



Computer Networks 2

AAT

▪ ML IN NETWORKS ▪

Submitted to
Mr. Yogesh N
Assistant Professor, Dept. of ISE

Prashanth Jaganathan
(1BM19IS115)

Prateek Gummaraju
(1BM19IS117)

Pruthvi Shetty
(1BM19IS122)

Samartha S
(1BM19IS219)



Sai Dhruv
(1BM19IS136)

INTRODUCTION

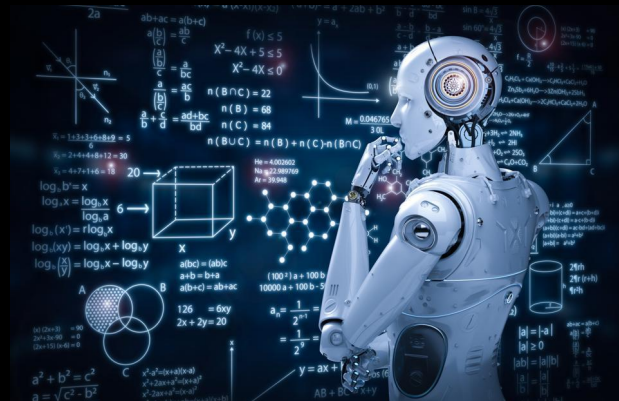
What is Machine Learning?

"Machine Learning is the field of study that gives computers the ability to learn without being explicitly programmed"

Arthur L. Samuel, 1959



- The goal of ML is to identify and exploit hidden patterns in “training” data.
- The patterns learnt are used to analyze unknown data, such that it can be grouped together or mapped to the known groups.



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.
 - ❖ Some applications are in Network Security, Network Management, Traffic classification, Performance prediction, Fault Management, etc.
- 


MACHINE LEARNING IN NETWORKS

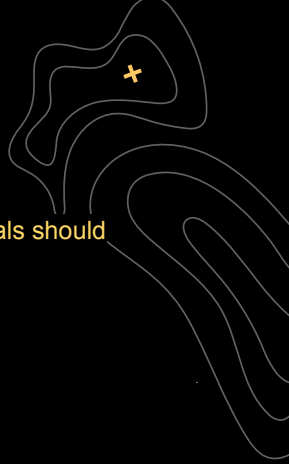


Incorporating machine learning tools into a network can help teams predict traffic flows, generate smarter analytics, monitor network health, tighten security measures and more.

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.






Network analytics

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.

ML IN NETWORK SECURITY




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 principle, machine learning can help businesses better analyze threats and respond to attacks and security incidents. It could also help to automate more menial tasks previously carried out by stretched and sometimes under-skilled security teams.

Google is using machine learning to analyze threats against mobile endpoints running on Android — as well as identifying and removing malware from infected handsets



How machine learning helps network security



Find threats on a network

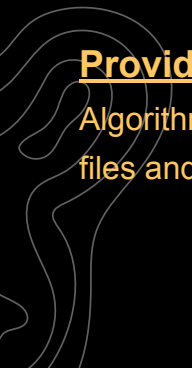
Machine learning detects threats by constantly monitoring the behavior of the network for anomalies. Machine learning engines process massive amounts of data in near real time to discover critical incidents. These techniques allow for the detection of insider threats, unknown malware, and policy violations.

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.

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.



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.

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.




ML IN NETWORK MANAGEMENT



WHAT IS NETWORKING 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.



HOW DO WE LEVERAGE MACHINE LEARNING FOR 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.

HOW DO WE LEVERAGE MACHINE LEARNING FOR NETWORK MANAGEMENT?



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.



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.

CONCLUSION

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.

THANK YOU

