Including P4 and AI: A Survey on SDN Security

Xiang Li, *Yeonjoon Lee
Major in Bio Artificial Intelligence, Dept. of Computer Science and Engineering, Hanyang University
*Dept. of Computer Science and Engineering, Hanyang University

lx913247225@hanyang.ac.kr, yeonjoonlee@hanyang.ac.kr

P4 와 AI 포함된 SDN 보안 기술 동향 연구

이향, * 이연준
한양대학교 컴퓨터공학과 바이오인공지능융합전공 석사과정
* 한양대학교 컴퓨터공학과 교수

Abstract

SDN (Software Defined Networking) is an emerging networking system which differs from traditional network architecture. Moreover SDN has many advantages and special capabilities that traditional networks do not have. SDN and P4 are related in that they can be combined to create more advanced and intelligent networking systems. Additionally, AI has emerged as a transformative force in various fields, including SDN. By applying AI and P4 to SDN, network administrators can leverage the power of them to make impact on SDN security. We offer an overview of recent trend of SDN security integrating P4 and AI in this study.

I Introduction

SDN is an important implementation method of NFV (Network Functions Virtualization), SDN is different from traditional networks. For network management, both SDN and traditional networks have control plane and data plane (or forwarding plane). Figure 1 show distributed control and management in traditional networks, control plane and data plane are coupled together in individual hardware device. Whereas in SDN, control plane and data plane are decoupled and separated, and control plane is centralized in a controller that manages countless devices.

Such structure gives SDN many advantages over traditional networks. From the perspective of administrators, because of the centralized controller, SDN enables them to manage traffic flows centrally rather than having to configure each device separately, through software rather than hardware with abstraction of lower-level functionality. This makes it easier to manipulate network resources, which can become more agile and responsive network performance, cost savings, even automation in productivity.

And thus the centralized controller provide a panoramic view over all the hardware devices in data plane, SDN has great flexibility, maintainability, scalability. It allows network administrators to quickly and easily adapt to changing network requirements instead of complex and inflexible network policy changes in traditional networks, they can create new network services and modify existing ones without having to make changes to the underlying hardware. they also can fastly and clearly spot and locate faults then solve them.

Besides, administrators can implement security policies centrally and enforce them throughout the network. This can help prevent unauthorized access and protect against security threats, finally achive better network security.

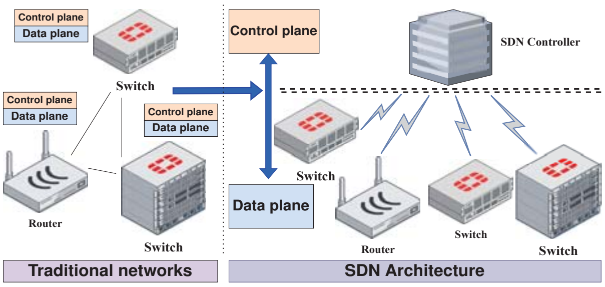

Figure 1: **Comparison**

The controller is the core of SDN, SDN controller plays the following roles: separates data plane and control plane, enables centralized networking, provides open interfaces. Through NBI (NorthBound Interface) and SBI (SouthBound Interface), under certain protocols, SDN controller connects with application plane and data plane respectively.

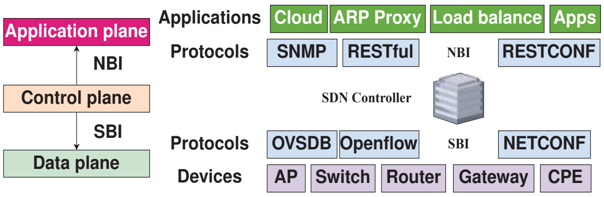

Figure 2: **SDN controller**

Figure 2 depicts how the controller works. The application plane provides interface directly to users, so we can add different applications into the controller for various intend. SDN applications are rich in capabilities, including network monitor, load balance, quality of service (QoS), controlling various elements in SDN by sending instructions to network devices through SDN controllers. In SBI, the most important protocol is Openflow, which defines a standard interface between controller and switch that allows controller to handle switch's behavior, such as routing, forwarding, filtering, etc. Openflow protocol is standardized by ONF (Open Networking Foundation), until now it has evolved many versions.

SDN has become increasingly popular particularly in large data center, there are lots of rich communities and perfect ecosystem now, significantly enriched edge computing and cloud platform. To date, the research on SDN is combined with some novel techniques, such as P4 and AI, the technological convergence has been a great achievement. The rest of this paper presents these research trend in detail.

