악성 암호화 트래픽 기반 공격 방어를 위한 퍼지 해시 기반 고속 경량 침입 탐지 시스템

김소연[1], 이연지[2], 이진민[1], 이일구[3]
[1]성신여자대학교 미래융합기술공학과 박사과정
[2]성신여자대학교 융합보안공학과 박사과정
[3]성신여자대학교 융합보안공학과, 미래융합기술공학과 교수
sykim.cselab@gmail.com, 220247018@sungshin.ac.kr,
csewa56579@gmail.com, iglee@sungshin.ac.kr

Fuzzy Hash-based Fast and Lightweight Intrusion Detection System for Defending Malicious Encrypted Traffic-based Attack

So-Yeon Kim[1], Yeon-Ji Lee[2], Jin-Min Lee[1], Il-Gu Lee[1,2]
[1]Dept. of Future Convergence Technology Engineering, Sungshin Women's University
[2]Dept. of Convergence Security Engineering, Sungshin Women's University

요 약

최근 종단간 암호화 기술이 널리 적용됨에 따라, 이를 악용한 보안 위협 또한 증가하고 있다. 종래의 심층 패킷 분석(Deep Packet Inspection, DPI) 방식은 페이로드를 복호화하여 트래픽을 분석하므로 종단간 암호화 환경에 적용하기 어렵다. 또한, 동형암호는 연산 지연이 크기 때문에 실시간 탐지가 요구되는 환경에서는 실용적이지 않다. 본 논문에서는 복호화 없이 암호화된 트래픽을 효율적으로 탐지할 수 있는 퍼지 해시 기반 침입 탐지 시스템(Fuzzy Hash-based Intrusion Detection System, FH)을 제안한다. FH는 페이로드에서 퍼지 해시 값을 생성하고, 이를 별도의 제어 프레임으로 병렬 전송한 뒤, 머신러닝 탐지 모델을 통해 악성 여부를 판별한다. 실험 결과에 따르면, FH는 DPI 대비 전송 지연을 최대 11.41% 감소시키고, 스루풋을 12.88% 향상시켰다. 또한, 탐지 정확도를 유지하면서도 학습 시간과 메모리 사용량을 각각 최대 90.44%, 91.86% 개선하였다.

1. 서론

최근 인공지능 기반 공격과 자동화 도구의 확산으로 사이버 보안 위협이 고도화되고 있다. 개인정보 보호와 데이터 무결성 확보를 위해서 HTTPS(Hypertext Transfer Protocol Secure), TLS(Transport Layer Security) 등의 암호화 프로토콜과 종단간 암호화(end-to-end encryption) 기술이 보편적으로 사용되고 있다[1]. 그러나 암호화된 트래픽은 가시성이 낮아서 보안 장비가 위협 요소를 식별하는 데에 제약이 따른다[1]. 이러한 특성을 악용하여 암호화된 채널을 통해 탐지를 회피하거나, 악성 페이로드를 은닉하는 해킹 사고가 지속적으로 증가하고 있다. Zscaler의 2024년 암호화된 트래픽 기반 공격 보고서에 따르면, 분석된 공격 중 대략 87%가 TLS/SSL 기반 암호화 트래픽을 통해 수행되었으며, 이는 전년 대비 약 10% 증가한 수치로 보고되었다[2].

악성 트래픽을 탐지하는 방식 중 하나인 심층 패킷 분석(Deep Packet Inspection, DPI) 방식은 정확한 트래픽 분석이 가능하지만, 모든 패킷의 내용을 검사해야 하기 때문에 연산 비용이 크고 처리 시간이 길어지는 문제가 있다[3]. 또한, 암호화된 환경에서는 데이터 페이로드에 접근하기 위해서 복호화를 수행하므로, 종단간 암호화 환경에서는 적용하기 어려운 한계가 있다[1]. 이러한 한계를 보완하기 위해 복호화하지 않고 암호화된 데이터 연산이 가능한 동형암호 기술이 주목받고 있다[4]. 그러나 동형암호는 계산 복잡도와 처리 지연이 매우 커서 실시간 탐지가 요구되는 환경에서는 활용 가능성이 낮다[4]. 따라서 본 논문에서는 암호화된 악성 트래픽을 효율적으로 탐지할 수 있는 퍼지 해시 기반 침입 탐지 시스템(Fuzzy Hash-based Intrusion Detection System, FH)을 제안한다.

