ADAM : An Adaptive DDoS Attack, mitigation scheme in software –defined cyber-physical system

Tianyang Cai, Tao Jia, Sridhar Adepu, Yuqi Li, and Zheng yang

Supervisor: Prof. Jong Hyuk Park

Presented by

Bhagyashree Kakde

04-24-2023

Seoul National University of Science and Technology, Seoul, South Korea

SeoulTech UCS Lab

Content

Abstract

- Modern society heavily relies Internet of things(IoT) Software define network(SDN), cloud computing, cyber-physical Systems(CPS).
- Shutdown of CPSs systems such as Smart grids and transportation systems lead to serious consequences.
- Distributed denial of service (DDoS) are major threat to internet enabled CPSs due to their ease of execution.
- Since constant updating of attack methods there is need for a method which will defend against both known and unknown DDoS attacks.
- Through this paper author presents Adaptive DDoS attack mitigation(ADAM) scheme.
- By combining information entropy and unsupervised anomaly detection method ADAM can automatically determines the current state but also adaptively identify suspicious features which are thereafter used to mitigate DDoS attacks in more precise way. Additionally pipeline filtering mechanism is proposed to accurately drop attack traffic .
- Real data-driven experimental results show that ADAM has an average mitigation accuracy of 99.13%. And false positive rate by 35% ~ 59%.

Introduction

- With the introduction of technologies such as physical sensors, IoT, Cloud computing in recent years , the physical world such as sensors and actuators in factories and transportation system has gradually become more closely linked to cyber systems .
- Convergence of SDN at the communication layer transforms the CPS into Software-defined cyber-physical system(SD-CPS) leading efficiency and functionality of CPS.
- Ever increasingly deployed IoT device introduce several vulnerabilities at the same time such as insecure ecosystem interfaces and insecure or outdated components. attacker can compromise IoT devices by installing malware and turning them into botnet such as Mirai and gafgyt botnet to launch distributed denial-of-service(DDoS).
- Transportation CPSs have high requirement for high-speed, low-latency, reliable data transmission, DDoS not only degrade Quality of service but bring down critical device of network.
- For example there was spike in datagram transport layer security.(DTLS) amplification attacks in the third quarter of 2021 and DTLS flooding increased by 3,549% compare to previous quarter[5].

Introduction

- DDoS attack continue to evolve in frequency, volume, intensity and severity, Traditional DDoS defense methods that have shown limitation including large computational resource overhead and budget. They are unable to defend against sophisticated attackers. Cost is too high to apply victim-centric solution for each IoT devices.

- Hence SDN-based DDoS defense method have become a significant research direction due to its features such as programmability, centralization, global view of network and dynamic network policy updating.

- SDN-based DDoS defense methods have become a significant research direction. SDN have some features such as programmability, centralization, global view of network and dynamic network policy updating.

- Author discussed previously proposed solutions. Which have limitations: firstly, detection method based on supervised machine learning could only detect known attacks that were presented in training set. Attack pattern where Attack has already taken troll on victim ”strawman solution” are not sufficient.

- Secondly, previous statics-based solution uses predefined threshold to detect DDoS attacks. when statics are above the threshold DDoS attack is considered to be detected. Here calculation of threshold is considered to be subjective factors. And the threshold may change at different moment under different circumstances.

Introduction

- Thirdly method where it focuses on Detection of DDoS Attacks using different features such as 1) SEAL JESS :which cannot filter attack traffic with multiple features. 2) FLEAM, JESS : mitigation method requires physical device deployment or requires SDN switches with additional functionality leading to bottleneck in network performance.
- Two main focus of studies are how to combine machine learning and statistical-based method. second is to how to finely filter the attack traffic based on detection results without affecting the legitimate traffic.
- ADAM can be easily deployed to the application layer of the existing SDN network which runs openflow protocol so there is no need to change network architecture and equipment.
- To detect and mitigate known and unknown attacks ADAM enables information entropy and unsupervised machine learning . This allows to counter Evolving DDoS methods.
- Author proposed novel pipeline filter mitigation which allows to precisely filter attack traffic without affecting normal traffic. ADAM scheme approach turns every switch in the SDN network into detector and dynamic filter. This allows to extinguishing the attack traffic from the source traffic along with spreading of attack in network.
- For proposed scheme Author implemented ADAM on miniset simulator . With real data-driven evaluation. And demonstrated that ADAM can mitigate various high intensity DDoS attack with average accuracy of 99.13%. False positive rate is 3.36% in single attack, 5.07% on hybrid attacks, they are reduces by 35% and 59% respectively.

