Применение гетерогенной нейросистемы для обнаружения кибератак в крупных самоорганизующихся коммуникационных сетях

Д. П. Зегжда, М. О. Калинин, В. М. Крундышев, Е. А.Зубков
Санкт-Петербургский политехнический университет Петра Великого
project@ibks.spbstu.ru

***Аннотация*. Проанализированы основные проблемы применения нейросетей для решения задачи выявления киберугроз в крупных самоорганизующихся сетевых инфраструктурах (VANET/MANET, сенсорных сетях WSN, IoT, сетях Smart Home и Smart Building). Представлены результаты исследований применимости для решения данной задачи классических нейросетей в сравнении с современными рекуррентными, глубокими, LSTM-нейросетями в условиях быстрого обучения и обработки BigData. Дана экспериментальная оценка применимости современных нейросетей в составе гетерогенной нейросистемы обнаружения кибератак в крупных самоорганизующихся коммуникационных сетях, обосновано построение ансамбля из рекуррентной и LSTM-нейросетей.**

Ключевые слова: глубокая нейросеть; кибератака; нейросеть; рекуррентная нейросеть; LSTM-нейросеть; нейросетевой ансамбль; IoT; VANET; MANET; WSN

I. Введение

Самоорганизующиеся коммуникационные сети (VANET – сеть между автомобилями, FANET – сеть между летательными аппаратами, MARINET – сеть между плавательными средствами, WSN – сенсорные сети, IoT/MANET – Интернет вещей) характеризуются одноранговой инфраструктурой, перемещением узлов и реализацией динамической маршрутизации на каждом узле. Функциональные преимущества таких сетей: возможность коммуникаций при отсутствии базовых станций, обеспечение передачи данных при перемещении узлов в динамической сетевой топологии [1]. Для новых сетей появились предпосылки для реализации новых киберугроз, например, перехвата трафика, управления потоками передачи данных и управления, удаленного контроля и управления над устройствами, организация ботсетей из устройств, отказ в обслуживании киберсистем.

Встраивание средств защиты в самоорганизующуюся сеть – сложная теоретическая и прикладная задача из-за особенностей данных сетей и недостаточности вычислительных ресурсов в узлах сети. В этой связи для таких сетей необходимы средства априорной защиты, обеспечивающие предупреждение киберугроз. Не смотря на то, что искусственные нейросети (ИНС) для этой задачи используются давно, в последнее время появились нейромодели, для которых еще не выполнялось исследования их применимости для выявления киберугроз в самоорганизующихся сетях. Среди новых ИНС выделяются глубокие ИНС, рекуррентные ИНС, LSTM-нейросети.

Работа выполнена при финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы» (Соглашение 14.575.21.0131 от 26.09.2017, уникальный идентификатор соглашения RFMEFI57517X0131).

Результаты работы получены с использованием вычислительных ресурсов суперкомпьютерного центра Санкт-Петербургского политехнического университета Петра Великого – СКЦ «Политехнический» (http://www.spbstu.ru).

II. Анализ области исследования

Задача системы обнаружения вторжений (IDS) – по известным наборам (выборкам) значений признаков классифицировать киберугрозу [3]. Известные подходы к решению данной задачи:

- статистический метод [3, 4], который основан на создании профиля-эталона поведения системы и контроле отклонений от него. Данный метод позволяет нарушителю натаскивать детектор на усредненный профиль и пропускать атаки;
- метод прогнозирования шаблонов [3, 5], в котором IDS предсказывает будущие состояния системы, аппроксимируя трассу прошедших событий. Множество современных кибератак нельзя описать подобными правилами, и они будут пропущены детектором;
- искусственные нейросети [3, 6-8]. Ассоциативная модель знаний в виде нейросетей известна достаточно давно и предоставляет возможности по параллельной обработке данных и неалгоритмической классификации. Процедура классификации заключается в отборе идентифицирующих признаков киберугроз, в обучении нейросети на данном наборе данных, при этом формируется эталон безопасного состояния системы. В процессе работы на вход нейросети подаются реальные данные, и она определяет их принадлежность к ранее сформированным классам киберугроз.