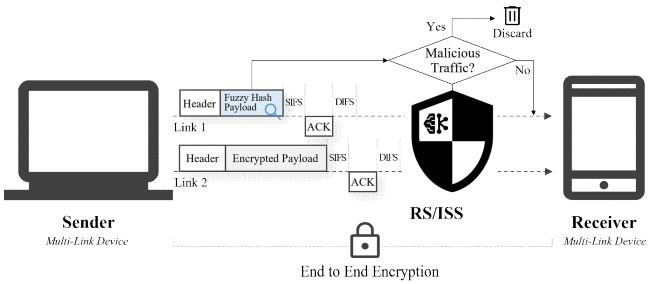
본 논문의 주요 기여점은 다음과 같다.

- 퍼지 해시 생성과 멀티링크 기반 병렬 전송 구조를 통해서 데이터 페이로드를 복호화하지

않고도 암호화된 트래픽을 빠르고 효율적으로 검사할 수 있는 시스템을 제안하였다.

- 제안하는 FH는 종래의 DPI 대비 전송 지연을 최대 11.41% 감소시키고, 스루풋은 12.88% 향상시켰다.
- FH는 DPI 대비 유사한 탐지 정확도를 유지하면서도 학습 시간은 최대 90.44%, 메모리 사용량은 91.86% 절감하였다.

2. Fuzzy Hash-based Intrusion Detection System



(그림 1) FH의 전체 구조도

그림 1은 제안 시스템의 전체 구조를 나타내며, 송신자와 수신자는 여러 주파수 대역 또는 채널을 활용하여 동시에 데이터를 송수신할 수 있는 멀티링크 동작을 지원한다. 송신자는 전송하려는 데이터 페이로드로부터 퍼지 해시 값을 생성하고, 해당 해시 값을 별도의 제어 프레임의 페이로드 바디 필드에 삽입한다. 제어 프레임은 암호화된 데이터 프레임과 병렬로 전송되며, 각각 독립된 링크를 통해서 동시에 RS/ISS(Relay Server/Intermediate Security System) 장비로 전송된다.

퍼지 해시는 원본 데이터의 미세한 차이를 반영하면서도 고정된 길이의 해시 값을 생성하며, 일반 해시 함수와 다르게 유사성을 기반으로 악성 여부를 판단하는 데에 활용할 수 있다[5]. 그러나 본 논문에서는 퍼지 해시 값을 직접 비교하지 않고, 이를 머신러닝 기반 탐지 모델의 입력으로 활용하여 악성 여부를 판단하도록 하였다. 퍼지 해시는 데이터 페이로드의 복잡한 특징을 고정된 길이의 축약 표현으로 변환하므로 별도의 특징 추출 과정 없이 경량 탐지 모델을 구성할 수 있다.

RS/ISS 장비에서는 암호화된 데이터 프레임을 복호화하지 않고, 제어 프레임에 포함된 퍼지 해시 값을 추출하여 머신러닝 모델에 입력한다. 이를 통해 트래픽의 악성 여부를 판별하고, 탐지 결과가 악성일 경우에 해당 트래픽은 폐기되고, 정상적으로 분류된 트래픽은 수신자에게 전송된다. FH는 종래 DPI와 달리 복호화 과정을 거치지 않기 때문에 탐지 지연 및 전체 패킷 전송 시간을 줄일 수 있다.

3. 실험 및 결과

본 논문에서는 DPI와 FH 간의 링크 평균 전송 지연, 스루풋, 탐지 정확도, 학습 시간, 메모리 사용량을 비교하였다. 링크 평균 전송 지연 및 스루풋을 평가할 때 충돌 및 노이즈가 없는 이상적인 네트워크 환경을 가정하였다. 이와 함께 퍼지 해시 값을 데이터 프레임의 헤더에 삽입하는 방식(Fuzzy Hash-based Header Insertion, FH-HI)을 추가로 고려하여 전송 효율성도 함께 평가하였다. 본 논문에서는 전체 m개의 링크에서 발생하는 전송 지연 시간의 평균값을 기반으로 링크 평균 전송 지연을 수식 (1)과 같이 모델링 하였다.

$$\overline{T}_{link}(m) = (1/m)\cdot(\Sigma_{i=2}^{n} T_{data,i} + T_{FH-control}),\ m \geq 2 \quad (1)$$

각 파라미터의 정의는 표 1에 정리하였으며, 기법별 헤더 구성 및 페이로드 크기의 차이는 표 2에 정리하였다. 그리고 데이터 프레임 전송 지연 시간은 수식 (2)와 같이 계산하였다.