Background and related work

A. DDoS attacks and Intrusion detection system

- DDoS attack is malicious behavior of an attacker using distributed bots to exhaust the victim's server resources and network bandwidth through vulnerabilities and high value traffic. Thus causing denial of service. So far there are many DDoS attacks and they are increasing. Examples: TCP SYN flood attack, ICMP flood attack, low rate DDoS attack, Link Flooding attack.
- To solve network security attacks like DDoS previously many studies proposed intrusion detection systems(IDS). To evaluate the existing machine-learning based network IDS, cross-evaluation framework named XeNIDS was proposed[23].but this study focuses on detection and narrow attention on mitigation of specially DDoS attack.
- Characteristics of DDoS attack are obvious : large traffic, high bandwidth occupation, high server load, large number of duplicate IPs. But mitigation is difficult because IDS can detect DDoS attack happening doesn't know how to mitigate of defend.

Background and related work

B. DDoS Defense in IoT Network

- In the context of IoT network and CPS, previous study proposed an SDN-enabled proactive defense framework for DDoS Defense. In these study author combines moving target defense (MTD) with cyber deception methods to actively broadcast false information and influence the perception of the attacker. This system can meet the resource and latency restrictions in IoT system. Compared to ADAM ,this approach focuses on enhancing the resistance of cloud servers. But it did not consider the defense of data plane and IoT devices[25].
- Another study proposed distributed IDS to detect DDoS attack in Blockchain-enabled IoT network by exploiting the distributed nature of fog nodes. Federated learning is used to train global detection model and deploy them to every fog node in network. This process reduces the training time. This supervised learning model is hard to defend against unknown attacks.
- Many other studies are considered but they do not take advantages of SDN even though they ae applied to SDN network.

Background and related work

C. SDN-Based DDoS Defense method

- SDN is the model shift from traditional IP network to centralized software-based network control, with the focus to decoupling the control plane from the data plane. This network shift brings many benefits : programmability, flexibility and the global view of topology.
- Previous study [27] proposed a cost effective shuffling method is based on MTD, include IP hopping, port hopping, and application migration. This makes more difficult for attacker to find attack surface. This study of shuffling achieves best trade of between cost and effectiveness.
- Liu et al.[28] proposed a volumetric DDoS attack to achieve Internet service provider-scale defenses. Which is called Jaqen. These defense have large coverage it does not consider dealing with unknown attack.
- Cui et al.[9] proposed a DDoS defense mechanism based on cognitive-inspired computing in SDN. Here author used the entropy od source and destination IP addresses with threshold to detect DDoS attack. And it mitigates by block packets sent to the victim's IP. Drawback is high FPR compared to ADAM.
- ADAM Scheme Address above mensioned drawbacks by combining entropy and unsupervised learning techniques.

Threat Model

General assumption regarding threat is attacker come from external network. While SDN controller and switches in network are honest and are not compromised by attacker. Attackers goal is to disable some important devices in the CPS(eg. PLCs, server) to paralyze several function of CPS and disable terminal devices (eg. actuators) to achieve precise strike. Fig 2. depicts concisely depicts the attack scenario. Following are some of the characteristics of the attacker.

Attack Target : For variety of reasons, all IoT devices and server in CPS can be target of attackers.

Volumetric attacks: DDoS attack is a generic term for a large class of attacks. It is most commonly known attack among them. It is a malicious act in which an attacker sends a large amount of network traffic to the victim and exhausting the victims resources.

