Introduction

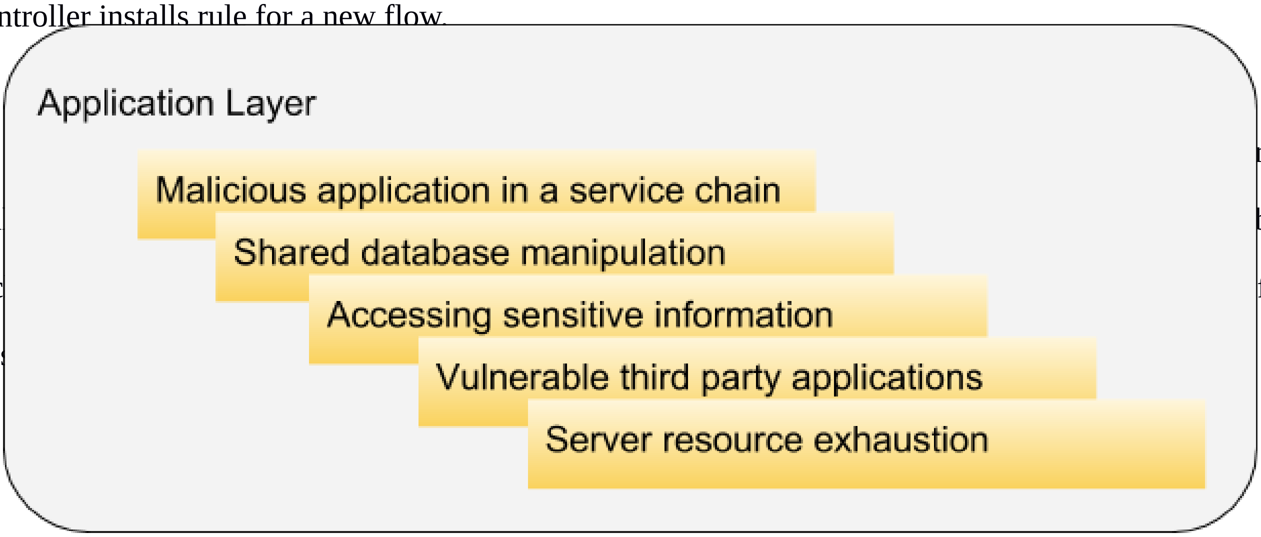
Software Defined Networking (SDN) is a thriving technology in computer networking where the control plane is decoupled from the infrastructure layer into a logically centralized entity called SDN controller. The infrastructure layer in SDN consists of switches that forward traffic according to rules installed by the SDN controller. The SDN controllers in turn run according to logic specified in the code from the application layer. Therefore, SDN architecture provides intrinsic programmability and flexibility to operate and administer a network.

Although due to the fraternity from both academia and industry, SDN has matured into a production technology, it brings new challenges in keeping the network secure. The split architecture of SDN makes it susceptible to a number of new attacks. For example, if attackers can gain privileged access to the SDN controller, they can easily control the entire network. The most prominent kind of attacks at different layers of SDN are as discussed below-

Application layer – A malicious application in a network service chain can comprise the whole service chain, a malicious application can manipulate shared database in the application server, malicious application can access sensitive information in the application server, third party applications used to ensure interoperability between devices can cause security problems due to their lack of standardization and programming model. Finally, system resources can be exhausted by malicious applications. [4]

Control layer – The SDN switches consult with the SDN controller for every new flow to install the correct flow rule. An attacker might exploit this fact to send a large number of new flows towards the SDN switch and thereby overwhelming the SDN controller with a large number of messages from the SDN switch. Stateful applications may face problem due to lack of synchronization, changing a parameter (e.g. system time) may crash the controller state. [4]