$$T_{data,i} = ((H+P_i)/R_{PHY}) + T_{SIFS} + (L_{ACK}/R_B) + T_{DIFS} \quad (2)$$

<표 1> 전송 지연 시간 파라미터 정의

Parameter	Meaning	Value
$\overline{T}_{link}(m)$	링크 평균 전송 지연 시간	-
m	전체 링크의 수	[2:16]
n	데이터 프레임을 전송하는 전체 링크의 수	-
$T_{data,i}$	i번째 링크에서의 데이터 프레임 전송 지연 시간	-
$T_{FH-control}$	퍼지 해시 제어 프레임 전송 지연 시간	-
H	헤더 크기	-
P_i	i번째 링크의 데이터 페이로드 길이	-
L_{ACK}	ACK 프레임 크기	112 bit
L_{MH}	MAC 헤더 크기	320 bit
L_{FHCH}	퍼지 해시 제어 프레임 헤더 크기	256 bit
L_d	전체 데이터 페이로드 크기	200B, 400B
R_{PHY}	PHY 계층 전송 속도	54 Mbps
R_B	제어 프레임 전송 속도	24 Mbps
T_{SIFS}	SIFS 간격 시간	16 μs
T_{DIFS}	DIFS 간격 시간	34 μs

<표 2> 전송 기법별 변수 정의 비교

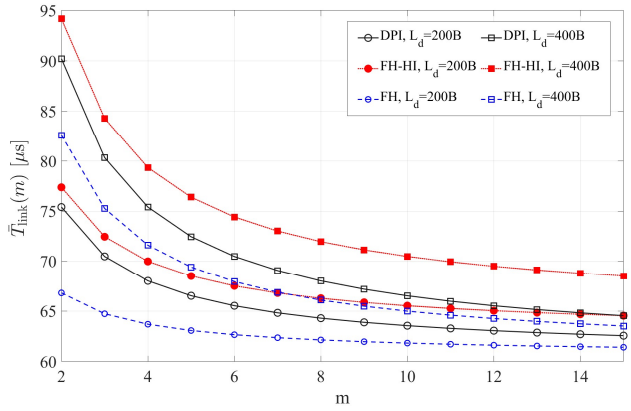
Method	n	H	P_i	$T_{FH-control}$
DPI	m	L_{MH}	L_d/m	0
FH-HI	m	$L_{MH}+(L_d/15)$	L_d/m	0
FH	$m-1$	L_{MH}	$L_d/(m-1)$	수식 (3)

제안하는 FH에서 사용되는 퍼지 해시 제어 프레임의 전송 지연 시간은 수식 (3)과 같이 계산한다. 이때, 퍼지 해시 제어 프레임에 포함되는 퍼지 해시 값의 길이는 원본 데이터 페이로드의 약 1/15 수준으로 설정하였다.

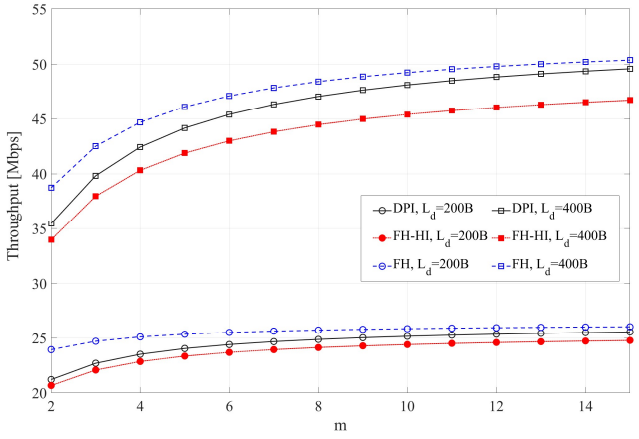
$$T_{FH-control} = ((L_{FHCH} + L_d/15)/R_{PHY}) + T_{SIFS} + (L_{ACK}/R_B) + T_{SIFS} \quad (3)$$

스루풋은 링크 평균 전송 지연 시간 대비 전송된 전체 페이로드 크기로 정의하였으며, 수식 (4)와 같이 계산하였다.

