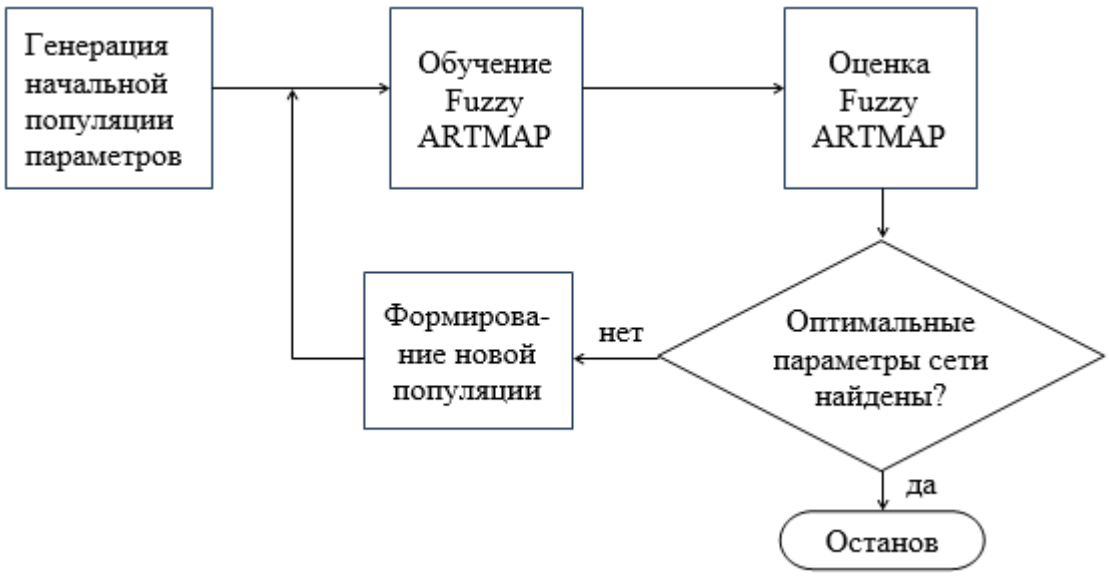

Рисунок 2 - Автоматический выбор параметров сети

3. Результаты и их обсуждение

Процесс построения подсистемы анализа для предлагаемой интеллектуальной системы обнаружения вторжений включает четыре основные фазы: предварительная обработка данных и отбор значимых признаков классификации, отыскание оптимальных гиперпараметров сети Fuzzy ARTMAP с использованием ГА, классификация атак с помощью Fuzzy ARTMAP и тестирование системы. На Рисунке 3 показана блок-схема построения подсистемы анализа для системы обнаружения вторжений.