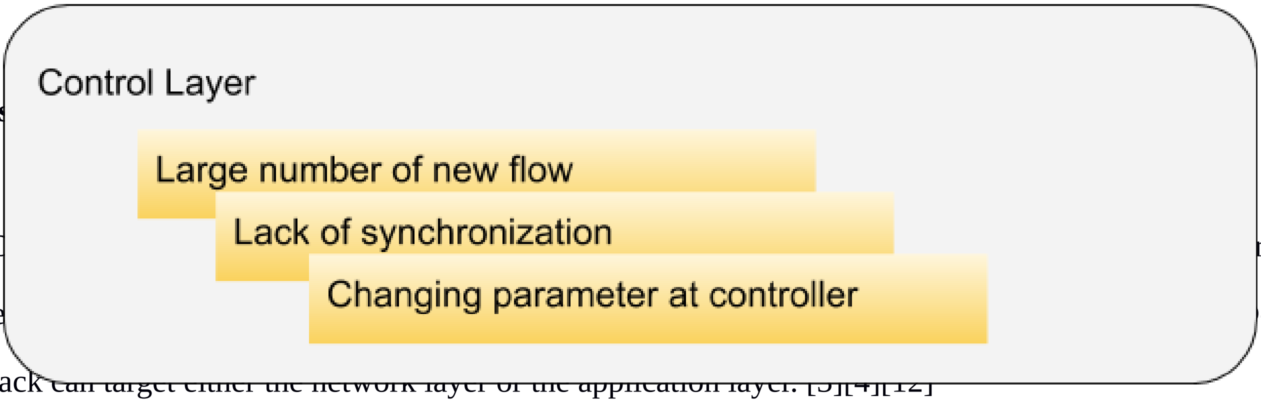
Infrastructure (forwarding) layer – A malicious SDN controller can install crafted flow rule to compromise the switch Firmware. Also fraudulent flow rule insertion and modification is possible. Data leakage can occur between logical network instance users due to improper isolation. [101] The TCAM used in by the switches to store flow rules has a slow update rate. If a large number of flow rule installation is requested, the TCAM may become irresponsive. Also a large number of packets will overflow the buffers of the switches. The buffers are used to temporarily store packets while SDN controller installs rule for a new flow.



Application Layer
Malicious application in a service chain
Shared database manipulation
Accessing sensitive information
Vulnerable third party applications
Server resource exhaustion

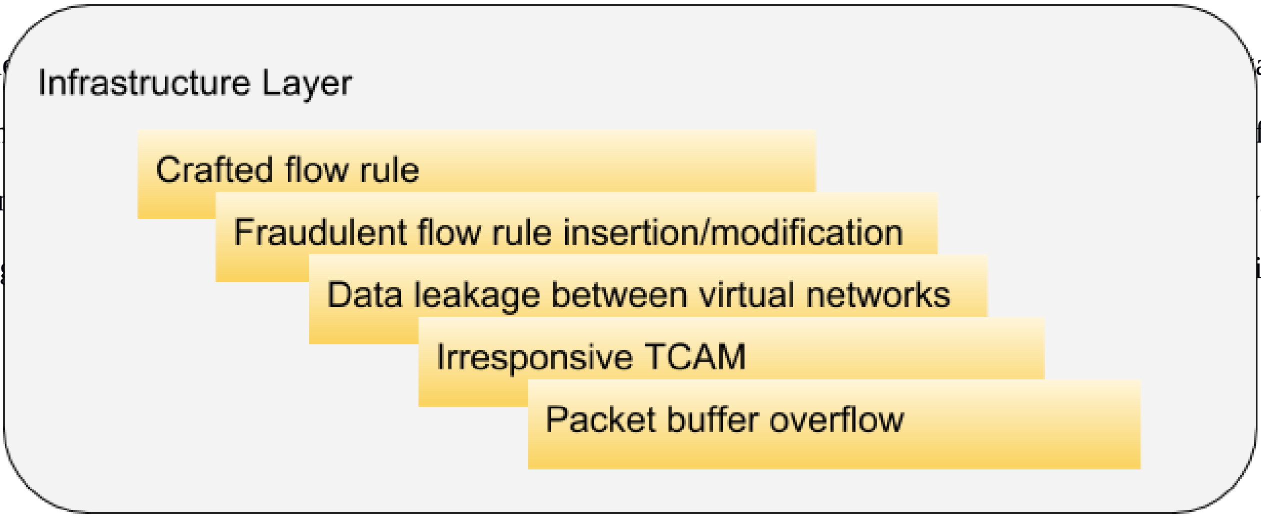
To rks
fol ble
tec fill
thi

Fig 1: Security issues in SDN



Dis

DD rds
the oS
attack can target either the network layer or the application layer. [3][4][12]