Не смотря на то, что нейросетевые методы развиваются много лет, в последнее время наблюдается активность в этой области, что связано с развитием вычислительных технологий и с потребностью в обработке больших данных (BigData). Сеть VANET из 1000 связанных автомобилей, в каждом из которых имеется управляющая CAN-шина и 20 контроллеров OBU, генерирует в минуту около 4 млн. параметров, которые влияют на работу движущегося автомобиля. Проблема BigData при выявлении киберугроз существенно усложняют задачу разработки современных IDS для крупных сетей с динамической топологией.

Далее представлена оценка применимости современных нейросетей в составе гетерогенной нейросистемы обнаружения кибератак в крупных самоорганизующихся коммуникационных сетях.

III. Исследование нейросетевых методов обнаружения киберугроз

Классические нейросети (например, персептроны с логическими передаточными функциями [7], прямого и обратного распространения ошибок [7]) не удовлетворяют возросшим требованиям к объему обучающих выборок (проблема насыщения на BigData). Также они обладают низкой точностью, долго обучаются, избыточны и требовательны к объемам вычислительных ресурсов [8].

Для определения, какие нейросети необходимо включить в гетерогенную нейросистему обнаружения кибератак в крупной самоорганизующейся коммуникационной сети, отобраны следующие нейросети:

- классический персептрон прямого распространения;
- рекуррентная нейросеть [9];
- нейросеть глубокого обучения [10];
- LSTM-нейросеть[11].

Для исследования используется типовая кибератака на доступность самоорганизующейся сети – атака black hole [12]. Атака направлена на нарушение связности сети, использует динамическую маршрутизацию, в результате чего узел-нарушитель не передает (отбрасывает) поступающие сетевые пакеты, которые он должен был бы передавать далее по маршруту.

В табл. 1 указаны результаты, полученные в ходе обучения исследованных нейросетей.

ТАБЛИЦА I СРАВНЕНИЕ НЕЙРОСЕТЕЙ НА ЭТАПЕ ОБУЧЕНИЯ

Нейросеть	**Доля ошибки для обучающей выборки (%)**	**Объем выборки (обучающая/рабочая) (шт.)**	**Период обучения (с)**
Глубокая	0,1	22/11	2,2
Персептрон	0,2	22/11	3,9
Рекуррентная	4	4500/1500	44,5
LSTM	4	4500/1500	50,6

Персептрон и нейросеть глубокого обучения имеют простую архитектуру и за счет этого выигрывают у современных нейросетей. Персептрон не может быть применен к работе с BigData, рекуррентная и LSTM нейросети наоборот хорошо справляются с BigData. Отмечено сходство персептрона и глубокой нейросети (рис. 1).

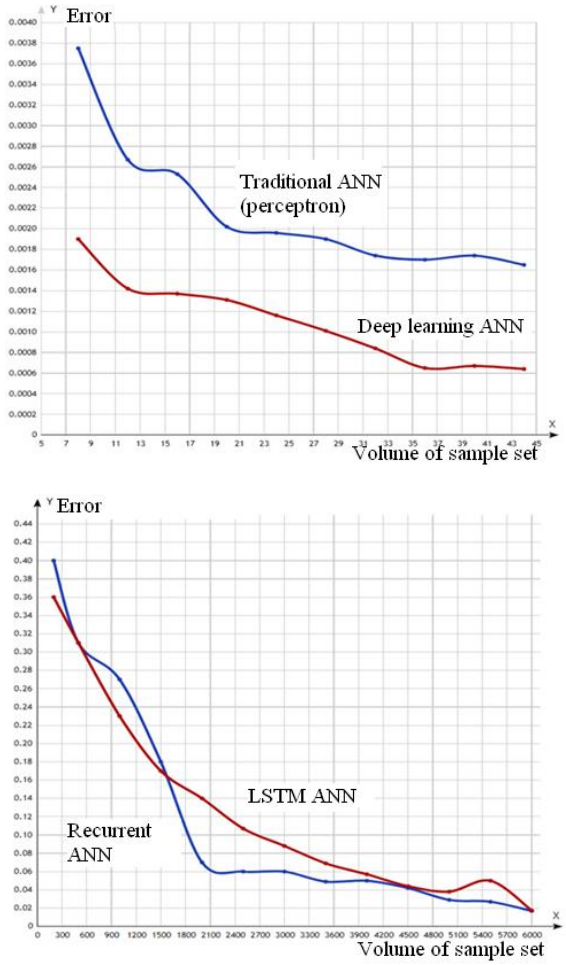

Рис. 1. Влияние объема выборки на результативность нейросетей

На одинаковой выборке глубокая нейросеть обучается быстрее, с меньшей ошибкой, при этом не наблюдается резких спадов при увеличении выборки. Рекуррентная и LSTM нейросети (рис. 1) схожи по своему поведению, однако LSTM нейросеть использует механизм памяти, который позволяет запоминать обучение и мягко реагировать на изменения в выборке.