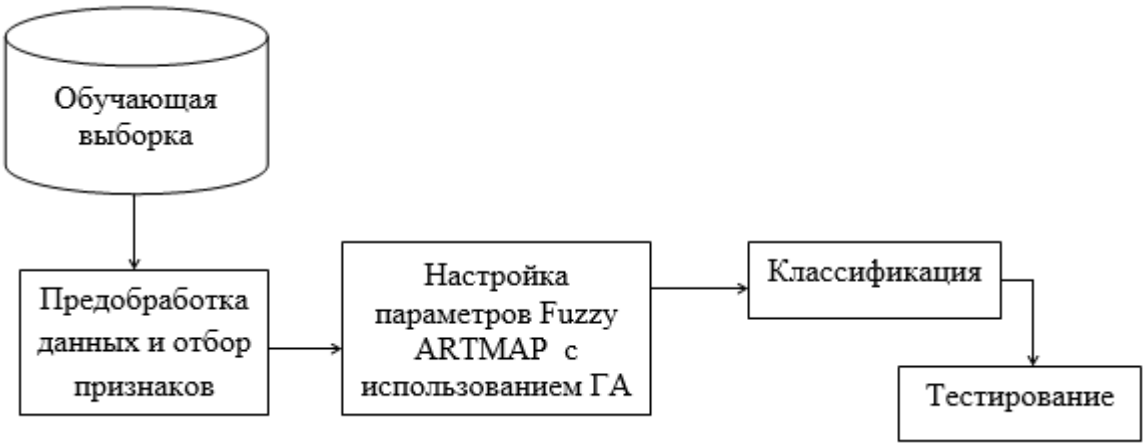

Рисунок 3 - Построение системы обнаружения вторжений

На этапе предварительной обработки данных (препроцессинга) проводится очистка от шумов, а также комплементация входных и выходных векторов. Отбор значимых признаков проводится с помощью алгоритма последовательного обратного поиска с возвращением. После отыскания набора значимых признаков эти признаки используются для обучения Fuzzy ARTMAP. Стадия классификации разделена на этапы. Первый этап определяет, есть ли вторжение или нет; а второй этап определяет характер атаки. На Рисунке 4 показана блок-схема фазы классификации.

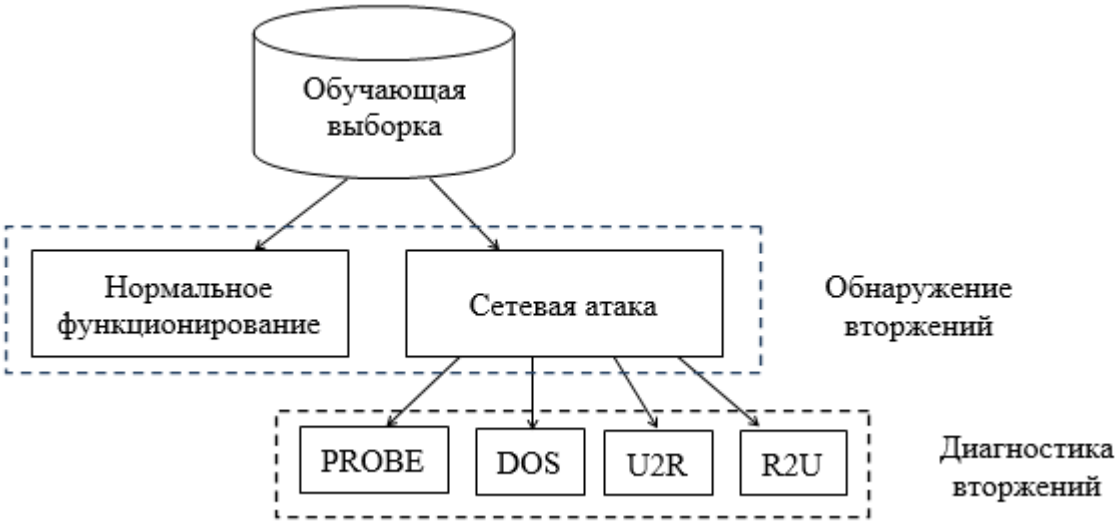

Рисунок 4 - Схема этапа классификации

Исследование в этой статье основано на наборе данных DARPA, полученных специально для оценки IDS [10]. Данные содержат 4900000 обучающих наборов, в которых встречаются как примеры нормального функционирования системы, так и 38 различных типов атак. Все атаки можно классифицировать на четыре основных класса: зондирование (Probe), отказ в обслуживании (DoS), получение прав администратора (U2R) и удаленное получение локального доступа (R2U). Данные содержат 7 символьных и 34 числовых признака (таких, как продолжительность соединения, тип протокола, сетевая служба, параметры хоста и т.д.) Для этапа обнаружения все атаки помечаются как один класс, то есть алгоритм определяет, есть ли вторжение или нет. На этапе диагностики атаки классифицируются на четыре класса.

С помощью предлагаемой системы обнаружения вторжений на этапе отбора признаков было отобрано 12 наиболее значимых признаков из 41-го. На Рисунке 5 показана точность метода классификации на основе сети Fuzzy ARTMAP для этапа обнаружения вторжений, вычисленная по формуле (1), по мере увеличения количества признаков. Можно видеть, что точность впервые достигает единицы (что является максимальным значением), когда число признаков составляет двенадцать. Поэтому было выбрано 12 признаков как оптимальное число.