Infrastructure Layer
Crafted flow rule
Fraudulent flow rule insertion/modification
Data leakage between virtual networks
Irresponsive TCAM
Packet buffer overflow

Th ain
ser f a
co ity
(e.g ion

of the attacker, DDoS can cause great damage to internet services even in a short time period [6]. This type of attack can make the Internet ineffective by exhausting bandwidth.

DDoS attack is extremely costly for the victim. These costs come from the re-establishment cost, loss of intellectual property, loss of customer trust and even the victim can be infected by malware. Therefore, it is very important to detect and prevent it quickly.

As mentioned earlier, DDoS attack mitigation has recently received enormous research attention. We have surveyed the literature to bring the tools, techniques and datasets under one umbrella. In the following sections, we present the state of the art of DDoS detection in SDN. After that, we will briefly discuss these works.

Well known DDoS Attacks

DDoS attack can be volumetric or based on protocol exploitation. In volumetric approach, small aount of traffic can be used to generate gigabits of traffic. The attacks include UDP flood attack, NTP amplification etc. On the other hand, protocol based attacks consume server resources or other sensitive resources by exploiting the protocol mechanism. These attack include TCP SYN flood attack, Smurf attack etc.

Names of common DDoS attacks mentioned in the literature is listed in TABLE 1.

TABLE 1: Common DDoS attacks

Attack Name	**Reference**
UDP Flood	46

ICMP Flood	46
Smurf	46
Fraggle	46
SNMP amplification	46
Coremelt	46
SIP flood	46
Land	46
TCP SYN	46
CGI request	46
Authentication server	46
UDP fragmentation	49
DNS amplification flooding	49
NTP amplification flooding	49

Based on the approach of the attack the DDoS attack classification is shown below.