$$Throughput(m) = L_d / \overline{T}_{link}(m) \quad (4)$$

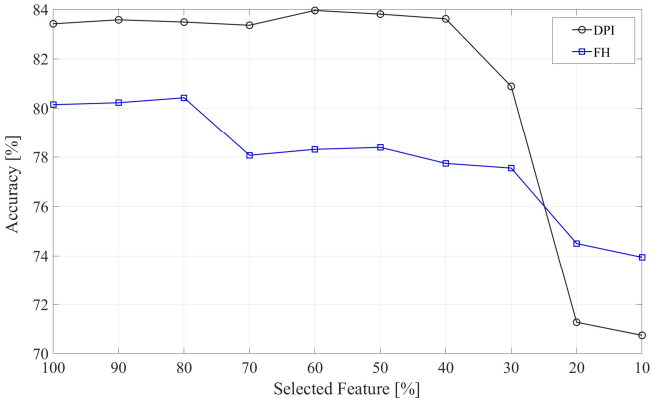


(그림 2) 링크의 개수(m)에 따른 링크 평균 전송 지연

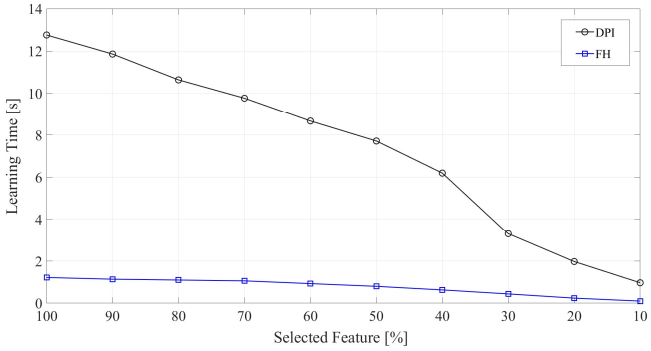


(그림 3) 링크의 개수(m)에 따른 스루풋

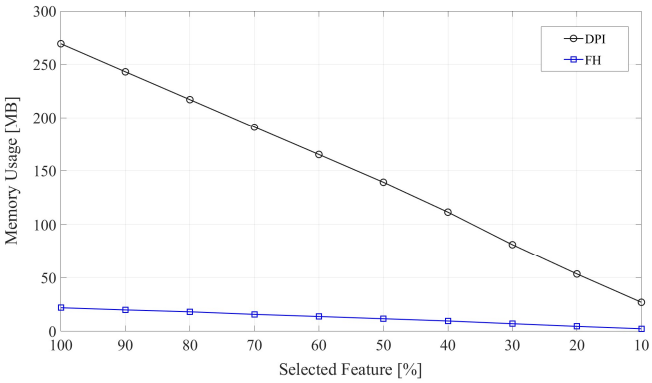
그림 2와 3은 링크의 개수에 따른 링크 평균 전송 지연 시간 및 스루풋 측정 결과를 나타낸다. 전반적으로 링크의 개수가 증가할수록 전송 지연 시간은 감소하고, 스루풋은 향상되는 경향을 보였다. 제안하는 FH 기법은 원본 페이로드의 대비 약 1/15 크기로 축소된 퍼지 해시 값을 별도의 링크를 통해 병렬 전송하므로 전체 링크에서의 평균 전송 지연이 감소하였다. 이로 인해, 종래 방식 대비 가장 낮은 전송 지연과 가장 높은 스루풋을 달성하였다. 반면, FH-HI는 퍼지 해시 값을 페이로드 헤더에 삽입하는 방식이므로 전송 오버헤드가 증가하여 지연 시간이 가장 높고, 스루풋은 가장 낮았다. DPI는 전체 페이로드를 복호화하여 처리하는 구조로 페이로드 크기가 가장 크지만, 퍼지 해시 생성에 따른 오버헤드가 없으므로 FH-HI보다는 낮은 지연과 높은 스루풋 성능을 기록했다. 결론적으로 FH 기법은 전송 지연 시간 측면에서 DPI 대비 최대 11.41%, FH-HI 대비 최대 13.67% 개선하였으며, 스루풋 측면에서는 각각 12.88%, 15.84% 향상되었다.



(그림 4) 선택된 특징 비율에 따른 정확도



(그림 5) 선택된 특징 비율에 따른 학습 시간



(그림 6) 선택된 특징 비율에 따른 메모리 사용량

탐지 정확도, 학습 시간, 메모리 사용량 평가는 Payload-Byte[6] 도구를 이용하여 전처리한 UNSW-NB15 데이터셋을 기반으로 수행되었으며, 분류 모델로는 의사결정트리를 사용하였다. 전처리된

UNSW-NB15 데이터셋은 각 패킷의 헤더 정보 4개와 전체 페이로드(1500바이트)를 1바이트 단위로 분할하여, 총 1504개의 특징(feature)로 구성된다. DPI 기법은 복호화된 페이로드까지 포함하여 전체 데이터를 학습에 활용하므로 전체 1504개의 특징을 모두 사용한다. 반면, 제안하는 FH 기법은 ssdeep 도구를 통해서 퍼지 해시 값을 생성하고, 이를 특징 벡터로 변환하여 학습에 사용하였으며, 평균적으로 100개의 특징으로 구성된다.

