IP카메라의 DoS 공격 탐지 머신러닝 모델에 대한 연구

정웅교[1], 김동영[1], 곽병일[2]
[1]한림대학교 빅데이터전공 (학부생)
[2]한림대학교 정보과학대학 소프트웨어학부 (조교수)
20175161@hallym.ac.kr[1], klgh1256@s.hallym.ac.kr[1], kwacka12@hallym.ac.kr[2]

A Study on Machine Learning model for detection of DoS Attack

Woong-Kyo Jung[1], Dong-Young Kim[1], Byung Il Kwak[2]
[1]Major of Big Dataept, Hallym University (Undergraduate Student)
[2]Division of Software, Hallym University (Assistant Professor)

요 약

ICT 기술의 빠른 발전과 함께 Internet of Things (IoT) 환경에서의 Internet Protocol (IP) 카메라의 사용률이 증가하면서, IP 카메라에 대한 개인정보 이슈와 제품의 보안성 검토 관련 소비자의 개인정보 유출 우려가 증가하고 있다. 본 논문에서는, IP 카메라에 대한 4개 종류의 Denial of Service (DoS) 공격을 통해 IP 카메라 이상 반응을 확인했다. 또한, 이 과정에서 수집한 공격 패킷 데이터를 기반으로, DoS 공격을 탐지하는 간단한 피쳐 구성과 머신러닝 모델을 제안하였다. 최종적으로, DoS 공격을 통해 실제 IP 카메라에 대한 가용성 테스트를 수행하였으며 머신러닝 알고리즘 4개 Decision Tree, Random Forest, Multilayer Perceptron, SVM에서의 DoS 공격 탐지 성능을 비교하였다.

1. 서론

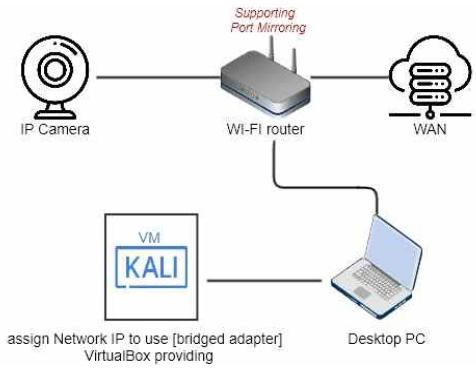
최근 IoT 기술 발전과 함께 관련 장비의 수가 증가하면서 CCTV를 대체할 수 있는 IP 카메라의 사용 숫자 역시 증가하고 있다. 국내 인터넷 사용자의 약 12.4% 가 IP 카메라를 이용하고 있으며, 전년 대비 약 6.9% 증가하였다. 이러한, IP 카메라의 사용량 증가와 함께 적절한 보안성 테스트를 수행하지 않아 IP 카메라 이용자 약 17.4%가 제품의 오작동 또는 개인정보 이슈를 우려하고 있다 [1].

한국인터넷진흥원(KISA)에서 배포한 “홈/가전 IoT 보안 가이드”에서 보안성 확보를 위한 다양한 대처방안을 권고하고 있음에도 불구하고, 여전히 IP 카메라는 보안 위협에 노출되어 있다. 또한, IP 카메라는 제품의 성능 상 다양한 네트워크 위협을 받을 수 있으며, 특히 서비스 거부 공격(DoS)에 의해 기기가 정지하는 등의 이상 반응을 보일 수 있다[2].

본 논문에서는 IP 카메라의 DoS 공격에 대한 취약점 확인과 DoS 공격을 탐지하기 위한 머신러닝 기반의 침입탐지 방법을 연구하였다. 또한, 이와 함께 4종의 DoS 공격을 실시하여 IP 카메라에 미치는 영향을 확인하였다. 추가로, 공격 패킷의 전송 간격을 설정하여 IP 카메라의 DoS 공격에 대한 수용 임곗값을 분석하였다.

