УДК 004.032.26:004.056 DOI: 10.26102/2310-6018/2021.32.1.012

Проблемы обучения глубоких нейронных сетей для обнаружения угроз нарушения безопасности в сетях с динамической топологией

С.Г. Клюев, Е.Е. Трунов

Краснодарское высшее военное училище,
Краснодар, Российская Федерация

Резюме: В настоящее время внедрение компьютерных сетей с динамической топологией становится повсеместным явлением. В повседневной жизни мы часто с ними сталкиваемся, сами того не подозревая. Мобильные, автомобильные, морские и воздушные динамические сети наблюдаются повсюду, а их отличительной особенностью является постоянное изменение структуры за счет обновления конечных узлов в сети. Благодаря такому широкому распространению в этих сетях возникает достаточное количество угроз нарушения безопасности как на аппаратном уровне, так и на уровне программного обеспечения. Такие угрозы не могут оставаться без внимания. В связи с этим данная работа посвящена рассмотрению основных угроз нарушения безопасности на программном и сетевом уровнях в сетях с динамической топологией и проблем, возникающих при обучении глубокой нейронной сети для обнаружения данных угроз. Проведен анализ проблем обучения глубоких нейронных сетей и предложена методика их устранения с использованием изученных методов решения подобных проблем. В результате практической реализации методики возможно получить правильно обученную нейронную сеть, которая позволит эффективно обнаруживать угрозы нарушения безопасности в режиме реального времени.

Ключевые слова: компьютерная сеть, динамическая топология, нейронная сеть, угрозы нарушения безопасности, глубокое обучение.

Для цитирования: Клюев С.Г., Трунов Е.Е. Проблемы обучения глубоких нейронных сетей для обнаружения угроз нарушения безопасности в сетях с динамической топологией. *Моделирование, оптимизация и информационные технологии.* 2021;9(1). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=898 DOI: 10.26102/2310-6018/2021.32.1.012

Deep neural networks training problems of detecting security threats in networks with dynamic topology

S.G. Klyuev, E.E. Trunov

Krasnodar Higher Military School,
Krasnodar, Russian Federation

Abstract: At present, the introduction of computer networks with dynamic topology is becoming a ubiquitous phenomenon. In everyday life, we often encounter them without knowing it. Mobile, road, sea, and air dynamic networks are everywhere, and their distinctive feature is the constant change in the structure due to the constant updating of the end nodes in the network. Due to such a widespread in these networks, there are a sufficient number of security threats both at the hardware level and at the software level. Such threats cannot be ignored. In this regard, this paper is devoted to the consideration of the main threats of security breaches at the software and network levels in networks with dynamic topology and the problems that arise when training a deep neural network to detect these threats. The analysis of the problems of training deep neural networks is carried out and the method of their elimination is proposed using the studied methods of solving such problems. As a result of the practical implementation

of the technique, it is possible to obtain a properly trained neural network that will effectively detect security threats in real-time.

Keywords: computer network, dynamic topology, neural network, security threats, deep learning.

For citation: Klyuev S. G., Trunov E. E. Problems of Training Deep Neural Networks for Detecting Security Threats in Networks with Dynamic Topology. *Modeling, Optimization and Information Technology*. 2021;9(1). Available from: https://moitvivt.ru/ru/journal/pdf?id=898 DOI: 10.26102/2310-6018/2021.32.1.012 (In Russ).

Введение

На сегодняшний день в открытых источниках информации практически отсутствуют сведения о сетях динамической топологии. Такие сети не входят в общеизвестные классификации компьютерных сетей, они не имеют строгого определения и получили свое развитие относительно недавно. Несмотря на повсеместное использование таких сетей, достаточно сложно сформулировать окончательное определение сетей динамической топологии, [1] а их наиболее встречающееся разъяснение говорит о том, что динамическая топология сети – это такая топология, где в процессе вычислений конфигурация взаимосвязей с помощью программных средств может быть изменена. Данное определение раскрывает понятие динамической топологии, но недостаточно говорит о сети, ведь для однозначного представления необходимо учесть сразу несколько факторов:

1. Самоорганизация. Сеть не имеет определенной структуры, она меняется и распределяет функции между узлами при появлении нового устройства в сети и изменении проходящего через узлы трафика.
2. Отсутствие фиксированной инфраструктуры. Оборудование и программное обеспечение узлов, находящихся в сети, может постоянно меняться.
3. Поддержка множественных связей между узлами. Каждый узел в динамической сети имеет несколько соединений, с учетом того, что адрес узла определяется однозначно.
4. Адаптивная маршрутизация на узлах сети. На каждом из узлов с определенной частотой происходит процесс поиска оптимального пути от источника к конечному узлу-получателю, который может измениться в любой момент времени.

Исходя из данных факторов и на основе вышесказанного определения динамической топологии, можно сформулировать определение сети динамической топологии. Сеть динамической топологии – это такая самоорганизующаяся сеть, в которой отсутствует постоянная инфраструктура, а обмен информацией через множество связей между узлами осуществляется на основании протоколов адаптивной маршрутизации.

К таким сетям относятся: Автомобильные самоорганизующиеся сети - VANET, Мобильные самоорганизующиеся сети - MANET, Беспилотные самоорганизующиеся сети - FANET и Морские самоорганизующиеся сети - MARINET. Между собой они отличаются характером передаваемой информации и скоростью обновления узлов в сети. Так, мобильная, автомобильная и беспилотная структура сети гораздо чаще обновляется, в сравнении с морской. Данные сети могут использоваться как в гражданской сфере, так и для организации управления войсками (силами) в период ведения боевых действий, что подчеркивает актуальность работы.

Кроме того, важность рассмотрения данной темы заключается в возникновении широкого спектра угроз нарушения безопасности сетей динамической топологии и, как следствие, обеспечение безопасности в таких сетях. Появление большого количества угроз связано в первую очередь с множеством управляющих механизмов, в качестве которых могут выступать как аппаратные, так и программные средства.

Основные уровни угроз и их характеристики в сетях с динамической топологией показаны в Таблице 1.

Таблица 1 – Угрозы нарушения безопасности
Table 1 – Security threats

Уровни угроз	Объект воздействия	Последствия
Программный уровень	Управляющее программное обеспечение	1. Несанкционированный доступ и сбор информации. 2. Фальсификация данных. 3. Уничтожение данных. 4. Вывод устройств из строя. 5. Заражение устройств вредоносным программным обеспечением
Сетевой уровень	Отдельные узлы сети	1. Нарушение маршрутизации. 2. Изменение топологии сети. 3. Вывод узлов из строя

Как видно из характеристики угроз, их проявления в сетях с динамической топологией очень разнообразны, а значит требуются подходы, которые позволят выявлять различные угрозы нарушения безопасности.

В настоящее время обнаружение угроз в сетях с динамической топологией в основном сводится к SIEM-системам как надстройки для антивирусов, систем обнаружения атак и сетевого оборудования, что не позволяет отслеживать состояние сети с динамической топологией в реальном времени. Несмотря на то, что основной целью SIEM-систем является предупреждение угроз и управление инцидентами в близком к реальному времени режиме, они не способны эффективно прогнозировать события, происходящие в сетях с динамической топологией. В первую очередь это связано с тем, что SIEM-системы используют уже сформированный банк данных об угрозах, а в случае с постоянно изменяющейся структурой динамических сетей сбор такой информации не дает высокой вероятности правильного прогнозирования. В качестве альтернативы в диссертационной работе 2018 года [2] Романом Алексеевичем Демидовым был предложен подход выявления многоуровневых угроз в сетях динамической топологии на основе интеллектуальных методов глубокого обучения. Основной концепцией данного подхода является построение глубокой нейронной сети и дальнейший процесс ее обучения.

Наша работа посвящена анализу проблем, возникающих в ходе обучения такой сети, и предложена методика их решения.

