

УДК 004.8

НЕЙРОННІ МЕРЕЖІ – ШЛЯХ ДО ГЛИБИННОГО НАВЧАННЯ

Бойко К.В., студ. Гр КБ-161

Петренко Т.А., ст. викладач кафедри кібербезпеки та математичного моделювання
Чернігівський національний технологічний університет

Нейронні мережі - це комп'ютерні програми, що імітують нейронні мережі мозку при прийнятті будь-яких рішень. Нейронні мережі зазвичай включають велику кількість процесорів, які розташовані в окремих шарах та паралельно працюють. [1] Простіше кажучи, є вхідний шар, прихований шар і вихідний шар (Рис.1). Перший рівень отримує інформацію аналогічно до зорових нервів людини. Кожний наступний рівень отримує вихідні дані від рівня, що передує йому, а не від їх первинного вводу. Таким же чином, нейрони, що знаходяться далі від зорового нерва, отримують сигнали тільки від тих, хто ближче до них. Останній шар виробляє вихідні дані системи.

Кожний вузол, що обробляється має свою власну невелику сферу знань, яка включає те, що він бачив, і будь-які правила, які він спочатку запрограмував або розробив для себе. Ці шари дуже взаємопов'язані, тобто кожен вузол рівня n буде з'єднаний з багатьма вузлами рівня $n - 1$, та його вхідними даними в шарі - $n + 1$, що забезпечує ввід даних для цих вузлів. У вихідному шарі може бути один або декілька вузлів, де й читається створена їм відповідь.

Нейронні мережі відрізняються тим, що вони адаптивні, а це означає, що вони можуть модифікувати себе під час початкового навчання, а наступні "пробіжки" забезпечують більше інформації про сам світ. Найпростіша навчальна модель перш за все зосереджена на зважування вхідних потоків, тому кожен вузол оцінює важливість введення від кожного з його попередників. Вхідна інформація, що сприяє одержанню правильних відповідей, буде оцінюватися вище.[2]

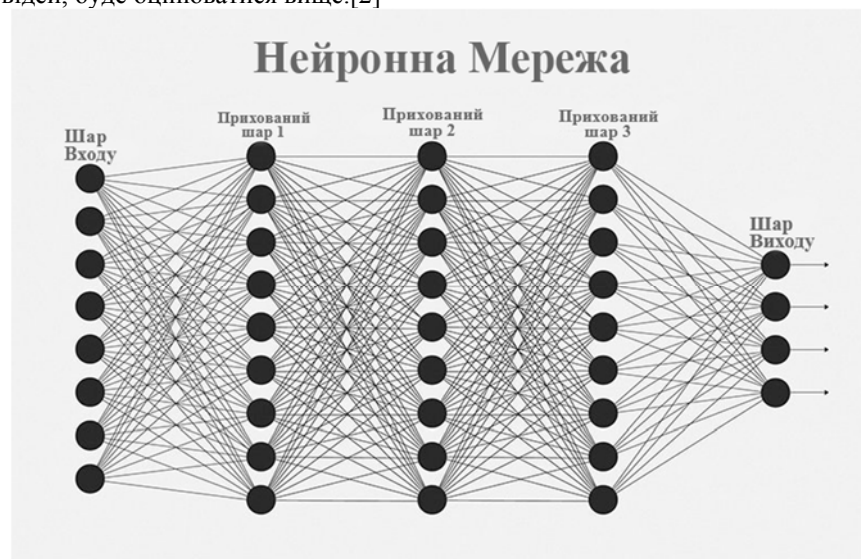


Рис. 1. Склад нейронної мережі

Нейромережі перш за все навчаються на досвіді, будучи корисними для розпізнавання образів, узагальнення та прогнозування. Хоча і не так швидко, але вони здатні "витримувати" недосконалі дані, і тому вам не потрібно вибирати статистичні формули або заздалегідь знати, які фактори будуть важливими. Нейронні Мережі навчаються, повторно представляючи приклади в мережі.[3] Кожен приклад включає в себе як вхідні дані (інформацію, яку ви будете використовувати для прийняття рішень), так і вихідні дані (результуючі рішення, передбачення чи відповідь). Мережа намагається вчитися на кожному з прикладів, обчислюючи результат для вихідних даних на основі наданих вхідних даних. Якщо вихідні дані мережі не збігаються з цільовим виходом, мережа виправляє себе, змінюючи свої внутрішні з'єднання. Цей метод спроб і помилок триває, доки мережа не досягне певного рівня точності. Як тільки мережа навчилася та була перевірена, ви можете надати нову вхідну інформацію, і це дасть деякий подальший прогноз. Ключем до розробки успішної нейронної мережі є чітке формулювання проблеми та збирання великої кількості відповідних даних.

Для більш наглядного прикладу, я дослідила нейронну мережу BrainMaker, яку використовувала Microsoft для прямої розсилки.