2. 실험 환경

본 연구는 IP 카메라를 유선 환경에서 연결하여 3종의 DoS 공격 실험을 진행하였다. 해당 실험에서는 IP 카메라(EasyN사의 ES100A2), 라우터, Desktop PC, Kali Linux가 설치된 가상머신으로 구성했으며, 그림 1은 본 실험 환경의 구성도를 나타낸다. Kali Linux에서 공격자가 DoS 공격을 수행했을 때 네트워크 트래픽을 분석할 수 있도록 포트 미러링이 지원되는 공유기를 적용했으며, IP 카메라의 트래픽은 동일 내부 네트워크로 연결된 Desktop PC에서 수집하였다. 또한, Desktop PC에서 구동하는 가상머신에는 Kali Linux를 설치하여 DoS 공격 실험에 필요한 Nmap과 Hping3 도구를 사용하였다.



<그림 1> 실험 환경 구성도

공격자의 입장에서 IP 카메라가 존재하는 네트워크 구성도 확인, IP 카메라의 IP Address 및 포트 번호를 조사하기 위해 네트워크 스캐닝 도구인 Nmap을 사용하였으며, IP 카메라의 IP Address를 확인한 후 TCP (-sT), UDP (-sU) 포트 스캔으로 IP 카메라에 열린 포트를 확인하였다. Nmap을 통해 확인한 TCP 관련 포트는 21 (FTP), 23 (Telnet), 6789 (ibm-db2-admin)이며, UDP 관련 포트는 사용하지 않은 것으로 확인되었다.

3. 실험 방법 및 결과

본 공격 실험에서는 DoS 공격에 대한 IP 카메라의 가용성을 확인하기 위해 4가지 종류의 DoS 공격, 2가지 공격 옵션, 공격 대상 포트, 공격 패킷 전송 간격을 다르게 설정하여 실험을 진행하였다.

DoS 공격 수행을 위해 Hping3 도구를 활용하였으며, 실험에서는 Ping of Death, SYN Flooding, Teardrop, Local Area Network Denial (LAND) Attack을 적용하였다. 공격 대상이 되는 IP 카메라의 포트는 관리용 포트 번호로 사용되는 포트 21번과 IP 카메라의 영상을 전송하는 포트로 설정하였다. DoS 공격 시, 패킷 전송 간격은 Hping3의 faster (10,000 Packet Per Second (PPS)), flood (최대한 모든 패킷 전송) 옵션으로 적용하여 IP 카메라의 이상 여부를 확인하였다 [3].

<표 1> DoS 공격 결과 정리

공격 종류	공격 옵션			
	faster		flood	
	21번 포트	열린 포트	21번 포트	열린 포트
Ping of death	7.3초 (O)	7.4초 (O)	6.7초 (O)	6.9초 (O)
Syn Flooding	7.8초 (O)	7.1초 (O)	6.2초 (O)	6.7초 (O)
TearDrop	7.5초 (O)	7.2초 (O)	6.7초 (O)	7초 (O)
LAND	화면 정지 (X)	화면 정지 (X)	화면 정지 (X)	화면 정지 (X)

표 1은 DoS 공격의 유형 및 옵션에 따른 실험 결과를 나타낸 것이다. IP 카메라는 DoS 공격에서 faster 옵션(10,000 PPS)보다 flood 옵션(초당 전송 가능한 최대한의 패킷)으로 설정했을 경우, 더 짧은 시간 안에 재부팅되었으며, 포트 번호의 경우 포트 번호별 재부팅 걸리는 시간이 서로 다르게 나타났다. LAND 공격 수행 시 IP 카메라는 faster 및 flood 옵션에서 화면이 정지상태로 들어갔지만 모두 재부팅되지 않음을 확인하였다.

IP 카메라의 DoS 공격에 대한 허용 PPS 및 BPS를 확인하기 위해 Ping of Death 공격에서 PPS를 조절하여 실험을 진행하였다. 초당 패킷 생성의 정도를 조절하기 위해 Hping3의 -interval 옵션을 활용하였고, 열린 포트를 대상으로 Ping of death 공격을 수행하였다. 표 2는 해당 공격에 관한 결과를 나타낸 것이며, 공격에 따른 IP 카메라의 재부팅 여부를 괄호 안에 추가하였다.