Проблемы, возникающие в процессе обучения глубокой нейронной сети

В процессе практического применения методов глубокого обучения нейронной сети перед разработчиком встают две основные проблемы: дискретность элементов описания сетей динамической топологии и плохая обучаемость глубокой нейронной сети. И если в качестве решения первой учеными предложено применение семантического векторного представления для слов естественного языка, то вторая проблема стоит остро и до настоящего времени нет реализованных решений эффективного обучения глубокой нейронной сети. Глубокие сети в целом плохо поддаются обучению, на что есть две основные причины:

1) эффект затухания градиента;
2) малый набор входных данных для обучения нейронной сети.

Причина затухания градиента возникает в связи с большим количеством промежуточных слоев. Так как обучение нейронной сети начинается с конца (конечных слоев), то в процессе изменения весовых коэффициентов связей между нейронами сигнал ошибки в недостаточной степени проходит к начальным слоям. Это приводит к тому, что верхние слои оперируют с плохими представлениями входных данных и, как следствие, достигается низкая точность обучения нейронной сети в целом.

Обучающие данные являются неотъемлемой частью обучения любой нейронной сети, ведь именно на основании этих данных формируются контрольные веса между нейронами. В свою очередь, исходя из полученных весов, нейронная сеть распознает тот или иной набор подаваемых на вход данных и делает вывод о принадлежности их к какому-либо классу (в данном случае прогнозирует вероятную угрозу нарушения безопасности). Таким образом, если обучаемый набор данных был достаточно маленький и (или) неправильно сформирован, результат работы нейронной сети будет чрезвычайно неточен. Именно поэтому необходим правильно построенный и большой набор обучающих данных, который в данном случае реализовать практически невозможно. Все открытые источники предоставляют небольшие наборы данных угроз безопасности, приблизительно 5–10 тысяч значений. Это несоизмеримо маленькое число, если рассматривать его в сравнении с крупными компаниями, например, АО «Лаборатория Касперского», ООО «Доктор Веб» и многими другими, где формируются наборы обучаемых данных размером от 100 до 500 тысяч значений. Соответственно, по объективным причинам данных наборов нет в открытом доступе и, не имея колоссальных средств, самостоятельно генерировать такие данные не получится.

Методика решения проблем обучения глубокой нейронной сети

Проблема затухания градиента

Для решения данной проблемы необходимо предварительно сузить пространство входных значений. Используя знания о характере входных данных, их можно отобразить в такое пространство, в котором будут наиболее проявлены глубинные различия входов. Иначе говоря, цель состоит в том, чтобы отфильтровать начальные данные грубым образом, определяя их явные различия. Для достижения данной цели существует два подхода:

1. Предварительное обучение начальных слоев.

Суть метода заключается в том, что нейронная сеть сама учится настраивать весовые коэффициенты в начальных слоях. Для этого ей подаются непомеченные данные на вход, то есть данные, к которым не приставляется правильный ответ с точки зрения человека. Нейронной сети лишь дается общая оценка всех ее действий в процессе

решения поставленной задачи. На основании этих оценок нейронная сеть подстраивает весовые коэффициенты в начальных слоях.

2. Обучение с переносом.

Данный метод позволяет обойти проблему недостатка помеченных тренировочных данных для задач обучения глубокой нейронной сети. Принцип обучения с переносом заключается в частичном обучении начальных слоев основной сети при решении вспомогательной задачи и, как следствие, использовании обученной части сети при решении основной задачи. Так, используя наиболее доступные обучающие данные, обучается фрагмент сети. Полученные весовые коэффициенты полагаются фиксированными и подключаются на вход основной нейронной сети для решения основной задачи.

Недостаток обучающих данных

Данная проблема является актуальной для практически любой нейронной сети, целью которой становится решение специфической и узконаправленной задачи. Возможных решений, как и в случае с затуханием, всего два:

использование методов обучения, где не требуется большая выборка с помеченными данными;

создание собственного банка данных угроз, который будет включать в себя признак конкретной угрозы и метку, указывающую на принадлежность признака к конкретной угрозе.

