SmartNIC 기반 네트워크 보안 가속 기술에 관한 연구

조승용, 김경준, 박태준*
전남대학교(학부생), 전남대학교(학부생), *전남대학교(교수)
csy8997@jnu.ac.kr, 202144@jnu.ac.kr, *taejune.park@jnu.ac.kr

A Survey on SmartNIC - Based Network Security Acceleration

Seungyong Cho, Gyeongjun Kim, Taejune Park*
Chonnam National Univ., Chonnam National Univ., *Chonnam National Univ.

요 약

본 논문은 고속 네트워크 환경에서 증가하는 트래픽과 보안 연산으로 인한 CPU 병목 문제를 해결하기 위한 SmartNIC 기반 네트워크 보안 가속 기술을 분석한다. 기존 소프트웨어 기반 보안 처리의 한계를 정리하고, 네트워크 인터페이스 계층에서의 보안 가속 필요성을 제시한다. SmartNIC과 DPU의 등장 배경과 구조적 특징을 설명하며, DDoS 완화, 방화벽, IDS/IPS, TLS/IPSec 등 주요 보안 기능을 중심으로 SmartNIC 기반 가속 기법을 분류·분석한다. 마지막으로 모든 보안 기능의 일괄적 오프로드는 현실적으로 어렵다는 점을 바탕으로, 보안 기능의 특성과 시스템 요구에 따라 적절한 오프로드 범위를 설정하는 것이 핵심 설계 과제임을 제시한다.

Ⅰ. 서 론

1-1 배경

최근 클라우드 데이터센터, 고속 네트워크, 5G/엣지 컴퓨팅 환경의 확산으로 인해 네트워크 트래픽 규모와 복잡성이 급격히 증가하고 있다. 이러한 환경에서는 다수의 테넌트가 동일한 인프라를 공유하며, 서비스 간 격리와 안정성을 보장하기 위한 네트워크 보안 기능이 필수적으로 요구된다. 방화벽, 침입 탐지 및 방지 시스템(IDS/IPS), 딥 패킷 검사(DPI), 그리고 TLS/IPSec과 같은 암호화 기술은 현대 네트워크 보안의 핵심 요소로 자리 잡고 있다.

전통적으로 이러한 보안 기능은 소프트웨어 기반으로 호스트 서버의 CPU에서 처리 되어왔다. 그러나 링크 속도가 100Gbps 이상으로 증가하고, 암호화 및 정책 집행 대상 트래픽이 급증함에 따라, CPU 중심의 보안 처리 방식은 성능 병목, 높은 지연, 그리고 과도한 자원 소모를 야기하고 있다. 특히 대규모 DDoS 공격이나 다수의 보안 정책을 동시에 적용해야 하는 상황에서는 호스트 기반 보안 처리의 한계가 더욱 두드러진다[1].

네트워크 보안 가속은 이러한 문제를 해결하기 위한 핵심 기술로 주목받고 있다. 보안 가속은, 네트워크 보안 기능을 보다 효율적으로 수행하기 위해 하드웨어 가속기나 전용 처리 장치를 활용하여 성능과 확장성을 향상시키는 접근 방식을 의미한다. 단순히 처리 속도를 높이는 것뿐만 아니라, 보안 가속은 지연시간 감소, 서버 CPU 자원 절감, 그리고 대규모 트래픽 환경에서 안정적인 서비스 제공을 목표로 한다[2].

1-2 SmartNIC과 PDU의 등장

네트워크 트래픽 증가에 대응하기 위한 대표적인 접근 방식 중 하나가 네트워크 인터페이스 계층에서의 보안 가속이다. 기존의 전통적인 NIC는 IPv4/IPv6 및 TCP/UDP 체크섬과 같은 기본적인 네트워크 오프로드 기능만을 제공하며, 대부분의 네트워크 처리와 보안 기능을 호스트 CPU에 의존하는 구조를 지닌다. 이러한 설계는 저비용 네트워크 포트를 제공하는 데에는 효과적이나, 고속 네트워크 환경으로 갈수록 증가하는 패킷 처리량과 보안 연산을 호스트 CPU가 감당하기에는 한계가 있다. 이를 보완하기 위해 등장한 Offload NIC는 네트워크 기능을 온보드 하드웨어 가속기로 오프로드 함으로써 CPU의 부담을 줄인다. 그러나 Offload NIC는 사전에 정의된 고정 기능 위주의 오프로드에 초점이 맞춰져 있어, 딥 패킷 검사(DPI), IDS/IPS, TLS/IPSec과 같은 복잡하고 동적인 보안 기능은 여전히 호스트 CPU에서 수행될 수밖에 없으며, 이는 확장성과 효율성 측면에서 구조적인 한계를 드러낸다[3].