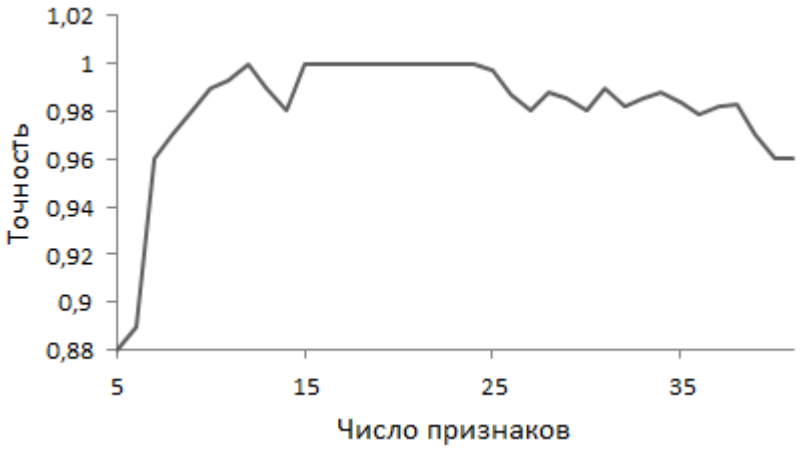

Рисунок 5 - Зависимость точности алгоритма от числа признаков.

Продолжительность процесса обучения нечеткой ARTMAP с 12 признаками составила приблизительно 59% от времени обучения сети с полным набором признаков, при использовании того же компьютера. Это важно для обнаружения вторжений в режиме реального времени.

В процессе тестирования сети на данных, не использовавшихся во время обучения, на этапе диагностики вторжений атаки DoS и Probe сеть обнаруживала в 100% случаях и процент ложных срабатываний для них был равен 0%. При этом для атак U2R и R2U дали точность обнаружения составила 99,87% и 99,78% соответственно, процент ложных срабатываний для них 1,4% и 1,3%. Общая точность классификации системы на тестовой выборке для этапа диагностики вторжений составила 99,89%

4. Заключение

В статье представлена процедура обнаружения и диагностики сетевых атак с использованием нейронной сети Fuzzy ARTMAP. Подмножество значимых признаков было выбрано с помощью алгоритма последовательного обратного поиска с возвращением. Значения гиперпараметров сети Fuzzy ARTMAP настраивались в автоматическом режиме с использованием генетического алгоритма. В процессе вычислительного эксперимента было обнаружено, что уменьшение признаков с 41 до 12 сокращает время обучения на 41%. Сеть Fuzzy ARTMAP с отобранным множеством признаком показала точность классификации 100% для фазы обнаружения и 99,89% для диагностики.

ЛИТЕРАТУРА

1. Denning, Dorothy E. An Intrusion Detection Model// Proceedings of the Seventh IEEE Symposium on Security and Privacy, 1986, pp. 119—131
2. Нестерук Г.Ф. Информационная безопасность и интеллектуальные средства защиты информационных ресурсов / Г.Ф. Нестерук, Л.Г. Осовецкий, А.Ф. Харченко.– СПб.: Изд-во СПбГУЭФ, 2003
3. Нестерук Ф. Г. Инструментальные средства создания нейросетевых компонент интеллектуальных систем защиты информации/ Ф. Г. Нестерук, И. В. Котенко// Труды СПИИРАН. 2013 Вып. 26. С. 7–25
4. Carpenter, G.A. & Grossberg, S. (2003), Adaptive Resonance Theory, In Michael A. Arbib (Ed.), The Handbook of Brain Theory and Neural Networks, Second Edition (pp. 87-90). Cambridge, MA: MIT Press
5. Carpenter G.A., Grossberg S., Reynolds J.H. ARTMAP: Supervised real-time learning and classification of nonstationary data by a self-organizing neural network // Neural Networks. – 1991. – № 4. – P. 565-588.
6. Carpenter G.A., Grossberg S., Markuzon N., Reynolds J.H., Rosen D.B. Fuzzy ARTMAP: An adaptive resonance architecture for incremental learning of analog maps. // Proc. of the Int. Joint Conf. on Neural Network. 1992
7. Каширина И.Л. Нейросетевое моделирование формирования кластерной структуры на основе сетей ART/ Каширина И.Л., Львович Я.Е., Сорокин С.О.// Информационные технологии. 2017. Т. 23. № 3. С. 228-232
8. Каширина И.Л. Кластеризация непрерывного потока данных на основе обобщенной модели нейронной сети семейства ART/ И.Л. Каширина, К.А. Федутинов //Системы управления и информационные технологии. - 2018. Т. 71. № 1. С. 33-39.
9. Каширина И. Л. Эволюционное моделирование: учебное пособие/ И. Л. Каширина. -Воронеж: ИПЦ ВГУ, 2011. -60 с.
10. KDD Cup 1999 Data [Электронный ресурс] URL: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (дата обращения: 10.08.2018)