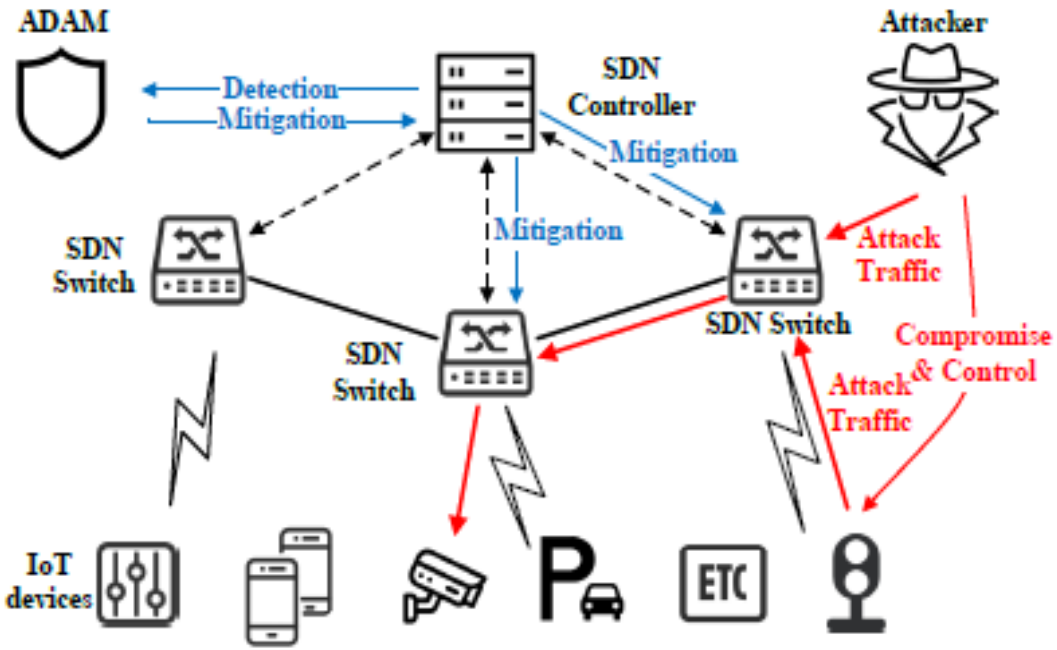


Fig. 2: Attack scenario in SD-CPS.

Threat Model

- This paper focuses on volumetric DDoS attacks.eg: TCP SYN flood attack, DNS flood Attack and ICMP Flood Attack. These attack overwhelm network infrastructure and resources of the victim through large amount of traffic.
- Proposed threat model consider amplification error. Volumetric attack have some common characteristics such as IP address may be imitated or taken from some public server and traffic has same protocol type, port number and destination IP address. Author mensioned that in some cases even the packet size, Transmition control protocol flag.
- Non volumetric DDoS attack is not considered in Proposed scheme.

Attackers' Capabilities: Since threat model is based on volumetric attacks it is assumed that there are one or more DDoS attacks simultaneously.

- It is assumed that known DDoS attack is launched in much more sophisticated way which are unknown to DDoS detectors in advance. Compromised IoT devices in the CPS can be exploited for DDoS attacks.

Design of ADAM

- This Section focuses on overall ADAM workflow and details of 2 modules of ADAM: Detection and Mitigation
- As seen from fig 3 : workflow is divided into 3 parts nominal stage, detection stage and mitigation stage.

ADAM workflow

- Nominal stage : this stage is designed to detect attack in normal operation when no attack is occurred. In this stage ADAM samples normal traffic and perform sample extraction. E.g., source IP, source port and entropy vector(EV). Which helps in training datasets for attack detection and suspicious feature extraction.
- Detection stage : ADAM periodically monitor the band width of switches. If congestion occurs on the switch, ADAM starts sampling the current traffic, calculates the EV. Anomaly detection module decides whether attack is in process. IF attack detected then mitigation stage begins.
- Mitigation stage : After DDoS attack is detected. Mitigation rules are deployed. EV is input to the suspicious feature extraction module to obtain the suspicious features set(SF)