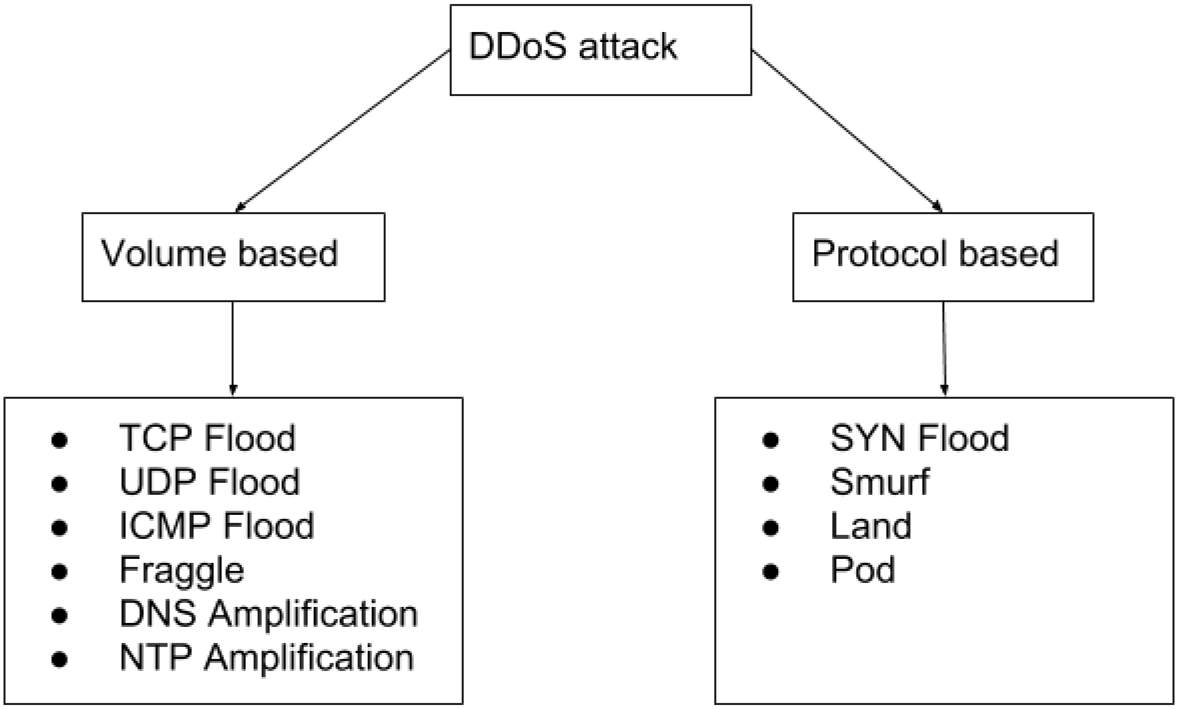


Fig 2: Types of DDoS attack

Datasets used in SDN DDoS Research

Various datasets are available to test DDoS attack detection techniques. We list these datasets in TABLE 2.

TABLE 2: Datasets used in DDoS detection mechanism testing

Name	**Details**	**Attack Traffic**	**Normal Traffic**	**Reference**
CIDDS-001	Coburg Intrusion Detection Dataset	Yes	Yes	24
NSL-KDD	KDD cup dataset and balances the proportion of normal and abnormal data	Yes	Yes	29, 30, 47
CAIDA	Collects diverse real network traffic types, including Web, FTP, Ping and etc at different locations worldwide	Yes	Yes	4, 32
DARPA 2000	DDoS attack by a novice attacker	Yes	No	
DARPA 1998	Network based attack in the midst of normal background traffic	Yes	Yes	
FIFA	Contains flash event (FE) traffic data		Yes	4
CIC-IDS-2017	Contains both simple and advanced attacks	Yes	Yes	6

Tools used in DDoS detection research

A number of tools are available and used in DDoS detection. These can be for attack generation, reading datasets or testing classifier algorithms. We list some of these tools in TABLE 3.

TABLE 3: Tools used in DDoS mitigation research

Name	Description	Reference
bonesi	DDoS botnet simulator	21
Jpcap	Java based open-source library to capture and send network packets	22
Weka	Machine learning algorithms	30

Features in Detecting DDoS using SDN

Various features have been used to detect DDoS attack in different research. We list these features in TABLE 4.

TABLE 4: Features used in DDoS detection using machine learning

Feature Name	Reference
Average Length of IP Flow	21, 43, 18
The Ratio of TCP Protocol (Rt), Ratio of UDP Protocol (Ru) and Ratio of ICMP Protocol (Ri)	21, 43, 18
Entropy of Protocols	21
Incoming and Outgoing Ratio of IP Packets	21, 43, 18
Source IP Address Number and Destination IP Address Number Ratio	21, 18
Flow Duration	32, 47
Number of packets	32, 47
Number of bytes	32, 47
Protocol	32, 47

Total source bytes	6, 47
Total destination bytes	6, 47
Flow Duration	
Source bytes per packet	
Destination bytes per packet	
Number of hosts	37
Delay	37
Protocol	6, 37
Bandwidth	37
Source IP	6, 37
Destination IP	6, 37
One way connection density	43
Number of connections to the same host as this connection	47
Number of connections to the same service as this connection	47
Change in incoming request rate	
Change in rate of new source IP addresses	
Distribution of request among source IP addresses	

Algorithms used in DDoS Detection

A number of classifier algorithms have been used in various research works. These are listed in TABLE 5.

TABLE 5: Machine learning algorithms for DDoS detection

Algorithm Name	**Reference**
Naive Bayes	21
Decision Tree	21
Logistic Regression	21
Random Forest	24
K-Nearest Neighbor (KNN)	24
Multilayer Perceptron (MLP)	24
Support Vector Machines (SVM)	27
Neural Networks	27
Self Organizing Map (SOM)	32
Linear Discriminant Analysis (LDA)	36
Quadratic Discriminant Analysis (QDA)	36
K-Means	43

Fuzzy c-means	43
C4.5	43
Bagging	46
Radial Basis Function Network	46
J48 decision tree	46
Deep learning	47
NB Tree	47
Random Tree	47

Performance Indicators for DDoS Detection

To evaluate performance of DDoS detection algorithm we can use different metrics. We list these metrics in TABLE 6.