В качестве методов обучения, не требующих большого набора тренировочных данных, можно использовать методы предварительного обучения и с переносом, которые были рассмотрены выше.

Создание же собственного перечня угроз нарушения безопасности является задачей непосильной, за исключением случаев, когда вы являетесь участником крупной компании и имеете большие вычислительные возможности и крупную пользовательскую аудиторию. При таком варианте сбор статистики пользователей позволит упорядочить полученные данные и на их основании создать собственный банк данных угроз компании. Примером таких компаний выступают АО «Лаборатория Касперского», ООО «Доктор Веб», Avast Software и другие.

Исходя из вышесказанного, процесс обучения глубокой нейронной сети для обнаружения угроз нарушения безопасности в сетях с динамической топологией можно представить в виде двух алгоритмов, изображенных на Рисунках 1 и 2 соответственно.

На Рисунке 1 для обучения глубокой нейронной сети используется вспомогательная нейронная сеть с меньшим числом скрытых слоев. Она позволяет предварительно обучить начальные слои основной сети в ситуации с недостатком обучающих данных. За первый проход (одну эру обучения) малая нейронная сеть сужает круг входных значений грубым методом, используя общие знания о характере входных данных, и затем передает их на вход основной сети. Все последующие эры обучения происходят уже без участия малой нейронной сети, так как затухания градиента в данном случае уже не происходит и вероятность прямого распространения ошибки в последующие слои достаточно невысока.

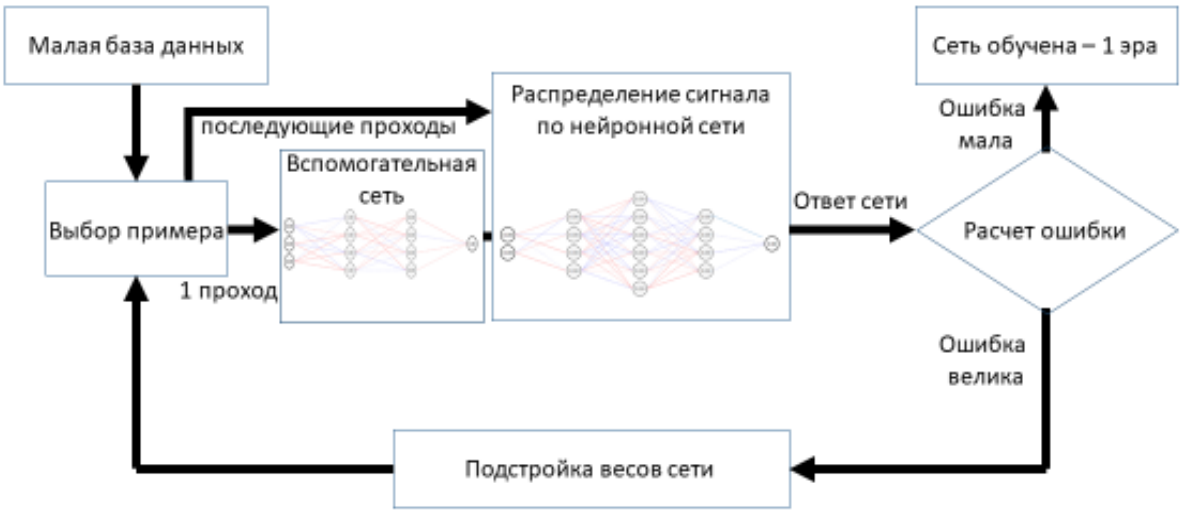

Рисунок 1 – Метод обучения с недостатком базы данных
Figure 1 – Training method with a database flaw