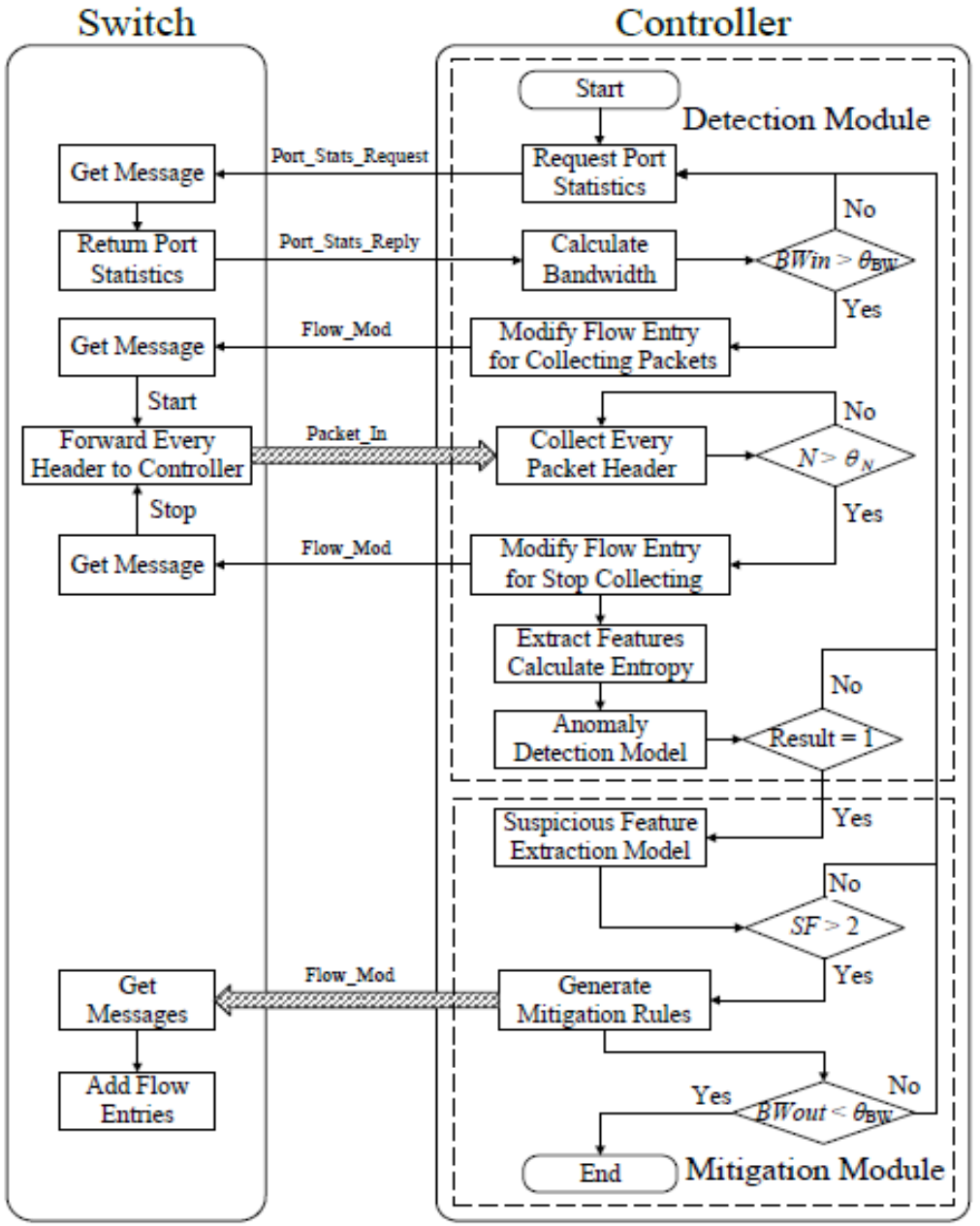


Fig. 3: Detailed design of ADAM Workflow

Design of ADAM

- Mitigation rules are based on SF and then they are deployed to switch. Later pipeline filter starts dropping packets that matches with mitigation rules.

Detection Module

Main function of this module is to periodically monitor the receiving bandwidth and transmitting bandwidth of the switch. Once the receiving bandwidth exceeds bandwidth threshold. Detection module starts traffic sampling, features extraction and attack detection.

- Bandwidth Monitoring: This mechanism acts as a trigger mechanism for ADAM . It refers to amount of data that is transmitted over network connection. If receiving bandwidth exceeds threshold value switch is said to be I congestion. ADAM starts feature extraction and attack detection at the same time.
- Traffic sampling: Once the congestion is observed, the controller sends message to modify the flow entries in switch. In order to let the switch copy and forward every pockets header of the traffic to the controller.
- Feature extraction: It refers to identifying and selecting specific character of network traffic.
- Entropy Vector: It is a measure of uncertainty. Lower the entropy, lower the uncertainty in the information. For volumetric DDoS attack traffic, contents of the packet are heavily duplicated leads to reduction in entropy of traffic. The entropy value of each feature is calculated and formed into an entropy vector, which represents the state of current network traffic.
- Attack Detection: In data analysis, anomaly detection refers to the identification of rare items. This paper aims to use light weight anomaly detection model combined with entropy. Experimental results even simple KNN algorithm have very high precision in detection DDoS attack. This is because entropy itself can significantly reflect the variation in the randomness of network traffic. Anomaly detection have better results.

Design of ADAM

Mitigation module

Author particularly design a suspicious feature-based pipeline filtering mitigation method that can be applied to every switch, so it can defend the DDoS attack at first place where it is detected.

