NickWare Group Science
Бабич Н. А.
06.05.2020

О ПРИМЕНЕНИИ ИНТЕРФЕРЕНЦИОННОЙ НЕЙРОННОЙ СЕТИ ДЛЯ ДИНАМИЧЕСКОГО АНАЛИЗА ДАННЫХ В РЕАЛЬНОМ ВРЕМЕНИ

Аннотация

В настоящее время в операционных системах реального времени имеются инструменты, позволяющие получать данные об активности системных процессов. Анализ этих данных является сложной задачей, учитывая количество этих данных и их структуру. Интерференционная модель нейронной сети зарекомендовала себя как удобный и надёжный инструмент, применяющийся для решения различных задач машинного обучения и машинного зрения. Применение этой модели к решению задачи динамического анализа позволит сделать процесс обучения нейронной сети более гибким и удобным, чем в классических нейронных сетях, а также позволит получить более высокую скорость обработки данных.

Ключевые слова: динамический анализ, обнаружение аномалий, операционные системы реального времени, машинное обучение, нейронные сети, персептрон, интерференционная модель.

Введение

В настоящее время производственные предприятия всё чаще внедряют цифровые инструменты в свою деятельность. Это позволяет им повысить качество принимаемых решений, сократить расходы и увеличить прибыль. В частности, в повышении эффективности производственных процессов важную роль играют решения на базе промышленного интернета вещей и аналитики больших данных. Они позволяют оперативно собирать информацию о физических показателях и преобразовывать её в данные для дальнейшей обработки. В связи с цифровизацией производственных процессов остро возникает вопрос о защите от нарушения этих процессов злоумышленниками, а также защите обрабатываемых и хранимых данных от кражи. Одним из способов такой защиты является динамический анализ активности информационной системы.

Операционные системы реального времени позволяют собирать данные об активности процессов во время их функционирования с помощью встроенных инструментов. Динамический анализ подразумевает верификацию этих данных и выявление нежелательной активности. Растущие объёмы данных приводят к тому, что старые методы динамического анализа становятся малоэффективны или даже непригоды к

использованию. Возникает необходимость разработки новых методов решения данной задачи.

Существующие подходы к решению задачи динамического анализа

Классический подход к решению задачи динамического анализа и обнаружения аномалий активности подразумевает наличие баз сигнатур, по которым можно определить, является ли поведение нежелательным. Такой подход имеет существенный недостаток – необходимо постоянно дополнять базу новыми сигнатурами, а, следовательно, нельзя обнаружить те паттерны нежелательной активности, которых в базе нет. Это делает такой подход малоэффективным.

С помощью технологий машинного обучения в настоящее время решается достаточно большое количество задач, в том числе, связанных с информационной безопасностью и поиском уязвимостей и вредоносного программного обеспечения [1, 2]. Исключением не стала и задача динамического анализа активности. Искусственная нейронная сеть, выступающая в роли классификатора, отлично подходит для обнаружения аномалий в наборе данных. Использование данного метода можно разделить на два этапа. На первом этапе необходимо выполнить обучение нейронной сети, используя данные о доверенной активности процессов в операционной системе, полученные на определённом промежутке времени. Второй этап подразумевает использование обученной нейронной сети для сравнения текущей активности с той, которая была запомнена.

Чаще всего в качестве классификатора используется многослойный персептрон. Для него характерно обучение с учителем – необходимо заранее подготовить желаемые выходные сигналы, каждый из которых будет соответствовать определённому классу. В качестве алгоритма обучения наиболее часто используется метод обратного распространения ошибки. Обучение происходит в несколько итераций, называемых эпохами обучения – нужно повторить подачу всех обучающих сигналов на вход сети некоторое количество раз, рассчитывая при этом ошибку обучения относительно желаемого выходного сигнала для каждого класса сигналов и корректируя весовые коэффициенты каждого из нейронов, тем самым минимизируя ошибку обучения сети. Для того, чтобы выполнить распознавание с помощью многослойного персептрона, необходимо подать сигнал на вход сети и рассчитать ошибку распознавания (сравнить выходной сигнал сети с каждым из желаемых выходных сигналов, соответствующих заданным классам).

Распознаваемый сигнал считается принадлежащим тому классу, желаемый выходной сигнал которого наиболее соответствует полученному выходному сигналу.

На практике использование классических моделей нейронных сетей сопряжено со множеством трудностей. На этапе проектирования нейронной сети возникают вопросы, получить ответы на которые чаще всего возможно только эмпирическим путём, а использование готовых решений не всегда подходит по тем или иным причинам. Выбор количества слоёв, подбор количества нейронов на них, настройка параметров обучения становятся нетривиальными задачами [3].

Кроме того, состав компонентов операционной системы может изменяться на этапе эксплуатации, например, может быть изменён список доверенных процессов. Появление нового типа доверенной активности приведёт к тому, что нейронная сеть всегда будет воспринимать её как аномальную. Чтобы избежать этого, необходимо дообучить сеть. В случае с персептроном сделать это невозможно – нужно начинать обучение с нуля (на что требуются дополнительные вычислительные ресурсы и время), а иногда может потребоваться и переконфигурирование сети.

Таким образом, применение классических моделей нейронных сетей имеет существенные недостатки: сложность разработки нейронной сети для решения конкретной задачи, высокая вычислительная ресурсоёмкость, отсутствие возможности дообучения. Возникает необходимость разработки нового метода решения задачи динамического анализа.