TABLE 6: Metrics used in DDoS detection algorithm performance evaluation

Name	**How to calculate**	**Reference**
True positive Ratio (TPR)	$TPR=\frac{TP}{TP+FN}$	21, 30
False positive ratio	$FPR=\frac{FP}{FP+TN}$	21, 30
Detection Rate	DR=(TP+TN)/(TP+FP+TN+FN)	30
Detection Rate	DR=TP/(TP+FN)	36
Precision	TP/(TP+FP)	36
F-Measure (F1 Score)	2 x DR X Precision / (DR + Precision)	36, 43
Receiver operating characteristic (ROC)	Plot of two metrics	43, 47

We present review of contemporary works on detection of DDoS in SDN in the following section.

Literature Review

Detection of DDoS attack in cloud environment is studied in [3]. They work on detecting both network layer and application layer attack. They capture both network layer and application layer traffic and analyze separately. After the analysis, they correlate the outcome of both analysis for early DDoS detection. DBSCAN clustering to group the network layer and application layer traffic in their work. They mention features such as network bandwidth, source and destination port, session time for network layer attack. Features for application layer is not mentioned in this paper.

In [4] an overview of various DDoS attacks for each layer of SDN. They also discuss countermeasures and proposed solution by other researchers. They classify different attacks in traditional networks, identify research endeavors for DDoS prevention using SDN, discuss various DDoS attack at different layers of SDN itself. Finally, they propose an information distance-based flow discrimination framework to prevent DDoS attack originated from flash events at edge devices. The information distance uses the fact that attack traffic will have high similarity among them compared to legitimate flash events. They discuss causes of DDoS attack. They discuss both SDN as a DDoS detection tool and a victim of DDoS. The key feature of SDN to detect and prevent DDoS is the ability of the SDN controller to centrally allow or deny flows. To the victim end, at the infrastructure layer, slow rule update process can be exploited to overload TCAM by large number of flows. Also switch can produce a maximum number of requests per second. This can be exploited by attackers to overwhelm the switch. At the control layer, a large number of packet_in messages generated by each new flows will exhaust resources of the controller. This is known as saturation attack. If the buffer of a switch overflows, the actual packet will be also included in the message exhausting the bandwidth of control link. Manipulation of packet_in message might cause side channel attack. At application layer, a malicious application can exhaust server resources by creating large number of working threads and also can install forged traffic flows.

Their proposed IDFD systems runs inside the edge switch. It is an statistical method.

An entropy based approach is used in [5]. They implement their proposed system in a raspberry-pi based testbed. They use entropy of a feature to detect an attack.

Entropy,

$$H(X) = -\sum_{i=1}^{N} p(x_i) \log_2(p(x_i)) \qquad (1)$$

Where, $p(x_i) = \frac{x_i}{N}$ and $x_i = x_{1,} x_{2,} x_{3,} \ldots, x_n$

They calculate threshold for various windows sizes to find the optimum windows size.

In [6] authors argue that inspecting raw packet is challenging due to high volume nature of todays traffic and use statistical information available from NetFlow to detect DDoS attack. They use random forest to detect attack. They divide features into flow-based and pattern-based.

The features used are source IP, Destination IP, number of bytes and packets transferred, start and finish timestamp, protocol. They aggregate traffic within a specific interval and flows are identified by IP address and direction (up/down). They ignore port numbers to avoid overfit. They divide the features in two types: flow based and pattern based.

In flow based features they use number of packet, number of bytes and duration for both direction.

In pattern based features they use sequence of number of packets and number of bytes in each direction. Then they calculate minimum, maximum, average, 25th/50th/75th quartiles and standard deviation as the features.

They generate their dataset using DDoS tools.

Naive Bayes classification algorithm to detect DDoS attack in [7]. They have used 25 features as input but found that some of the features are redundant. After reducing the number of features to 7, the precision was greatly improved.