- Suspicious Feature Extraction: These features are used to identify attack traffic.
- Algorithm for suspicious feature extraction have 3 steps:
- Step 1: Intialize a set of KNN model M for all features and the model are trained using the entropy of corresponding features in training set X.
- Step 2: for the i^{th} entropy EV_i in EV taking it as input for corresponding model M_i to obtain prediction result. If result is 1, then EV_i is detached .
- Step 3: If EV_i is an outlier and lower than the mean value of training set cumulative probability CP of F_i .
- Step 4 : Repeat step 2 and step 3, until all features have been iterated over. Finally, the suspicious feature set SF is obtained.

Algorithm 1 Suspicious Feature Extraction

Input: Training set X, Feature set F, Entropy vector EV, Profiles PF
Output: Suspicious feature set SF.

```
init model list M = []
for i = 0; i < length(EV); i++ do
    init model m = KNN(), m.fit(X_i)
    M.append(m)
init Suspicious feature set SF = []
for i = 0; i < length(EV); i++ do
    tmp = M[i].predict(EV_i)
    if tmp == 1 and EV_i < X_i.mean() then
        init Cumulative probability CP = 0
        for all p in PF_i[1] do
            if p > θ_P then
                CP = CP + p
        if CP > θ_CP then
            SF.append(F_i)
return SF
```

Design of ADAM

- Mitigation rule generation : In order to finely filter attack traffic without filtering legitimate traffic. Author proposed a pipeline mitigation method based on openflow. Here traffic is drops before it can reach the victim.
- Mitigation Deployment :The mitigation rules generated by ADAM are deployed to the target switch via SDN API and start to mitigate DDoS attack. It is explained in example for mitigation DNS amplification attack in figure.6. during deployeent each entry in flow table tries to match packets corresponding to its rule and perform appropriate action.

Profile of SF_1: IPsrc	
Value	Probability (P)
10.0.0.1	0.51
10.0.0.2	0.42
10.0.0.3	0.005
10.0.0.4	0.001
...	...

$P > \theta_P$

Mitigation Rules: IPsrc	
Match	Action
10.0.0.1	Set metadata 1/1 Goto next table
10.0.0.2	Set metadata1/1 Goto next table

Fig. 4: An Example of Mitigation Rules Generation

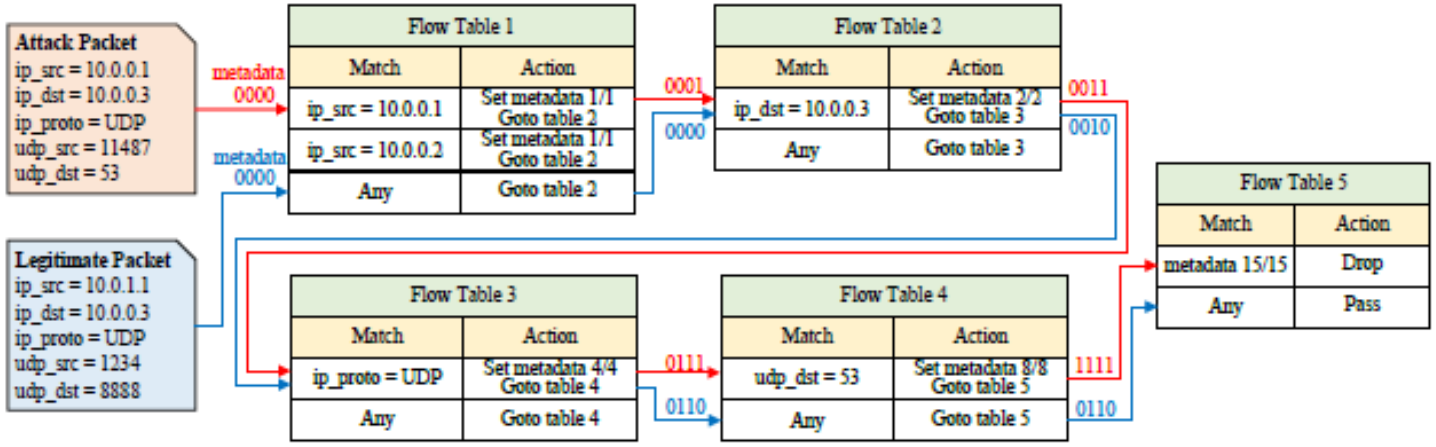


Fig. 6: An Mitigating Example of DNS amplification attack.