С учетом чувствительности нейросетей к размеру выборки, выполнено исследование для большого объема данных (табл. 2, объем выборки – 4 млн. признаков). Персептрон демонстрирует короткое время обработки BigData, но это сопровождается падением качества результатов. Глубокая нейросеть лишена проблемы BigData на стадии обучения, а в рабочем режиме она также показывает низкую результативность.

ТАБЛИЦА II СРАВНЕНИЕ НЕЙРОСЕТЕЙ НА ЭТАПЕ РАБОТЫ ПРИ ОБРАБОТКЕ BIGDATA

Нейросеть	**Доля ошибки для рабочей выборки (%)**	**Период обработки (с)**
Персептрон	37	2,1
Глубокая	50	3,0
Рекуррентная	1	28,8
LSTM	2	27,2

IV. ЗАКЛЮЧЕНИЕ

Результаты исследований показывают непригодность для решения указанной задачи традиционных нейросетей вследствие их неспособности работать с BigData. Для поставленной задачи обнаружения киберугроз в самоорганизующихся сетях рекомендуется включить в гетерогенную нейросистему ансамбль из LSTM и рекуррентной нейросетей, которые способны эффективно работать в сложных условиях, используя механизмы запоминания и обработки BigData.

Использование новых нейросетевых методов позволяет создавать системы IDS, адекватные угрозе и условиям эксплуатации, что позволит обеспечить кибербезопасность современных сетевых инфраструктур.

СПИСОК ЛИТЕРАТУРЫ

[1] B. Krishna. Study of Ad hoc Networks with Reference to MANET, VANET, FANET // International Journals of Advanced Research in Computer Science and Software Engineering. 2017. Т. 7, вып. 7. С. 390-394.

[2] M. Erritali, B. El Ouahidi. A Survey on VANET Intrusion Detection Systems // International Journal of Engineering and Technology. 2013. Т. 5, вып. 2. С. 1985-1989.

[3] K.R. Karthikeyan, A. Indra. Intrusion Detection Tools and Techniques – A Survey // International Journal of Computer Theory and Engineering. 2010. Т. 2, вып. 6. С. 901-906.

[4] X. Li. Probabilistic techniques for intrusion detection based on computer audit data // IEEE Transactions on Systems Man and Cybernetics. Part A: Systems and Humans. 2001. Т. 31, вып. 4. С. 266-274.

[5] A. S. Sodiya, O. A. Ojesanmi, O. C. Akinola, O. Aborisade. Neural Network based Intrusion Detection Systems // International Journal of Computer Applications. 2014. Т. 106, вып. 18. С. 19-24..

[6] B. Widrow, M. A. Lehr. 30 years of adaptive neural networks: perceptron, Madaline, and back propagation // Proceedings of the IEEE. 1990. Т. 78, вып. 9. С. 1415-1442.

[7] С. Николенко., А. Кадурин, Е. Архангельская. Глубокое обучение. Погружение в мир нейронных сетей. СПб: Питер, 2018, 480 с.

[8] A. Mallya. Introduction to RNNs.// Available at: http://slazebni.cs.illinois.edu/spring17/lec02_rnn.pdf (2018).

[9] V. Sze, Y. H. Chen, T. J. Yang, J. S. Emer. Efficient processing of deep neural networks: A tutorial and survey // Proceedings of the IEEE. 2017. Т. 105, вып. 12. С. 1-31.

[10] R. Adhikari, R. K. Agrawal. A Homogeneous Ensemble of Artificial Neural Networks for Time Series Forecasting // International Journal of Computer Applications. 2011. Т. 32, вып. 7. С. 1-8.

[11] N. K. Chaubey. Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study // International Journal of Security and Its Applications. 2016. Т. 10, вып. 5. С. 261-274.