Authors in [9] define three metrics to evaluate DDoS attack. These are: visit volume of each target server (P1), transmission rate for flow traffic (P2) and ratio of traffic into and out of the servers (P3). Once a suspected server under attack is found by P1, they use P2 and P3 to confirm the attack.

[12] uses an intermediate layer of servers between cloud and Internet to filter out protocol based attacks such as TCP SYN Flood and UDP storm flood attack. Their approach requires handling each attack specifically by knowing exactly how these attacks work.

In [13] authors highlight that a big challenge in detecting DDoS attack is their similarity to Flash Crowd (FC) that occurs during different events or high profile news. The authors notice that most DDoS detection mechanisms rely on the fact that DDoS traffic has automated behavior and low entropy. They challenge this assumption and evaluate the possibility of DDoS attack traffic being similar to real traffic in terms of entropy and randomness. They discuss common features used by various DDoS detection algorithms that assume the difference between DDoS attack and legitimate FC traffic. They investigate the possibility to mimic legitimate traffic using a generative machine learning framework which uses Deep Generative Networks.

The work in [14] classifies DDoS solutions in SDN as extrinsic and intrinsic. They focus on intrinsic solution approach because extrinsic solution may be infeasible due to requiring change in SDN architecture itself. They further categorize intrinsic solutions into statistical and machine learning based ones. Authors argue that statistic solutions are more preferable due to their lower computational requirement. But the highlight that existing statistic based solutions lack the capability to mitigate DDoS attacks. They use an entropy based system to both detect and mitigate DDoS attack. Their proposed method operates in three phases. They gather nominal information during non-attack phase called nominal phase. Once traffic exceeds a threshold called nominal threshold, the second phase called preparatory phase is initiated. In the second phase DDoS attack is detected and some parameters are determined. In the third stage, they mitigate the attack.

[16] uses a two stage approach to detect and mitigate DDoS attack using clustering. The train a model using normal flow (when no attack is happening). Using the clustering during non-attack period, they calculate the distribution (ratio) of traffic between different clusters. Then flows are mapped to the existing clusters at a fixed time interval. Then new distribution is calculated. The difference between two consecutive distribution is used to detect DDoS. Here, the key principle is that, without DDoS attack, the difference will be small.

In [17] the concept of joint entropy is used where two random variables are used to calculate entropy instead of a single variable. Entropy is given by Equation (1).

Whereas, joint entropy is defined as,

$$H(XY) = -\sum_{i=1}^{N}\sum_{i=1}^{M} p(x_i\, y_i)\log_2(p(x_i\, y_i)) \qquad (2)$$

They use source IP as the first feature and the second feature depends on the protocol. For ICMP and TCP SYN flooding detection packet length is used as the second feature whereas destination port is used as the second feature for UDP flood detection. Here flow duration is used as a feature instead of source IP address in case of forged IP addresses.

[18] uses a correletion based feature selection. Correlation between two random variables X and Y is found from,

$$gain = H(Y) - H(Y \vee X) \tag{3}$$

or,

$$gain = H(X) + H(Y) - H(X, Y) \tag{4}$$

To eliminate bias towards features with more input values, symmetric uncertainity is used,

$$symmetric\,uncertainity = 2 * \frac{gain}{H(X) + H(Y)} \tag{5}$$

They define an evaluation metric, Ms,

$$M_S = \frac{k\,\overline{r_{cf}}}{\sqrt{k + k(k-1)\overline{r_{ff}}}} \tag{6}$$

The feature set with highest evaluation metric is selected.

Attack traffic is generated by using bonesi a simulator for DDoS botnet in this work.

Authors in [19] propose a DDoS detection framework based on Gradient Boosting algorithm and parallel computing.

As mentioned in [20], the DDoS attacks in SDN can be different from that in traditional networks. The new type of attack can have different source and IP addresses. Therefore, entropy based methods will not work well. They proposed a method based on PCA (Principal Component Analysis).

Five features are used in [21] in their machine learning algorithm. These are Average Length of IP Flow, The Ratio of TCP Protocol (Rt), Ratio of UDP Protocol (Ru) and Ratio of ICMP Protocol (Ri), Entropy of Protocols (Ep), Incoming and Outgoing Ratio of IP Packets (Rio), Source IP Address Number and Destination IP Address Number Ratio (Rsd). Correlation based feature selection is used in this work. They also use the correlation metric given in Equation (6).