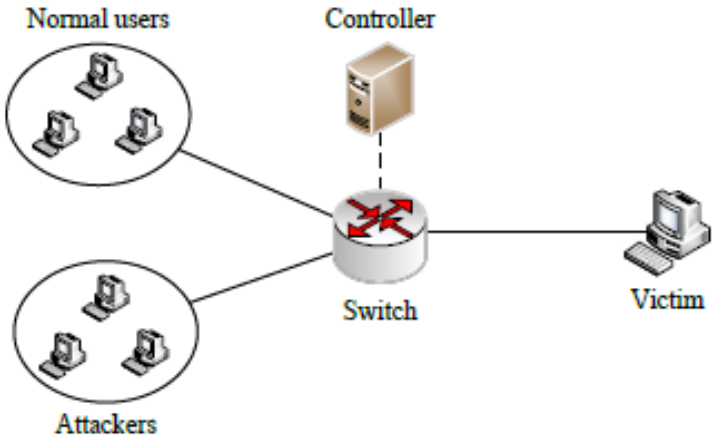


Fig. 5: Experiment network topology.

Simulation And Performance Evaluation

- Author performed experiment through simulations to verify the performance and effectiveness of ADAM.
- Dataset: The anomoly detection of ADAM is based on legitimate traffic samples.
- Author used traffic traces collected by MAWI working group traffic archive. This database consist of nearly 88 million packets of normal traffic. Author generated corresponding entropy vector for every 5000 packets and generated a total of 14600 entropy vectors as a training set.
- For attack database author generated attack traffic and the synthesis rules were decided according to section V-C.
- Experimental Setup: The experimental environment is set up on a computer with 16 GB of RAM, intel core i5-7500 CPU, and Ubuntu20.041.
- Mininet SDN simulator is used and the topology is as shown in fig.5
- Controller is Ryu based on python and it follows openflow 1.3. ADAM deployed on controller to monitor bandwidth of the switch.
- Author reply the MAWI dataset using one host as a normal host while making benign traffic appear to come from different source IPs and sent to different destination IPs.
- Attack Types: Packets were constructed to launch attack based on five DDoS attacks as follows:
- SYN flood Attack ,UDO Flood Attack, DNS amplification Attack, NTP amplification attack, Hybrid Atttack.

Simulation And Performance Evaluation

Performance Metrics: This section evaluate the effectiveness of the proposed ADAM mechanism in detecting and mitigation attacks. Here task is to identify DDoS packets from legitimate packets which is a binary classification problem.

- Author use the metrics based on true positive(TP), true-negative(TN), false-positive(FP) and False-negative(FN) to evaluate the effectiveness of the model.
- TP represents the number of attack packet dropped and TN represents the number of legitimate packets successfully transmitted. FP represents the number of legitimate packets dropped. And FN represents the number of attack packets not dropped.

Attack Detection Evaluation: To verify effect of anomaly detection and suspicious feature detection, Author define the attack strength (AS) as a ration of number of attack packet to the number of normal packets.

- Precision and FPR of Anomaly Detection Model: This is used due to imbalance between normal and abnormal samples.
- Extracted Suspicious Features: Author noticed that it is model is difficult to detect all exploited SF when attack is intensity is low. As AS increases number of detected SF also keeps increasing.

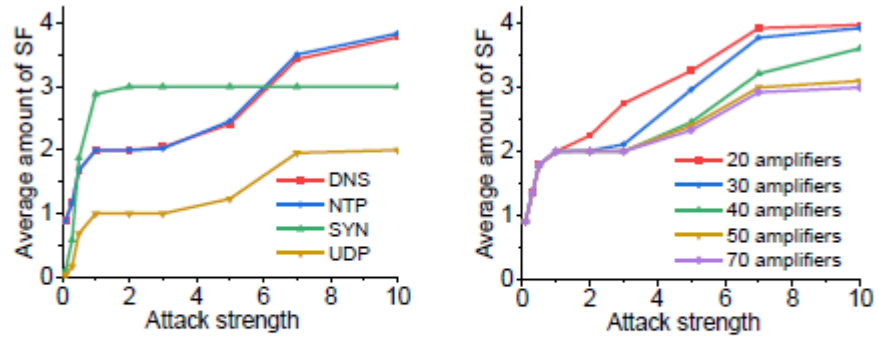
TABLE I: Precision and FPR of anomaly detection.