I.L. Kashirina, K.A. Fedutinov

APPLICATION OF FUZZY ARTMAP NETWORK IN INTELLIGENT SYSTEMS OF INVASION DETECTION

Voronezh State University, Voronezh, Russia

The article deals with the organization of intelligent intrusion detection and detection systems. Research in the field of development of information security tools shows that today the most promising and flexible solutions are based on machine learning methods that can prevent damage from intrusions that were not noticed by standard means of combating computer attacks. In the proposed approach, it is proposed to use a sequential reverse search with a return to select significant features and the Fuzzy neural network ARTMAP to detect and diagnose attacks. Network Fuzzy ARTMAP is able to adapt to the dynamics of computer attacks and allows you to recognize intrusions in the information system in real time, without the need to load datasets in batches. This makes it possible to automate the analysis of safety protocols in a continuous mode. The extensive use of ART family networks in intrusion detection tasks makes it possible to consider the search for approaches that improve their performance. In this paper, the control hyperparameters network Fuzzy ARTMAP proposed to adjust automatically with the use of a genetic algorithm According to the results of the computational experiment, the reduced set of characteristics reduces the computation time by 21%. The accuracy of the classification algorithm was 100% and 99.89% for the detection stage and the diagnostic stage, respectively.

Keywords: neural network, Fuzzy ARTMAP, genetic algorithm, intrusion detection, intelligent information security systems.

REFERENCES

1. Denning, Dorothy E. An Intrusion Detection Model// Proceedings of the Seventh IEEE Symposium on Security and Privacy, 1986, pp. 119—131
2. Nesteruk G.F. Informatsionnaya bezopasnost' i intellektual'nye sredstva zashchity informatsionnykh resursov / G.F. Nesteruk, L.G. Osovetskiy, A.F. Kharchenko.– SPb.: Izd-vo SPbGUEF, 2003
3. Nesteruk F. G. Instrumental'nye sredstva sozdaniya neyrosetevykh komponent intellektual'nykh sistem zashchity informatsii/ F. G. Nesteruk, I. V. Kotenko// Trudy SPIIRAN. 2013 Vyp. 26. C. 7–25
4. Carpenter, G.A. & Grossberg, S. (2003), Adaptive Resonance Theory, In Michael A. Arbib (Ed.), The Handbook of Brain Theory and Neural Networks, Second Edition (pp. 87-90). Cambridge, MA: MIT Press
5. Carpenter G.A., Grossberg S., Reynolds J.H. ARTMAP: Supervised real-time learning and classification of nonstationary data by a self-organizing neural network // Neural Networks. – 1991. – № 4. – R. 565-588.
6. Carpenter G.A., Grossberg S., Markuzon N., Reynolds J.H., Rosen D.B. Fuzzy ARTMAP: An adaptive resonance architecture for incremental

learning of analog maps. // Proc. of the Int. Joint Conf. on Neural Network. 1992
7. Kashirina I.L. Neyrosetevoe modelirovanie formirovaniya klasternoy struktury na osnove setey ART/ Kashirina I.L., L'vovich Ya.E., Sorokin S.O.// Informatsionnye tekhnologii. 2017. T. 23. № 3. S. 228-232
8. Kashirina I.L. Klasterizatsiya nepreryvnogo potoka dannykh na osnove obobshchennoy modeli neyronnoy seti semeystva ART/ I.L. Kashirina, K.A. Fedutinov //Sistemy upravleniya i informatsionnye tekhnologii. - 2018. T. 71. № 1. S. 33-39.
9. Kashirina I. L. Evolyutsionnoe modelirovanie: uchebnoe posobie/ I. L. Kashirina. -Voronezh: IPTs VGU, 2011. -60 s.
10. KDD Cup 1999 Data [Elektronnyy resurs] URL: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (data obrashcheniya: 10.08.2018)