B.M.S College of Engineering

P.O. Box No.: 1908 Bull Temple Road,
Bangalore-560 019

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

Course – Computer Networks - 2
Course Code – 20IS6PCCON
AY 2021-2022

ML in Computer Networks

Submitted to – Yogesh N
(Assistant Professor)

Submitted by -
Prashanth Jaganathan 1BM19IS115
Prateek M Gummaraju 1BM19IS117
Pruthvi Shetty 1BM19IS122
Sai Dhruv 1BM19IS136
Samartha S 1BM19IS219

B.M.S College of Engineering

P.O. Box No.: 1908 Bull Temple Road,
Bangalore-560 019

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

BMS COLLEGE OF ENGINEERING

(Autonomous College under VTU)
Bull Temple Road, Basavanagudi, Bangalore – 560019

C E R T I F I C A T E

This is to certify that the presentation entitled "**ML in Computer Networks**" is a bona-fide work carried out by by **Prashanth Jaganathan, Prateek Gummaraju, Pruthvi Shetty, Sai Dhruv and Samartha S** bearing USN: **1BM19IS115**, **1BM19IS117**, **1BM19IS122**, **1BM19IS136** and **1BM19IS219** respectively, in partial fulfillment of the requirements for the VI Semester degree in **Bachelor of Engineering in Information Science & Engineering** of **Visvesvaraya Technological University, Belgaum** as a part of for the **course Computer Networks - 2, Course Code - 20IS6PCCON** during academic year 2021-2022

Faculty Name: Yogesh N

Designation: Assistant Professor

Signature:

Table of Content

Abstract

Recently, machine learning has been used in every possible field to leverage its amazing power. For a long time, the networking and distributed computing system has been the key infrastructure to provide efficient computational resources for machine learning. Networking itself can also benefit from this promising technology. This report focuses on the application of ML in Networking, which can not only help solve the intractable old network questions but also stimulate new network applications. In this article, we summarize the basic workflow to explain how to apply machine learning technology in the networking domain. Then we provide a selective survey of the latest representative advances with explanations of their design principles and benefits. These advances are divided into several network design objectives and the detailed information of how they perform. Finally, we shed light on the new opportunities in networking design and community building of this new inter-discipline.

Introduction

Machine learning is a branch of AI focused on programming computers to solve problems without human involvement.

Network performance management, security and health management tools all use ML to power better analytics. ML-based tools are excellent at learning normal network behavior and highlighting relatively abnormal actions. The tools implement one or more computational models, such as neural networks or genetic algorithms, to improve a pattern-matching algorithm.

The behavior of biological neurons serves as the basis for neural networks. Artificial neurons, or software, connect to each other in layers. Neurons in one layer send signals to neurons in the next, along weighted connections. Receiving signals of sufficient strength triggers a neuron to send an output: normal or abnormal. Through a training process, the ML system tunes the sent signals and the weightings on the connections.

Genetic algorithms also draw inspiration from nature. Developers start with multiple methods of identifying the correct output based on input data and then use ML to mimic what nature does: weed out the least-fit methods, mix and mutate the survivors, and repeat the cycle to improve results over time.

Why Machine Learning?

- **Explosion in the availability of data**
    - Colossal amount of data in today's networks.
    - It is bound to grow further with technologies like IoT and its billions of connected devices.
- **Significant improvements in ML techniques**
    - Techniques more flexible and resilient in their applicability to various real-world scenarios, e.g. ML in health for medical imaging and computer-aided diagnosis.
- **Advancement in computing capabilities**

- Storage and processing capabilities for training and testing ML models for the voluminous data, e.g. Cloud Computing

Networking Challenges

- Each network is unique and there is a lack of enforcement standards to attain uniformity across networks.
- The network is continually evolving and the dynamics inhibit the application of a fixed set of patterns that aid in network operation and management.
- We have a huge amount of data and it comes very fast and is very diverse.

Applications of Machine Learning in Networking

Incorporating machine learning tools into a network can help teams predict traffic flows, generate smarter analytics, monitor network health, tighten security measures and more.

ML tools can help with moment-by-moment traffic management, as well as longer-range capacity planning and management. After the tools identify when traffic spikes in some paths or fails to flow in others, they can send automated or manual direct management responses to correct the error.

Beyond management in the moment, ML tools can also predict traffic trends in ways that help guide future decisions. Network professionals should evaluate situations where it could be beneficial to use a ML tool to determine traffic flows, such as in the following examples:

- Is traffic in the data center shifting from rack-to-rack to server-to-server within a rack?
- Is traffic shifting from large numbers of small-packet flows to smaller numbers of large-packet flows?

Spotting trends can help IT determine what kinds of networks to design, such as leaf-spine, switch-based mesh or host-based mesh. The more data ML tools have access to across all segments of a network, the more detailed their analysis and recommendations can be. ML tools are especially helpful with root cause analysis.

Combining ML-driven analytics with other AI tools, like natural language processing, can make interacting with the systems easier and faster. Network engineers can create virtual assistants to help network administrators diagnose and fix network issues.

Applications of Machine Learning in Network Security

Network security and Cyber security are extremely important for organizations all over the world. Machine learning has many applications in Network security such as identifying threats, combating attackers etc.

Network security is any activity designed to protect the usability and integrity of your network and data.

- It includes both hardware and software technologies
- It targets a variety of threats
- It stops them from entering or spreading on your network
- Effective network security manages access to the network
- Examples: Firewalls, Email Security, Anti-virus, Network Segmentation

In network security, machine learning continuously learns by analyzing data to find patterns so we can better detect malware in encrypted traffic, find insider threats, predict where “bad neighborhoods” are online to keep people safe when browsing, or protect data in the cloud by uncovering suspicious user behavior.