Применение интерференционной модели к решению задачи динамического анализа

Интерференционная модель нейронной сети зарекомендовала себя в решении задач распознавания изображений, но в силу своей универсальности может быть применена и к задаче динамического анализа, в частности, для обнаружения аномалий в наборе данных [4, 5, 6]. Она принципиально отличается от большинства классических моделей нейронных сетей. Нейрон в этой модели представляет собой самоорганизующийся объект, а его обучение происходит за счёт перемещения рецепторов под действием нейромедиатора, который выделяется синапсами (как в биологическом нейроне) [4]. Сигнал подаётся последовательно, распределённо по времени, при этом количество данных обучения получается значительно меньше по сравнению с классическими моделями (что позволяет экономить память) – необходимо хранить только координаты рецепторов в конечный момент времени и длины их траекторий. Для успешной классификации данных достаточно

одного нейрона на один класс. Более того, нейронные сети этой модели более устойчивы к частичной потере данных.

На рисунке 1 представлено схематическое изображение интерференционной нейронной сети, спроектированной для решения задачи обнаружения аномалий в некотором наборе данных.

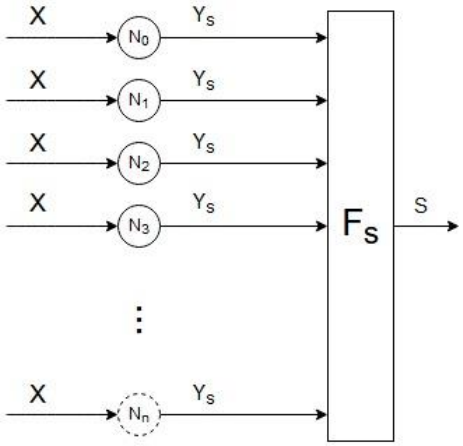

Рисунок 1 – Топология интерференционной нейронной сети, спроектированной для обнаружения аномалий в наборе данных

Здесь $N_i, i \in [0, n]$ обозначены нейроны, соответствующие классам активности информационной системы. Каждый из нейронов может иметь несколько входов (на схеме обозначены X) – это позволяет обучать сеть и распознавать активность сразу по нескольким параметрам. С помощью Ys обозначены выходы нейронов, которые позволяют получить информацию о текущем значении критерия расхождения I [4]. Как видно из схемы, нейронов может быть, вообще говоря, неограниченное количество и они никак не связаны с другими нейронами сети. Это означает, что можно легко дообучать нейронную сеть, добавляя новые классы активности для распознавания.

Блок Fs используется при распознавании паттерна активности и представляет собой функцию минимизации критерия расхождения I:

$$S = \min I_i, i \in [0, n],$$

где Ii – критерий расхождения входного паттерна тому, которому был обучен i-ый нейрон сети.

Таким образом, если значение S близко к нулю, можно сделать вывод о том, что распознанный паттерн соответствует паттерну доверенной активности. Если критерий I для всех нейронов имеет примерно одинаковое значение (изменяется от нейрона к нейрону в небольшом диапазоне, много меньшем, чем сами значения критерия), это означает, что ни один нейрон не «среагировал» на входной паттерн и активность может считаться аномальной. В этом случае необходимо выяснить, является эта активность доверенной (но новой для сети) или нежелательной. Этот выбор делает пользователь системы.

В первом случае необходимо дообучить сеть - добавить в неё новый нейрон и подать на вход данные о новой активности, во втором - принять необходимые меры по нейтрализации угрозы.

Заключение

Таким образом, применение интерференционной модели позволит, по сравнению с классическими моделями, сократить время построения и отладки нейронной сети, уменьшить ресурсоёмкость вычислительных процессов обучения и распознавания, дать возможность без труда адаптировать уже обученную сеть к изменениям в доверенной активности операционной системы реального времени.

В настоящее время интерференционная модель реализована в виде открытой свободно-распространяемой C++ библиотеки Interference [7]. Она позволяет создавать, обучать и применять нейронные сети к решению практических задач, а также поддерживает параллельные вычисления, что позволяет ускорять вычислительные процессы на многоядерных системах. Отсутствие зависимостей от сторонних компонентов делает библиотеку отличным решением для применения во встраиваемых системах, работающих под управлением операционных систем реального времени.

Список использованных источников

1. Wu Songyang, Wang Pan, Li Xun, Zhang Yong. Effective detection of android malware based on the usage of data flow APIs and machine learning. Information and Software Technology. Volume 75, 2016.

2. Sharma Rupam Kumar, Kalita Hemanta Kr, Issac Biju. Are machine learning based intrusion detection system always secure? An insight into tampered learning. Journal of Intelligent & Fuzzy Systems. Volume 35 (3), 2018.

3. Ding Shifei, Xu Xinzheng, Nie Ru. Extreme learning machine and its applications. Neural Computing and Applications. Volume 25 (3-4), 2014.

4. Бабич Н. А. Параметрический синтез интерференционной модели нейронной сети. Электронное научно-практическое периодическое издание «Вестник современных исследований». Научный центр “ОРКА”. Выпуск № 1-13 (28), 2019 г.

5. Бабич Н. А. Анализ эффективности применения интерференционной нейронной сети для решения задачи распознавания образов. Электронное научно-практическое периодическое издание «Вестник современных исследований». Научный центр “ОРКА”. Выпуск № 2-3 (29), 2019 г.

6. Бабич Н. А., Останин М. Л. Распознавание объектов на изображениях высокого разрешения с помощью интерференционной нейронной сети. Молодёжь. Техника. Космос: труды XI Общероссийской молодёжной науч.техн. Конф. Т1 / БГТУ “Военмех” -СПб.; 2019. -485 с.

7. Interference C++ library. GitHub open repository. [Электронный ресурс] — URL: https://github.com/nickware44/interference (дата обращения: 02.02.2020).