(a) Precision of different attacks

AS	0.1	0.3	0.5	1
DNS	0.97	1.0	1.0	1.0
NTP	0.97	1.0	1.0	1.0
SYN	0.91	1.0	1.0	1.0
UDP	0.99	1.0	1.0	1.0
Hybrid	0.95	1.0	1.0	1.0

(b) FPR of different contamination

subset	0.1	0.5	0.9	Avg
0.1	4.23%	4.39%	4.47%	4.36%
0.05	2.56%	2.30%	2.29%	2.38%
0.01	0.37%	0.39%	0.37%	0.38%
0.005	0.27%	0.20%	0.20%	0.22%
0.001	0%	0%	0%	0%



(a) Average amount of SF for different attacks

(b) Different amount of amplifiers for DNS amplification attack

Fig. 7: Average amount of detected SF.

TABLE II: Mitigation performance on different datasets.

Dataset	Synthetic Attacks					Bot-IoT		
	SYN	UDP	DNS	NTP	Hybrid	TCP	UDP	HTTP
ACC	98.8%	99.6%	99.0%	99.2%	57.80%	91.1%	99.7%	73%
FPR	7.6%	4.3%	4.1%	0.4%	5.2%	0.002%	0.001%	0.8%

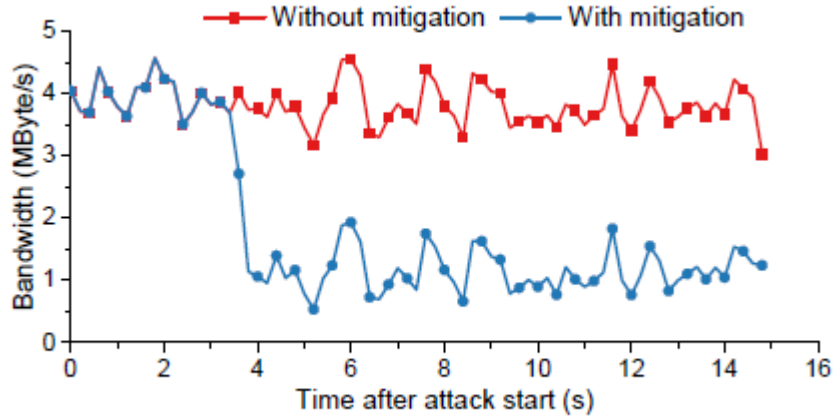
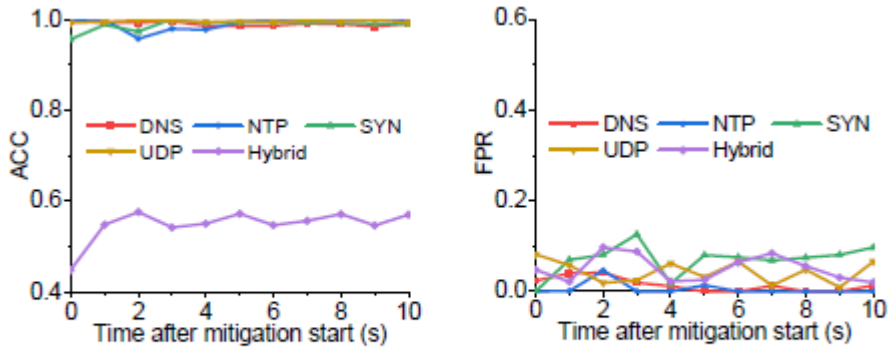


Fig. 8: The mitigation effect on DNS amplification attack.



(a) ACC for different attacks (b) FPR for different attacks

Fig. 9: Mitigation evaluation of ADAM.

Discussion

A)Limitations:

1) Feature selection and extension: Author proposed two direction of solution. One is to increase the extraction feature set F. Larger the feature set , the more features that can distinguish between attack traffic and normal traffic. This approach requires further support from openFlow. hence it is suggested to use P4 language in future to refine ADAM. Another is to define weights for suspicious features extraction this allows to detect attack at a fine-grained level but it reduces ability to detect unknown attacks in turn.
2) Non-volumetric DDoS Attack: Goal of DDoS a attacks is to cause a denial of service to the victims.this can be done in many ways which has evolved into different kind of DDoS attacks. In addition to volumetric attack there are attacks like low-rate DoS attacks, application-layer attacks, Link flooding attacks.These attacks can be archieved by exploiting a flaws or vulnerability in specific protocol.example: DoS attack exploits the congetion control mechanismof the TCP protocol by sending High-intensity, periodic pulse traffic, which significantly degrades the victims throughput and effect the network performance.