II SDN with P4

P4 is the short of "Programming Protocol-independent Packet Processors", P4 is a high-level domain-specific language (DSL) for forwarding devices that defines how packets are processed within devices in the data plane: switches, routers, Network Interface Cards (NICs). P4 works in conjunction with SDN and Openflow protocol. P4 has these features: (1) Reconfigurability: Programmers can change the way switches process packets once they are deployed. (2) Protocol-independence: Switches are not tied to any specific network protocols. (3) Target-independence : Programmers can describe packet processing functionality independently of the specifics of underlying hardware.

Nowadays P4 is always associated with "Programmable Switches and ASIC (Application Specific Integrated Circuit)". If a switch or chip is programmable and applicable to P4 language, P4 compiler can generate executable P4 program (prog.p4) that classifies packets' actions. PISA (Protocol Independent Switch Architecture) is also standardized by ONF, it actually has become the standard architectural model for factories to manufacture programmable switches. Data-plane-programmability and Openflow-based SDN gave opportunities for customizing protocol headers beyond TCP/IP, and P4 program is a completely hardware-level operation, running at line-speed, this hardware feature means a significant improvement in packet processing speed.

P4 is gaining traction from industry and academia, to the best of our knowledge, recent years, P4-enabled switches achieved a variety of goals especially in cybersecurity. Kang et al.[1] utilized P4 and programmable control plane to enforce CAS (Context-Aware Security) policies without involving SDN controller, they innovated new security primitives that runs in client-side devices and change defense decisions at hardware speeds, their system *POISE* is highly efficient and resilient over traditional SDN defenses, increasing reliability in this Bring Your Own Device (BYOD) era. Zhang et al.[2] developed a runtime management mechanism to mitigate dynamic Distributed DDoS (Denial-of-Service) attacks, they used SmartNICs and created a new language or orchestration *POSEIDON* for policy abstraction that provides transparent scheme and shield the low-level hardware complexity from programmers. Xing et al.[3] published new language *Ripple* for preventing LFA (Link-flooding attack), a new type of DDos attacks aiming to overwhelm the target (link)'s bandwidth and resources instead of nodes or terminals. *Ripple* decentralized defense in P4-enalbled switches in order to deal with the crisis of very fast adaptive LFA attacks, and to solve the key chanllenge that switches only see loccal signals, specifying needed panoramic views via some primitives in *Ripple* language, *Ripple* provided different panorama for network operators to program defense policies easily. Xing et al.[4] developed *Bedrock* for Secure RDMA (Remote direct memory access) systems which has gained popularity in cloud datacenters. *Bedrock* bypass server CPUs, operates transparently to legacy RDMA systems, secures the datapath traffic directly inside the network, it's feasible to develop datapath defenses that operate at hardware speeds. AlSabeh et al.[5] combined P4 and DPI (Deep Packet Inspection) method, developing *P4DDPI* (P4 for Domain name DPI) to parse and filter domains in the data plane without using the control plane. In this way, the flow pressure of the SDN controller can be greatly reduced without the need to check the flow packets through the SDN controller, the resources occupied by the P4 program are negligible, allowing other security and networking features to be implemented. Zhang et al.[6] leveraged P4 to analyze the limitations of the traditional HCF (Hop-Count Filtering) designs, proposeing *NetHCF*, a line-rate in-network system twoards Spoofed IP Traffic. Chinprutthiwong et al.[7] come up with *SWAPP*, which means Service Worker APplication Platform, *SWAPP* is a framework for implementing security mechanisms inside a service worker allowing web developers to offload a part of security tasks from server to client and enables deployment of emerging security features. Zhou et al.[8] proposed an IDP (Intelligent Data Plane) named *NetBeacon*, a novel design in which machine learning models are directly deployed, thus intelligent traffic analysis is at line-speed using data-driven models rather than predefined protocols. They deploy the programming to real-world devices, proving the product's effectiveness.

Academics praise SDN as the future of computer networks and P4 as the future of SDN, believing that P4 has made all the SDN's ideas come true, P4 is the real SDN.

III SDN with AI

AI (Artificial Intelligence) bring a lot to SDN: (1) Intelligent routing: SDN controller can use AI to learn network topology and traffic patterns thus dynamically adjusting QoS and optimizing routing policies accordingly to maximize network performance and throughput ensuring that requirements are met. (2) Predictive maintenance: SDN controller can monitor network connectivity, via AI to predict equipment failures and bottlenecks in advance, take appropriate measures to repair and avoid. (3) Traffic classification: AI help to identify traffic, then detect threats or abnormal, malicious traffic finally take steps to isolate affected device.