Microsoft використовувала нейронне мережеве програмне забезпечення BrainMaker, щоб максимізувати прибутки своїх прямих посилань. Щороку компанія відправляла близько 40 мільйонів прямих поштових листів, до 8,5 мільйона зареєстрованих клієнтів. Більшість цих прямих розсилок були спрямовані на те, щоб люди могли оновити програмне забезпечення або придбати супутні товари. До першої поштової розсилки входили усі, хто був у базі даних, але друга розсилка була лише для тих, хто, швидше за все, відповідав.

Таким чином, одним із головних плюсів BrainMaker'а є те, що ця нейронна мережа має більше функцій аналізу, ніж будь-яка інша, як для вихідних даних, так і для вже навчених нейронних мереж.

Але, на мій погляд точність мереж, які ми будемо і використовуємо (наприклад, той самий - BrainMaker), виявляється незадовільною, або взагалі не дає відповідних результатів чи не може досягти високих позицій в таблицях лідерів. Тому щоб уникнути цього, можна використати деякі способи для підвищення їх ефективності.

Перш за все, для того, щоб поліпшити НМ, я хочу запропонувати використання перевірки на перенавчання. Задля цього, потрібно перевірити нейронну мережу на його існування. Надмірне перенавчання відбувається тоді, коли модель НМ починає запам'ятовувати значення з навчальних даних, замість того, щоб вчитися на їх основі. Коли точність навчання набагато вища, ніж точність тестування, тоді НМ перенавчається. Для того, щоб уникнути цього, потрібно слідкувати за випадковими з'єднаннями між нейронами (Dropouts), паралельно змушуючи мережу знаходити нові шляхи та узагальнювати дані.

Також на мій погляд, можна покращити структуру нейронної мережі, шляхом додавання додаткового прихованого шару нейронів. Це дасть можливість досягти більшої точності, навіть якщо буде використано більше ресурсів. Для визначення помилок в режимі навчання нейромережі і прихованих шарів, зокрема, можна скористатися різними системами візуалізації внутрішнього процесу.

Як висновок, я хочу сказати, що мною було проведено дослідження нейронних мереж, та проаналізовано мережі на прикладі НМ - BrainMaker. Нейронні мережі - це потужний, але при цьому нетривіальний прикладний інструмент. Кращий спосіб навчитися будувати робочі нейромережеві конфігурації - починати з простіших моделей і багато експериментувати та напрацьовувати досвід.

Список використаних джерел

1. What is an artificial neural network? Here's everything you need to know [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: [https://www.digitaltrends.com/cool-tech/what-is-an-artificial-neural-network/..](https://www.digitaltrends.com/cool-tech/what-is-an-artificial-neural-network/)
2. Neural Network Analysis [Електронний ресурс] – Режим доступу до ресурсу: <http://www.ecommerce-digest.com/neural-networks.html>.
3. Neural network models (supervised) [Електронний ресурс] – Режим доступу до ресурсу: https://scikit-learn.org/stable/modules/neural_networks_supervised.html.

УДК: 004

ІНТЕРНЕТ РЕЧЕЙ ЯК ПРИЧИНА ВИНИКНЕННЯ НОВИХ КІБЕРЗАГРОЗ

Зубчевська А.О., студ.гр. КБ-161

Петренко Т.А., ст. викладач кафедри кібербезпеки та математичного моделювання
Чернігівський національний технологічний університет

Інтернет речей (Internet of Things – IoT) - одна з найпопулярніших концепцій у науці прогнозування майбутнього, футурології, яка складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані сенсори, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами, за допомогою використання стандартних протоколів зв'язку. Такі мережеві протоколи представляють собою набори правил, і дозволяють здійснювати з'єднання і обмін даними між двома і більше підключеними до мережі пристроями.[1]

Сьогодні поняття «інтернет речей» включає в себе відразу кілька явищ. Це і самі пристрої, які підключені до глобальної мережі і взаємодіють між собою. Це і спосіб підключення - M2M - тобто машина-до-машина, без участі людини. Це і великі об'єми даних, які тепер генерують ці пристрої. [2]

У 2018 році кількість пристроїв, підключених до Інтернету, за даними Statista, перевищила 20 млрд. штук. За прогнозами компанії Cisco до 2020 їх буде вже близько 50 млрд.[3] Інтернет речей - це не тільки розумний холодильник, який сам замовляє їжу для господаря, або чайник, який кип'ятить воду за командою зі смартфона. Це також і розумні датчики на полях, дрони з камерами, завдяки яким можна віддалено моніторити стан ґрунтів, це датчики у громадському транспорті та єдині системи «розумне місто» для моніторингу всіх сфер життя сучасних мегаполісів. Саме тому можна припустити, що вже за декілька років світ навколо нас стане дійсно цифровим, і людство скрізь буде оточувати інтернет речей.

У Австралії вже зараз за допомогою переносних датчиків кожен лікар може відслідкувати стан здоров'я свого пацієнта та реагувати в режимі реального часу. У США мобільний оператор AT&T розробив систему, яка покликана вирішити одну із найнебезпечніших проблем для літніх людей –