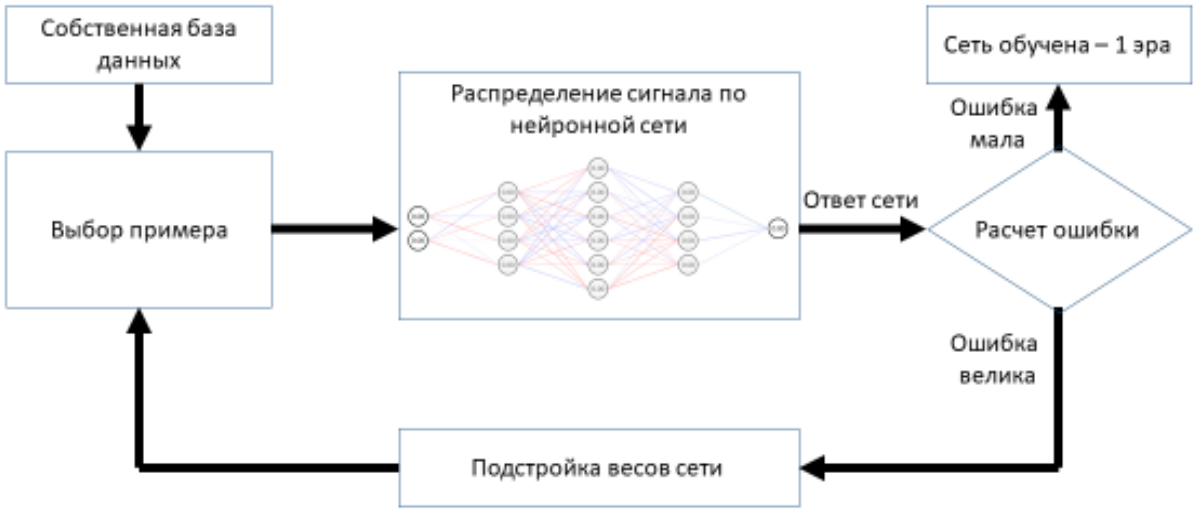

Рисунок 2 – Метод обучения с использованием собственной базы данных
Figure 2 – Training method using your own database

На Рисунке 2 обучение глубокой нейронной сети происходит с использованием собственной базы данных угроз. Данные условия являются эталонными, так как создание собственного банка угроз – задача ресурсозатратная и трудно реализуемая. Но если иметь такой структурированный банк угроз, в котором будет большое количество обучающих данных, то предварительного обучения основной нейронной сети можно избежать.

Заключение

Таким образом, выявление угроз нарушения безопасности в сетях динамической топологии на сетевом и программном уровнях может быть осуществлено с использованием глубокого обучения нейронных сетей. Но для эффективного

применения методов глубокого обучения необходимо решить ряд проблем, анализ и возможные пути решения которых приведены в данной работе. Именно практическая реализация предложенных методов будет способствовать логическому обучению нейронной сети, которая впоследствии может быть внедрена в любую динамически изменяющуюся сеть и выявлять угрозы в реальном времени, ведь от того, как быстро будет произведена локализация угрозы, напрямую зависит размер нанесенного ею ущерба.

ЛИТЕРАТУРА

1. Защита информации. Основные термины и определения: ГОСТ Р 50922-2006, взамен ГОСТ Р 50922-96. 2008:1-5. Доступно по: http://www.consultant.ru. (дата обращения: 15.12.2020).
2. Демидов Р.А. Выявление угроз нарушения информационной безопасности в сетях с динамической топологией с использованием методов глубокого обучения. *Диссертация на соискание ученной степени кандидата технических наук*. 2018:1-143.
3. Нейронная сеть. *Онлайн моделирование*. Доступно по: http://primat.org/demo/network/network.html#1. (дата обращения: 17.12.2020).
4. Нейросети и глубокое обучение, глава 1: *использование нейросетей для распознавания рукописных цифр*. Доступно по: https://habr.com/ru/post/456738/. (дата обращения: 10.12.2020).
5. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка): утв. заместителем директора ФСТЭК России 15.02.2008. 2008:1-8. Доступно по: http://fstec.ru/component/attachments/download/289. (дата обращения: 10.12.2020).
6. Воробьев Л.В. Системы и сети передачи информации: *учебное пособие для студентов высших учебных заведений*. 2009:1-336.
7. Гольдштейн Б.С. Сети связи: *учебное пособие для студентов высших учебных заведений*. 2010:1-400.
8. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения: ГОСТ Р 52488-2005. 2007:1-7. Доступно по: http://www.consultant.ru. (дата обращения: 13.12.2020).
9. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем: ГОСТ Р 56546-2015. 2016:1-17. Доступно по: http://www.consultant.ru. (дата обращения: 13.12.2020).
10. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель: ГОСТ Р ИСО МЭК 15408-1-2012 взамен ГОСТ Р ИСО МЭК 15408-2008.
    2013:1-56. Доступно по: http://www.consultant.ru. (дата обращения: 14.12.2020).
11. Крухмалев В.В., Гордиенко В.Н. Основы построения телекоммуникационных систем и сетей: *учебное пособие для студентов высших учебных заведений*. 2004:1-510.
12. Соколов А.В. Защита информации в распределенных корпоративных сетях и системах. 2002:1-656.