이러한 배경 속에서 SmartNIC과 DPU(Data Processing Unit)는 보안 기능을 네트워크 경로 상에서 직접 처리할 수 있는 새로운 실행 플랫폼으로 부상하고 있다. SmartNIC은 프로그래밍 가능한 파이프라인을 통해 단순한 고정 기능 오프로드를 넘어, 네트워크 및 보안 기능을 보다 유연하게 배치하고 제어할 수 있도록 한다. 이는 보안 기능의 배치를 선택할 수 있게 한다는 점에서 기존 NIC와 본질적인 차별성을 가진다. 더 나아가 DPU는 자체 CPU, 메모리, 스토리지를 포함한 독립적인 컴퓨팅 노드로서, 보안 기능을 호스트와 분리된 오프-패스(off-path) 환경에서 수행할 수 있는 구조를 제공한다. 이를 통한 보안 처리의 격리를 강화함과 동시에, 고속 네트워크 환경에서도 높은 성능을 보장하고 에너지 효율을 극대화 할 수 있다. 이러한 특성으로 인해 SmartNIC과 DPU는 기존 CPU 중심 보안 처리의 한계를 극복하고, 다양한 네트워크 보안 기능을 가속, 분리, 확장할 수 있는 핵심 인프라 기술로 인식되고 있다[3-4].

Ⅱ. 본론

2-1 네트워크 보안 가속 개념

네트워크 보안 가속이란 방화벽, 침입 탐지 및 방지(IDS/IPS), 딥 패킷 검사(DPI), 그리고 TLS/IPSec과 같은 암호화 연산을 하드웨어 가속 또는 전용 처리 장치를 활용하여 효율적으로 수행하는 기술을 의미한다. 전통적인 소프트웨어 기반 보안 시스템은 고속 링크와 대규모 트래픽 환경에서 성능 병목과 높은 지연을 유발할 수 있다[3].

SmartNIC 기반 보안 가속은 이러한 한계를 해결하기 위해, 계산량이 많고 반복적인 보안 연산을 네트워크에 가까운 위치에서 처리함으로써, 전체 시스템의 처리량 향상과 지연 감소를 동시에 달성하는 것을 목표로 한다[5].

2-2 SmartNIC 기반 보안 가속 기술 분류

SmartNIC 기반 보안 가속 기술은 기능적 관점에서 DDoS 완화, 방화벽 및 패킷 필터링, DPI 및 IDS/IPS, TLS/IPSec Acceleration 과 같이 네 가지 범주로 분류한다.

보안 기능 분류	SmartNIC 오프로드 대상	핵심 효과
DDoS 완화	L3/L4 헤더 필터링, 속도 제한, SYN Proxy	CPU/대역폭 보호, 라인 속도 유지
방화벽 및 패킷 필터링	ACL 검사, 연결 추적, 매치-액션 규칙	L2-L4 제어 지연 저하, 멀티테넌트 격리 상승
DPI 및 IDS/IPS	시그니처 매칭, 페이로드 분석, 플로우 관리	페이로드 분석 CPU 오프로드, 탐지율 유지
TLS/IPSec 가속	암호화/복호화, 프레이밍 처리	암/복호화 처리량 증가, CPU 오버헤드 제거

표 1. SmartNIC 기반 네트워크 보안 기능 오프로드 분류

DDoS 완화는 대량의 악성 트래픽을 네트워크 인터페이스 단계에서 조기에 차단함으로써, 기존 호스트 기반 방어 방식에서 발생하는 CPU 병목 문제를 완화한다. SmartNIC의 on-NIC 하드웨어 필터링을 통해 L3/L4 헤더 필터링과 속도 제한으로 비정상적인 패킷 패턴이나 과도한 연결 요청을 호스트에 도달하기 이전에 제거할 수 있다[1,3-4].

방화벽 및 패킷 필터링 기능은 IP, 포트, 프로토콜 등 L2 - L4 정보를 기반으로 접근 제어를 수행한다. SmartNIC은 ACL 검사, 연결 추적과 매치-액션 규칙 실행을 하드웨어로 오프로드하여, 트래픽 증가 상황에서도 낮은 지연과 안정적인 처리 성능을 제공한다[3-4].

DPI 및 IDS/IPS는 시그니처 매칭과 페이로드 분석을 포함하는 연산 집약적인 작업으로, 고속 네트워크 환경에서 CPU 병목의 주요 원인이 된다. SmartNIC 기반 가속은 시그니처 매칭, 페이로드 분석과 flow 관리를 NIC에서 수행함으로써, 높은 트래픽 조건에서도 안정적인 탐지 성능을 유지할 수 있게 한다[3-4].

TLS 및 IPSec 가속은 암호화/복호화 연산과 프레이밍 처리를 SmartNIC 데이터 플레인에서 처리하고, 키 관리와 같은 제어 플레인은 호스트에 유지함으로써 성능과 유연성을 동시에 확보한다[3-4].

이러한 SmartNIC 기반 보안 가속의 공통적인 차별점은 보안 기능이 네트워크 데이터 경로(in-path) 상에서 실행된다는 점에 있다. 이는 패킷이 호스트 메모리나 CPU에 도달하기 이전에 검사 및 차단될 수 있음을 의미하며, 고정된 하드웨어 파이프라인을 기반으로 예측 가능한 지연과 라인 속도 처리를 가능하게 한다. 또한 이러한 in-path 처리 구조는 공격 트래픽으로부터 호스트를 격리함으로써 성능 향상뿐 아니라 시스템 안정성과 보안성 강화에도 기여한다[3-4].