실험 결과, IP 카메라가 영상 스트리밍을 위한 포트에 500 PPS보다 많은 패킷을 받을 경우, 동영상 스트리밍 재생에 영향을 받는 것으로 확인되었다. 공격 패킷의 수가 2,000 PPS 이상일 경우, 화면 정지 및 IP 카메라 재부팅으로 정상적인 기능이 불가능했으며, 공격 시 공격 패킷의 정도가 500 PPS 이상일 경우, IP 카메라가 재부팅은 되지 않았지만, 영

<표 2> DoS 공격 관련 IP 카메라 허용 패킷 범위

Ping of Death 공격 PPS 범위	공격 결과
2,000 ≦공격 PPS	화면 정지 (O)
1,000 ≦ 공격 PPS ≦ 2,000	화면 정지 (X)
500 ≦ 공격 PPS ≦ 900	화면 송출 지연 (X)
400 ≦ 공격 PPS ≦ 500	화면 송출 지연 (X)
공격 PPS ≦ 400	화면 정상 출력 (X)

<표 3> Decision Tree, Random Forest, Multilayer Perceptron, SVM 모델에서의 DoS 공격 탐지 성능 지표

Attack Type	Target ports	Attack option	Classification Algorithm															
			Decision Tree				Random Forest				Multilayer Perceptron				SVM			
			Accuracy	F1-score	Recall	Precision	Accuracy	F1-score	Recall	Precision	Accuracy	F1-score	Recall	Precision	Accuracy	F1-score	Recall	Precision
Ping of Death	port 21	faster	0.9864	0.987	0.986	0.987	0.9864	0.987	0.986	0.987	0.9819	0.9819	0.9819	0.9819	0.9864	0.987	0.986	0.987
		flood	0.9745	0.9745	0.9745	0.9745	0.9809	0.9809	0.9809	0.9809	0.9809	0.9809	0.9809	0.9809	0.9809	0.9809	0.9809	0.9809
	open port	faster	0.986	0.986	0.986	0.987	0.986	0.986	0.986	0.986	0.986	0.986	0.986	0.986	0.986	0.986	0.986	0.986
		flood	0.972	0.972	0.972	0.972	0.986	0.986	0.986	0.986	0.972	0.972	0.972	0.972	0.986	0.986	0.986	0.986
SYN Flooding	port 21	faster	1.0	1.0	1.0	1.0	0.9942	0.9942	0.9942	0.9942	0.9942	0.9942	0.9942	0.9942	0.9942	0.9942	0.9942	0.9942
		flood	0.9864	0.987	0.986	0.988	0.9864	0.986	0.986	0.986	0.9796	0.98	0.98	0.98	0.9864	0.9864	0.9864	0.9864
	open port	faster	0.9574	0.96	0.957	0.965	0.9716	0.972	0.972	0.974	0.9645	0.965	0.965	0.966	0.9787	0.979	0.979	0.98
		flood	0.9801	0.98	0.98	0.98	0.9868	0.987	0.987	0.987	0.9801	0.98	0.98	0.98	0.9868	0.987	0.987	0.987
Tear drop	port 21	faster	1.0	1.0	1.0	1.0	0.9945	0.9945	0.9945	0.9945	0.9836	0.9836	0.9836	0.9836	0.9945	0.9945	0.9945	0.9945
		flood	0.9866	0.9866	0.9866	0.9866	0.9866	0.9866	0.9866	0.9866	0.9866	0.9866	0.9866	0.9866	0.9866	0.9866	0.9866	0.9866
	open port	faster	1.0	1.0	1.0	1.0	0.994	0.994	0.994	0.994	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
		flood	0.972	0.972	0.972	0.972	0.986	0.986	0.986	0.986	0.993	0.993	0.993	0.993	0.986	0.986	0.986	0.986

상이 정상적으로 스트리밍되지 않았다. IP 카메라의 정상 기능에 대한 수용 가능한 PPS 및 BPS를 계산해보면, 한 개 패킷당 1042 Byte이고 500 PPS를 통해 (1042 Byte * 500) / 1024 = 약 4MB를 계산할 수 있으며, 1초당 약 4MB의 네트워크 트래픽을 생성하거나 500 PPS 이상의 패킷들을 생성한다면 IP 카메라는 정상적으로 기능하지 못함을 확인하였다.