Research combining AI and SDN is a trendy topic, even ”AI+SDN+P4” such topic has emerged. Both ML (Machine Learning) and DL (Deep Learning) are critical branches of AI, and DL is subordinate to ML. Through AI approachs, there are very successful academic achievement in SDN secutiry. Bhardwaj et al.[9]was motivated by operational impact and trigger mechanism of bugs in SDN, so employed NLP (Natural Language Processing) to analysis existing bugs in several open-source SDN controllers, delivering a thorough understanding of these challenges to the whole SDN community. Zhou et al.[8] and Musumeci, et al.[14] leveraged ”AI+SDN+P4” to overcome SDN security problem.

Table 1 depicts previous works for DDoS mitigation in SDN, the literature that appears in conferences and journals.

Table 1: **Summary of ”AI+SDN” considered**

Author	Merits	Models
[10]	Collaboration of existing defense tools with AI algorithm	Stacked Autoencoders (SAE)
[11]	Validation of efficiency compared to other neural networks	Generative Adversarial Network (GAN)
[12]	Benchmarking several state-of-the-art ML models for evaluation	Recurrent Neural Network (RNN) with autoencoder
[13]	Comprehensive tests on five popular public datasets	Long Short-Term Memory (LSTM)
[14]	Experiments in three real-time scenarios, combination of P4 code and ML classifiers	Random Forest (RF), K-Nearest Neighbours (KNN), Support V ector Machine (SVM) and P4

SDN is the future of computer networks, AI is the future of human bings, AI and SDN already have a tight relationship, it’s of great academic value to bring them together to study.

IV Conclusion

This paper briefly introduces recent research on SDN security including P4 and AI. With the widespread use of SDN plus P4 and AI, it will be tremendous progress of this aspect.

ACKNOWLEDGMENT

This work was partly supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.RS-2022-00155885, Artificial Intelligence Convergence Innovation Human Resources Development (Hanyang University ERICA)) and Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2020-0-01343, Artificial Intelligence Convergence Research Center(Hanyang University ERICA)).

References

[1] Kang, Qiao, et al. ”Programmable in-network security for context-aware BYOD policies.” USENIX Security. 2020.

[2] Zhang, Menghao, et al. ”Poseidon: Mitigating volumetric ddos attacks with programmable switches.” the 27th Network and Distributed System Security Symposium (NDSS 2020).

[3] Xing, Jiarong, Wenqing Wu, and Ang Chen. ”Ripple: A programmable, decentralized link-flooding defense against adaptive adversaries.” USENIX Security. 2021.

[4] Xing, Jiarong, et al. ”Bedrock: Programmable Network Support for Secure RDMA Systems.” 31st USENIX Security Symposium (USENIX Security 22). 2022.

[5] AlSabeh, Ali, et al. ”P4DDPI: Securing P4-Programmable Data Plane Networks via DNS Deep Packet Inspection.” Proceedings of the 2022 Network and Distributed System Security (NDSS) Symposium. 1ś7. 2022.

[6] Zhang, Menghao, et al. ”NetHCF: Filtering Spoofed IP Traffic With Programmable Switches.” IEEE Transactions on Dependable and Secure Computing (2022).

[7] Chinprutthiwong, et al. ”SWAPP: A New Programmable Playground for Web Application Security.” 31st USENIX Security Symposium (USENIX Security 22). 2022.

[8] Zhou, et al. ”An Efficient Design of Intelligent Network Data Plane.” 32nd USENIX Security Symposium (USENIX Security 23). Anaheim, CA: USENIX Association. 2023.

[9] Bhardwaj, Ayush, Zhenyu Zhou, Theophilus A. Benson. ”A Comprehensive Study of Bugs in Software Defined Networks.” 2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). IEEE, 2021.

[10] Ujjan, et al. ”Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN.” Future Generation Computer Systems 111 (2020): 763-779.

[11] Novaes, et al. ”Adversarial Deep Learning approach detection and defense against DDoS attacks in SDN environments.” Future Generation Computer Systems 125 (2021): 156-167.

[12] Elsayed, Mahmoud Said, et al. ”Ddosnet: A deep-learning model for detecting network attacks.” 2020 IEEE 21st International Symposium on” A World of Wireless, Mobile and Multimedia Networks”(WoWMoM). IEEE, 2020.

[13] Zhou, Hongliang, et al. ”Collaborative prediction and detection of DDoS attacks in edge computing: A deep learning-based approach with distributed SDN.” Computer Networks 225 (2023): 109642.

[14] Musumeci, et al. ”Machine-learning-assisted DDoS attack detection with P4 language.” ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020.