Discussion

SDN itself introduces Vulnerabilities: Although SDN offers flexibility in managing network devices with network and data security, centralized SDN controller is responsible for the determination forwarding rules in SDN Switches. Controller can become single point of failure for whole SDN network.

- This leads to perform DoS, eavesdropping and even the man-in the middle attacks.

B) Comparison:

1) Compared with JESS: Main idea of JESS is to combine all features pairs and then calculate the current joint entropy of each pair separately. If the difference in the joint entropy of the feature pair is greater than threshold value, corresponding traffic is considered to contain attack traffic. Use of unsupervised anomaly detection techniques in ADAM avoids misjudgments in setting detection thresholds.

- For attack mitigation accuracy is similar that of JESS and ADAM reduces the mitigation by 35% to 59% .

TABLE III: Comparison Between JESS and ADAM.

Metrics	Detection		Mitigation accuracy		Mitigation FPR	
	Precision	FPR	Single	Hybrid	Single	Hybrid
JESS	N/A	N/A	90%~100%	50%~90%	0%~40%	0%~70%
ADAM	90.9%~100% 99.9% avg.	4.2%~4.5% 4.36% avg.	94%~100% 99.1% avg.	45%~59% 57.8% avg.	0%~14% 3.3% avg.	0%~11% 5.1% avg.

Discussion

2) Compared with SEAL : The main limitation is that SEAL only uses traffic rates. And threshold to detect DDoS attacks. Which results in high false positive rate and high false negative rates in their experimental results.

TABLE IV: Comparison Between SEAL and ADAM.

Aspect	SEAL	ADAM
Key method	Entropy and adaptive filter	Combination of entropy and unsupervised anomaly detection with pipeline filter
Working scenario	SDN enabled smart city data center	SDN enabled CPS
Defense strategy	Victim-centric	Attacker-centric
Detection method	Threshold detection on traffic rate and entropy of destination IP	Anomaly detection based on entropy vector
Mitigation method	Drop traffic, block port, and traffic redirection	Mitigation rule-base pipeline filtering mechanism
Evaluation method	Simulation on Mininet with synthetic traffic	Real data-driven simulation on Mininet

3) Compared with FLEAM : FLEAM defends DDoS attacks by training a classification model using supervised machine learning model for detecting DDoS attack through federated learning (FL) architecture. But with this approach attacks can be only detected in the training set.it follow many drawbacks. FLEAM approach is not cost effective compared to ADAM due to its easy implementation in SDN network with no equipment required.

4) Compared with other IDS systems: This study mainly focuses on high detection performance covering wide range of attacks. Here Mitigation is not focused on DDoS attacks hence if DDoS attack is detected it can start to drop all traffic to the victims. This can overcome with expensive setup . Compairing ADAM is cost effective since it can be applied directly to existing SDN controller without additional equipments.

TABLE V: Comparison Between FLEAM and ADAM.

Aspect	FLEAM	ADAM
Key method	Federated learning architecture with RNN model	Combination of entropy and unsupervised anomaly detection with pipeline filter
Working scenario	IoT networks with distributed collaborators	SDN enabled CPS
Attack coverage	Known attacks	Known and unknown attacks
Defense strategy	Attacker-centric	Attacker-centric
Defense method	Per-packet classification by additional mitigation intelligence	Rule-based pipeline filtering by existing SDN switches
Data source	Distributed labeled attack dataset	Distributed collected normal traffic
Evaluation method	OPNET Modeler	Real data-driven simulation on Mininet

Conclusion

- Author Proposed Framework ADAM for volumetric attack detection and mitigation in Software defined-cyber physical system.
- Entropy and supervised machine learning methods are combined to detect DDoS attacks and extract suspicious features.
- Novel pipeline filter mechanism is proposes without any additional device.
- Each switch in network can turn into a detector and an adaptive filter.
- Results have show that ADAM has high accuracy.
- Feature scope for system is new detection methods can be applied by conducting in large scale network.
- Hidden security issues and problems need to be explored.

Opinion :

- Novel approach of combining entropy and unsupervised anomaly detection is proposed.
- Experiment or proposed work is efficient with 99.3% results.
- It need to have real time application since experiment was conducted in simulated environment.