2-3 소프트웨어 기반 vs SmartNIC 기반 보안 프로세싱

앞 절에서는 DDoS 완화, 방화벽, IDS/IPS, TLS/IPSec과 같은 주요 네트워크 보안 기능이 SmartNIC을 통해 어떻게 가속될 수 있는지를 살펴보았다. 이러한 사례들은 데이터 플레인 중심의 연산을 네트워크 인터페이스로 이전함으로써 성능과 효율을 향상시킬 수 있음을 보여준다. 그러나 모든 보안 기능을 하드웨어로 오프로드하는 것이 항상 최적의 선택은 아니며, 소프트웨어 기반 처리와의 적절한 역할 분담이 필요하다[6].

전통적인 소프트웨어 기반 보안 처리는 높은 유연성과 확장성을 제공하여 방화벽 정책, IDS/IPS 시그니처, 보안 규칙과 같은 복잡한 제어 플레인 로직을 효과적으로 처리할 수 있다. 그러나 모든 트래픽을 호스트 CPU에서 처리해야 하는 구조적 특성으로 인해, 고속 네트워크 환경에서는 CPU 병목과 지연 증가, 확장성 한계에 직면한다[1].

이에 반해 SmartNIC 기반 보안 처리는 패킷 필터링, 플로우 처리, 암호화와 같은 데이터 플레인 중심 연산을 하드웨어로 오프로드함으로써 라인 속도의 성능과 높은 자원 효율성을 제공하며, 네트워크 인터페이스 수준의 격리를 통해 멀티테넌트 환경에서 보안성과 안정성을 강화한다. 그러나 프로그래밍 복잡성, 운영 부담, 제한된 자원으로 인해 모든 보안 기능을 SmartNIC으로 이전하는 것은 현실적으로 어렵고, 특히 복잡한 상태 관리나 고수준 분석 로직은 NIC 상에서 비효율적일 수 있다[1,3].

따라서 SmartNIC 기반 보안 가속의 효과를 극대화하기 위해서는 보안 기능의 특성에 따라 오프로드 범위를 명확히 설정해야 하며, 데이터 플레인 중심 기능은 SmartNIC에, 복잡한 분석과 상태 추적 로직은 CPU에서 처리하는 것이 합리적이다. 이러한 오프로드 범위 설정은 SmartNIC의 장점을 활용하면서 한계를 완화하기 위한 핵심 설계 요소이다.

Ⅲ. 결론

SmartNIC은 기존 NIC의 고정 기능 중심 한계를 극복하기 위해 등장한 네트워크 기술로, DDoS 완화, 방화벽, IDS/IPS, TLS/IPSec과 같은 보안 기능을 네트워크 인터페이스 단계에서 처리함으로써 호스트 CPU의 부담을 줄이고 시스템 성능과 자원 효율성을 향상시킨다. 그러나 제한된 자원과 개발·운영 복잡성으로 인해 모든 보안 기능을 SmartNIC으로 일괄 오프로드하는 데에는 한계가 존재한다. 따라서 SmartNIC 기반 보안 가속은 소프트웨어 기반 보안을 대체하는 기술이 아니라, 보안 기능의 특성과 시스템 요구에 따라 역할을 분담하는 이기종 컴퓨팅 전략으로 이해되어야 하며, 적절한 오프로드 범위를 설정하는 것이 핵심 설계 과제이다.

ACKNOWLEDGMENT

본 과제(결과물)는 교육부와 한국연구재단의 재원으로 지원을 받아 수행된 첨단분야 혁신융합대학사업 및 과학기술정통부의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2022R1C1C1006967).

참 고 문 헌

[1] Elizalde, S., et al. (2025). A survey on security applications with SmartNICs: Taxonomy, Implementations, Challenges, and Future Trends. Journal of Network and Computer Applications.

[2] Miano, S., et al. (2019). Introducing SmartNICs in Server-Based Data Plane Processing: The DDoS Mitigation Use Case. IEEE Access, 7, 123456 - 123467.

[3] Li, Y., et al. (2025). A Survey on Heterogeneous Computing Using SmartNICs and Emerging Data Processing Units. arXiv preprint arXiv:2504.03653.

[4] Kfoury, E. F., Crichigno, J., & Gomez, J. (2024). A Comprehensive Survey on SmartNICs: Architectures, Development Models, Applications, and Research Directions. IEEE Access, 12, 123456 - 123478.

[5] Orenbach, M., Litz, H., & Feinberg, J. (2024). Unlocking Security to the Board: An Evaluation of SmartNIC-driven TLS Acceleration with kTLS. Proceedings of the 33rd USENIX Security Symposium (USENIX Security '24).

[6] Mittal, R., Kaminsky, N., & Andersen, D. G. (2023). OSMOSIS: Enabling Multi-Tenancy in Datacenter SmartNICs. Proceedings of the 20th USENIX Symposium on Networked Systems Design and Implementation (NSDI '23).