This work is similar to [18]. Features are computed every time interval of 1s.

A system to detect HTTP DDoS attack is proposed in [24]. HTTP DDoS attacks are mainly of two types: high rate and low rate. In high rate attack the target is flooded with a large number of HTTP requests. Low rate attacks exploit the vulnerabilities of the target server and are hard to detect as they appear to be of normal rate.

Modeling ML algorithm customized for IoT behavior (e.g. communication with a small fixed number of end points, repetitive small packets) is proposed in [27].

A meta-heuristic algorithm to detect intrusion based on social behavior of lions is proposed in [29]. They use lion optimization algorithm (LOA) to select features. Convolutional Neural Networks (CNN) is used to classify DDoS attack.

A genetic algorithm based approach to select features to detect DDoS attack in [30].

[32] identifies several reasons that make DDoS attack challenging for SDN based cloud. These include limited number of flow entries of SDN switches. They introduce a hybrid machine learning model for DDoS classification based on SVM and SOM. They also propose a history based IP filtering. In brief, their system works as follows. In the first h hours of non-attack period the number of IP addresses x is discovered. Also a number of trusted IP addresses y are considered by the cloud provider. They assume that z number of attack IP addresses are introduced during the DDoS attack. Their objective is to keep the number of IP addresses close to x+y. When there is a DDoS attack, the number z will increase suddenly. With this approach they are able to distinguish attack source IP address from legitimate sources. They collect features frequently from the OpenFlow switch by using request messages. In this work SVM is used first to classify traffic. If the flow falls in a region close to the SVM hyperplane (called vague space) then SOM classifier is used for more accurate classification.

Results of DDoS detection using a number of machine learning classifiers is illustrated in [36]. They show the processing time, detection rate, False positive rate and accuracy of each algorithm.

Using Naive Bayes, K Nearest Neighbors (KNN) and Support Vector Machines (SVM) to detect DDoS in SDN, [37] finds that KNN classifier performs best.

In [43] 23 features were collected and then they reduced the number of features to 8 using Information Gain and Chi-Square statistic. They use a number of classification algorithms including SVM, K-NN, Naive Bayesian, Decision Tree, K-means and Fuzzy c-means. They find that fuzzy c-means is very effective in detecting DDoS attack. The top eight features found by them using the Chi-square ranking system are-

1. Ratio ICMP
2. Land (Number of packets having same source and destination IP address)
3. Ratio UDP
4. One way ratio (Ratio of flow packets that travel in only one direction)
5. Ratio TCP
6. Protocol Type
7. Average Lenght of IP Flow
8. Ratio of In/Out packets

With Information gain they find the same set of features with only difference that the last two features have different ranking. They normalize the features using the equation

$$Z = \frac{x - \overline{x}}{\sigma} \qquad (7)$$

Here, $\overline{x}$is the mean and σ is the standard deviation of the variable.

A sampling frequency of one second is used by them to collect the features.

Compares Performance of Support Vector Machine (SVM) classification with other algorithms is compared in [46]. They find that SVM performs better in terms of accuracy and false positive rate.

A deep learning approach is used to detect DDoS attack in [47]. They show the deep neural network (DNN) approach performs better than J48, Naive Bayes, NB Tree, Random Forest, Multi-layer perceptron and Support Vector Machines (SVM) classifier in terms of accuracy.

Conclusion

In order to reap the benefits of SDN, it must be secure because cost of attacks such DDoS is very high for the victim. A number of research works have been done in this area. In this work, we bring the essence of the state-of-the art research to the reader. We present the software tools, algorithms, input to these algorithms, methods to evaluate these algorithms and dataset used to test them in a comprehensive manner. We believe our effort will help the research community to build on what is already done in this area.

References

--This section is not updated. But, it contains approximately same number of placeholder entries that are used in this paper--

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.

[1] Yusof, A.R.A., Udzir, N.I. and Selamat, A., 2019. Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), pp.292-315.