4. DoS 공격 탐지 머신러닝 모델 학습

IP 카메라에 대한 네트워크 트래픽 기반의 이상징후 탐지 및 침입 탐지를 위해, Timewindow 1초로 정하고, 그에 따른 PPS, 초당 프로토콜별 BPS 및 PPS를 Feature로 설정하여 머신러닝 분류 알고리즘에 적용하였다. 침입 탐지에 사용한 머신러닝 알고리즘은 Decision Tree (DT), Random Forest (RF), Multilayer Perceptron (MLP), Support Vector Machine (SVM)이다. 성능 평가를 위해, 실제 공격을 공격으로 분류 시 True Positive, 실제 정상을 정상으로 분류 시 True Negative, 실제 공격을 정상으로 분류 시 False Negative, 실제 정상을 공격으로 분류 시 False Positive로 설정하였으며, 그에 따라 Accuracy, F1-score, Recall, Precision 값을 측정하였다. 표 3은 머신러닝 알고리즘별 3개 공격 및 공격 옵션에 따른 4개 평가 지표를 나타낸 것이다. 결과적으로 SYN Flooding과 faster 옵션을 적용했을 때 DT 알고리즘에서는 Accuracy 0.9574, F1-score 0.96으로 가장 낮은 성능을 나타내었다. 그 외 다른 알고리즘들에서는 높은 성능 지표를 달성하였다.

모든 공격 및 옵션에 대한 실험 결과를 비교하기 위해 표 4에 실험에서 사용한 4개의 머신러닝 알고리즘의 분류 결과를 평균값으로 나타내었다. 그 결과, SVM 알고리즘이 Accuracy 0.9877, F1-score 0.9878로 가장 높은 결과로 나타났지만, 다른 알고리즘에서도 그 차이가 크지 않음을 확인하였다. 또한, 해당 머신러닝 알고리즘에서 적용한 PPS, 프로토콜별 PPS, 프로토콜별 BPS와 같이 간단한 Feature 구성이 DoS 공격 탐지에 있어 유용한 것을 실험적으로 확인하였다.

<표 4> 머신러닝 알고리즘별 탐지 성능 평균값

공격 종류	Detection Performance			
	Accuracy	F1-score	Recall	Precision
DT	0.9835	0.9838	0.9833	0.9843
RF	0.9866	0.9867	0.9866	0.9869
MLP	0.9835	0.9836	0.9836	0.9837
SVM	**0.9877**	**0.9878**	**0.9877**	**0.9879**

5. 결론

본 연구에서는 다양한 종류의 DoS 공격을 수행하였으며, 공격 실험 수행 시 수집한 DoS 공격 트래픽을 통해 머신러닝 알고리즘 기반의 침입 탐지 모델 제안과 경량화된 Feature를 적용하였다. 본 연구에서 비교한 머신러닝 알고리즘 중 DT 알고리즘이 가장 낮을 탐지 성능을 나타내었으며, 나머지 3개 알고리즘에서는 Accuracy, F1-score, Recall, Precision 지표에서 높은 성능을 나타내었다.

또한, DoS 공격에 대한 IP 카메라 가용성 검사를 위해 공격 옵션, 공격 타겟 포트, 공격 PPS를 변경하면서 IP 카메라에서의 기능을 확인하였다. 해당 결과를 통해, IP 카메라의 정상 기능 관련 허용할 수 있는 DoS 공격의 최대 PPS를 확인하였다.

추후 연구로써, 딥러닝 기반의 경량화 알고리즘을 활용한 침입 탐지 및 이상 탐지 방법론을 연구할 예정이며, 다양한 IP 카메라를 대상으로 네트워크 공격 실험을 수행하여, IP 카메라에 대한 보안성 검토를 진행할 계획이다.

논문 사사

본 연구는 2022년 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학사업의 연구결과로 수행되었음(20180002160301001).

참고문헌

[1] 한국정보보호산업협회, “2021년 정보보호 실태조사”, 한국정보보호산업협회(서울), 2021. (최종 열람일: 2022년 9월 27일), https://www.kisia.or.kr/research/reference_board/23/

[2] 한국인터넷진흥원, “홈/가전 IoT 보안 가이드”, 한국인터넷진흥원, 2021. (최종 열람일: 2022년 9월 27일), https://www.krcert.or.kr/data/guideView.do?bulletin_writing_sequence=36355

[3] Salvatore Sanfilippo “hping3(8) - Linux man page”(최종 방문일: 2022년 9월 27일), https://linux.die.net/man/8/hping3