REFERENCES

1. Information security. Basic terms and definitions: GOST R 50922-2006, instead of GOST R 50922-96. 2008:1-5. Available at: http://www.consultant.ru. (accessed 15.12.2020). (In Russ)
2. Demidov R. A. Identification of threats to information security violations in networks with dynamic topology using deep learning methods. Dissertation for the degree of Candidate of Technical Sciences. 2018:1-143. (In Russ)
3. Neural network. Online modeling. Available at: http://primat.org/demo/network/network.html#1. (accessed 17.12.2020). (In Russ)
4. Neural networks and deep learning, Chapter 1: Using neural networks to recognize handwritten numbers. Available at: https://habr.com/ru/post/456738/. (accessed 10.12.2020). (In Russ)
5. Basic model of threats to the security of personal data during their processing in personal data information systems (extract): approved by the Deputy Director of the FSTEC of Russia 15.02.2008. 2008: 1-8. Available at: http://fstec.ru/component/attachments/download/289. (accessed 10.12.2020). (In Russ)
6. Vorobyev L. V. Systems and networks of information transmission: a textbook for students of higher educational institutions. 2009:1-336. (In Russ)
7. Goldstein B. S. Communication networks: a textbook for students of higher educational institutions. 2010:1-400. (In Russ)
8. Information security. Ensuring the security of telecommunications networks. General provisions: GOST R 52488-2005. 2007: 1-7. Available at: http://www.consultant.ru. (accessed 13.12.2020). (In Russ)
9. Information security. Vulnerabilities of information systems. Classification of information system vulnerabilities: GOST R 56546-2015. 2016:1-17. Available at: http://www.consultant.ru. (accessed 13.12.2020). (In Russ)
10. Information technology. Methods and means of ensuring security. Criteria for assessing the security of information technologies. Part 1. Introduction and general model: GOST R ISO IEC 15408-1-2012 instead of GOST R ISO IEC 15408-2008. 2013:1-56. Available at: http://www.consultant.ru. (accessed 14.12.2020). (In Russ)
11. Krukhmalev V. V., Gordienko V. N. Fundamentals of building telecommunications systems and networks: a textbook for students of higher educational institutions. 2004: 1-510. (In Russ)
12. Sokolov A.V. Information protection in distributed corporate networks and systems. 2002:1-656. (In Russ)

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Клюев Станислав Геннадьевич, кандидат технических наук, доцент Краснодарского высшего военного училища, Краснодар, Российская Федерация.
e-mail: s.g.klyuev@mail.ru

Stanislav Gennadievich Klyuev, Candidate Of Technical Sciences, Associate Professor Of The Krasnodar Higher Military School, Krasnodar, Russian Federation.

Трунов Евгений Евгеньевич, курсант Краснодарского высшего военного училища, Краснодар, Российская Федерация.
e-mail: ittehnology2018@gmail.com

Evgeny Evgenievich Trunov, Cadet Of The Krasnodar Higher Military School, Krasnodar, Russian Federation.