그림 4-6은 선택된 특징의 비율에 따른 탐지 정확도, 학습 시간, 메모리 사용량의 결과를 나타낸다. 전반적으로 선택된 특징의 수가 줄어들수록 탐지 정확도는 감소하지만, 학습 시간 및 메모리 사용량은 크게 개선되는 경향을 보였다. DPI는 전체 특징을 활용하기 때문에 가장 높은 정확도를 보였으나, 선택된 특징 수가 줄어들수록 정확도 감소 폭이 크다. 반면, 제안한 FH 기법은 DPI 기법 보다 최대 5.88%의 정확도 차이를 보였지만, 전반적으로 유사한 수준의 탐지 성능을 유지하였다. 그리고 FH 기법은 DPI 기법 대비 학습 시간은 최대 90.44%, 메모리 사용량은 최대 91.86% 개선하여, 제한된 자원 환경에서도 효율적으로 동작할 수 있는 경량 탐지 기법임을 입증하였다.

4. 결론

본 논문에서는 암호화된 트래픽 환경에서 복호화 없이 악성 트래픽을 효율적으로 탐지할 수 있는 퍼지 해시 기반 침입 탐지 시스템을 제안하였다. 제안한 FH는 페이로드로부터 퍼지 해시 값을 생성하여 별도의 제어 프레임으로 병렬 전송하고, 이를 머신러닝 모델을 통해 분석함으로써 고속·경량의 실시간 탐지 시스템을 구현하였다. 실험 결과에 따르면, FH는 종래 DPI 대비 전송 지연을 최대 11.41% 감소시키고, 스루풋을 12.88% 향상시켰으며, 유사한 수준의 탐지 정확도를 유지하면서도 학습 시간과 메모리 사용량을 90% 이상 절감하였다. 향후 연구에서는 충돌 모델링 및 노이즈 환경을 고려한 리얼 테스트베드를 구축하여 제안 시스템의 성능을 검증할 예정이다.

ACKNOWLEDGMENT

본 논문은 2025년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(No. RS-2025-00518150)과 과학기술정보통신부 및 정보통신기획평가원의 ICT혁신인재4.0 사업의 연구결과로 수행되었음 (No. IITP-2022-RS-2022-00156310)

참고문헌

[1] S.-Y. Kim, S.-W. Yun, E.-Y. Lee, S.-H. Bae, and I.-G. Lee, “Fast Packet Inspection for End-to-End Encryption,” Electronics, vol. 9, no. 11, pp. 1 - 10, 2020.

[2] Zscaler ThreatLabz, “Threats delivered over encrypted channels,” Zscaler Blog, [Online]. Available: https://www.zscaler.com/blogs/security-research/threatlabz-report-threats-delivered-over-encrypted-channels

[3] H. Doroud, M. A. A. Faruque, M. Sheikholeslami, and N. Ghani, “Speeding-Up DPI Traffic Classification with Chaining,” in Proc. IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, UAE, 2018, pp. 1 - 6.

[4] H.-Y. Shim, T.-R. Park, and I.-G. Lee, “Performance Evaluation of Fully Homomorphic Encryption for End-to-End Cryptographic Communication in Multihop Networks,” in Proc. 2022 24th Int. Conf. on Advanced Communication Technology (ICACT), PyeongChang, Korea, 2022, pp. 431 - 434.

[5] C. Jakobs, M. Lambertz, and J.-N. Hilgert, “ssdeeper: Evaluating and improving ssdeep,” Forensic Science International: Digital Investigation, vol. 42, Suppl., 2022, Art. no. 301402.

[6] Y. A. Farrukh, I. Khan, S. Wali, D. Bierbrauer, J. A. Pavlik, and N. D. Bastian, “Payload-Byte: A Tool for Extracting and Labeling Packet Capture Files of Modern Network Intrusion Detection Datasets,” in Proc. IEEE/ACM Int. Conf. on Big Data Computing, Applications and Technologies (BDCAT), Vancouver, WA, USA, 2022, pp. 58 - 67.