The following are the application of ML in Network Security:

1. **Find threats on network:**
   Machine learning detects threats by constantly monitoring the behavior of the network for anomalies. Machine learning engines process massive amounts of data in near real time to discover critical incidents. These techniques allow for the detection of insider threats, unknown malware, and policy violations. A cyber threat identification system that is powered by ML can be used to monitor all outgoing and incoming calls as well as all requests to the system to monitor suspicious activity. For example, Versive is an artificial intelligence vendor that provides cybersecurity software in conjugation with ML.

2. **Keep people safe when browsing:**
   Machine learning can predict “bad neighborhoods” online to help prevent people from

connecting to malicious websites. Machine learning analyzes Internet activity to automatically identify attack infrastructures staged for current and emergent threats.

3. **Provide endpoint malware protection:**

   Algorithms can detect never-before-seen malware that is trying to run on endpoints. It identifies new malicious files and activity based on the attributes and behaviors of known malware.

4. **Detect malware in encrypted traffic :**

   Machine learning can detect malware in encrypted traffic by analyzing encrypted traffic data elements in common network telemetry. Rather than decrypting, machine learning algorithms pinpoint malicious patterns to find threats hidden with encryption.

5. **Fraudulent theft:**

   Fraud theft is a very common attack and traditional methods have failed to prevent or detect attacks of sensitive identity theft. Because conventional security measures are lacking in speed and accuracy of capturing harmful links sent to the user to hide something familiar. Therefore, the solution to the problem lies in URL guess models based on the latest machine learning algorithms that can identify patterns that reflect the emails of the malicious sender. Models are trained to detect minor behaviors (important features) such as email titles, body data samples, writing patterns, etc.

Applications of Machine Learning in Network Management

What is Network Management?

Network management is the sum total of applications, tools and processes used to provision, operate, maintain, administer and secure network infrastructure. The overarching role of network management is ensuring network resources are made available to users efficiently,
effectively and quickly. It leverages fault analysis and performance management to optimize network health.

A network brings together dozens, hundreds or thousands of interacting components. These components will sometimes malfunction, be misconfigured, get over utilized or just fail. Enterprise network management software must respond to these challenges by employing the best suited tools required to manage, monitor and control the network.

Role of Machine Learning in Network Management

Machine learning can ultimately automate many of the processes network managers must do manually. For example, machine learning algorithms can predict potential network problems prior to them happening. They can pinpoint capacity requirements early. These algorithms can also identify user network problems and make recommendations to fix them. Machine learning takes the questioning out of the network management game and instead allows managers to get to the bottom of network issues fast, without pointing fingers.

As a network manager, being able to pinpoint problems that fast would change the way you work and use your time on a daily basis. You would be able to start fixing network issues before they became too large and brainstorm on ways to improve the network for the future.

The best part is that Machine learning uses the data that is already running throughout your network, without the need to use extra servers or software. ML requires large amounts of data to

be fed through its system in order to work properly. In some industries, this is incredibly difficult. Within network management, data is already abundant, making it easy for a machine learning solution to be utilized daily.

In network management, there are many issues that require a quick response. There are four areas of network management where AI is being used to address these time-sensitive problems. They are:

- Traffic management
- Performance monitoring
- Capacity planning
- Security monitoring

In most of these cases, ML is proving to be the biggest aide in addressing problems of all AI techniques.

Many problems associated to networking can be formulated as a *prediction* or *classification* problem.

Traffic prediction: Depends on whether the traffic prediction is performed with direct observations or not, there are two research directions:

- Time series analysis for traffic prediction with direct observations. However, it is sometimes difficult to observe in the context of large-scale and high speed network environment.
- Network tomography which predicts traffic using indirect metrics either (1) with engineered features with domain knowledge or (2) using machine/deep learning approaches for end-to-end learning, i.e., learning high-level features automatically.

Traffic classification: This aims to match network applications & protocols with the corresponding traffic flows. As the misclassfication causes a big cost in the context of

networking, it is challenging to deal with robustness such as how the devised model performs on unknown traffic.

Resource prediction: In order to improve the network performance in a cost efficent way, there are many dynamic allocation problems to deal with such as assigning optimal number of Virtual Machines (VMs). The fundamental step is predicting resource usage, e.g., predicting the CPU consumption based on traffic features.

CONCLUSION

Machine learning is essential in many ways in traditional computer networks to enhance computer networking capabilities. For instance, in Network performance management, security and health management tools all use ML to power better analytics. ML-based tools are excellent at learning normal network behavior and highlighting relatively abnormal actions. The tools implement one or more computational models, such as neural networks or genetic algorithms, to improve a pattern-matching algorithm.Artificial neurons, or software, connect to each other in layers. Neurons in one layer send signals to neurons in the next, along weighted connections. Receiving signals of sufficient strength triggers a neuron to send an output: normal or abnormal. Through a training process, the ML system tunes the sent signals and the weightings on the connections. Ml is also needed for network performance management ML tools can help with moment-by-moment traffic management, as well as longer-range capacity planning and management. After the tools identify when traffic spikes in some paths or fails to flow in others, they can send automated or manual direct management responses to correct the error.

REFERENCES

1. https://www.cisco.com/c/en/us/products/security/machine-learning-security.html
2. Stream-based Machine Learning for Network Security and Anomaly Detection by Mulinka, Casas
3. Impact of Machine Learning in Various Network Security Applications by Banerjee, Maiti, Chakrabothy
4. Machine Learning on Networks by Surya
5. https://www.networkmanagementsoftware.com/machine-learning-network-management/
6. https://www.networkworld.com/article/3587131/machine-learning-in-network-management-has-promise-challenges.html