A Deep Learning Based DDoS Detection System in Software-Defined Networking (SDN)

security

Niyaz Q , Sun W , Javaid A Y . A Deep Learning Based DDoS Detection System in Software-Defined Networking (SDN)[J]. Security & Safety, 2016, 4(12).

没有看的价值，跟深度学习完全扯不上关系，被标题和页码骗了。。

DDoS Detection System的实现

分为三个部分：信息收集，特征提取，流量收集，结构图如下：

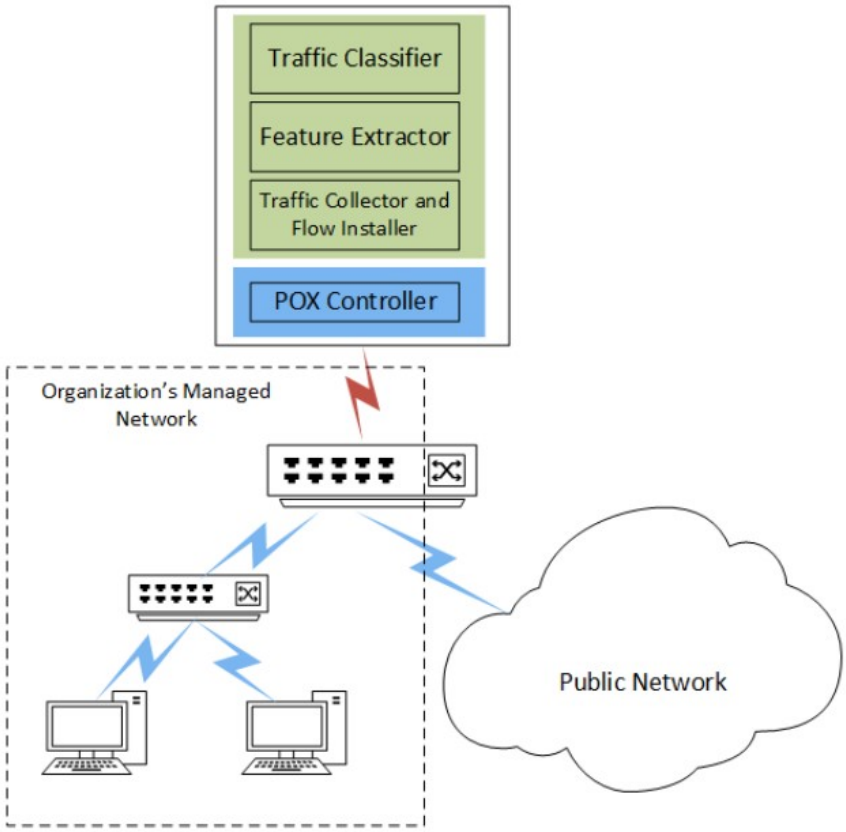

Figure 3: A DDoS detection system implemented in SDN

信息收集方法命名为TCFI，具体算法流程如Algorithm1:

Algorithm 1: TCFI Module

```
Data: Incoming network packets at the controller
Result: List of extracted packet headers for TCP, UDP, and ICMP
begin
    packets_list ⟵ ∅
    flows_list ⟵ ∅
    while Timer for the FE is not triggered do
        Receive a packet from switch
        Store headers in packets_list
        if Packet arrives due to flow table miss then
            Compute flow for the packet
            Compute symmetric flow, symflow, for flow
            if symflow ∈ flows_list then
                Remove symflow from flows_list
                Install flow rule for symflow in switch(es)
                Install flow rule for flow in switch(es)
            else if flow ∉ flows_list then
                Add flow in flows_list
                Output the packet to desired port
            else
                Output the packet to desired port
```

意思是：抽取所有的包头放到packets_list里，将新产生的流存入flow_list里。
被抽取的特征有如表1

TCP		UDP	ICMP
Src IP	Window	Src IP	Src IP
Dst IP	SYN	Dst IP	Dst IP
Src Port	ACK	Src Port	ICMP Type
Dst Port	URG	Dst Port	ICMP Code
Protocol	FIN	Protocol	Protocol
Data Size	RST	Data Size	Data Size
TTL	PUSH	TTL	TTL

Table 1: Different headers extracted from TCP, UDP, and ICMP packets

特征提取和流量分类

特征提取设置时间间隔进行，特征提取模块从TCFI中获得统计信息，并计算特征，按流分类，TCFI的特征被提取后重设特征集。
可抽取的特征总结如下：
TCP：

#	Feature Description
1	# of incoming TCP flows
2	Fraction of TCP flows over total incoming flows
3	# of outgoing TCP flows
4	Fraction of TCP flows over total outgoing flows
5	Fraction of symmetric incoming TCP flows
6	Fraction of asymmetric incoming TCP flows
7	# of distinct src IP for incoming TCP flows
8	Entropy of src IP for incoming TCP flows
9	Bytes per incoming TCP flow
10	Bytes per outgoing TCP flow
11	# of packets per incoming TCP flow
12	# of packets per outgoing TCP flow
13	# of distinct window size for incoming TCP flows
14	Entropy of window size for incoming TCP flows
15	# of distinct TTL values for incoming TCP flows
16	Entropy of TTL values for incoming TCP flows
17	# of distinct src ports for incoming TCP flows
18	Entropy of src port for incoming TCP flows
19	# of distinct dst ports for incoming TCP flows
20	Entropy of dst ports for incoming TCP flows
21	Fraction of dst ports $\leq$ 1024 for incoming TCP flows
22	Fraction of dst port $>$ 1024 for incoming TCP flows
23	Fraction of TCP incoming flows with SYN flag set
24	Fraction of TCP outgoing flows with SYN flag set
25	Fraction of TCP incoming flows with ACK flag set
26	Fraction of TCP outgoing flows with ACK flag set
27	Fraction of TCP incoming flows with URG flag set
28	Fraction of TCP outgoing flows with URG flag set
29	Fraction of TCP incoming flows with FIN flag set
30	Fraction of TCP outgoing flows with FIN flag set
31	Fraction of TCP incoming flows with RST flag set
32	Fraction of TCP outgoing flows with RST flag set
33	Fraction of TCP incoming flows with PUSH flag set
34	Fraction of TCP outgoing flows with PUSH flag set

Table 2: Features extracted for TCP flows

UDP：

#	Feature Description
35	# of incoming UDP flows
36	Fraction of UDP flows over total incoming flows
37	# of outgoing UDP flows
38	Fraction of UDP flows over total outgoing flows
39	Fraction of symmetric incoming UDP flows
40	Fraction of asymmetric incoming UDP flows
41	# of distinct src IP for incoming UDP flows
42	Entropy of src IP for incoming UDP flows
43	Bytes per incoming UDP flow
44	Bytes per outgoing UDP flow
45	# of packets per incoming UDP flow
46	# of packets per outgoing UDP flow
47	# of distinct src ports for incoming UDP flows
48	Entropy of src ports for incoming UDP flows
49	# of distinct dst ports for incoming UDP flows
50	Entropy of dst ports for incoming UDP flows
51	Fraction of dst port $\leq$ 1024 for incoming UDP flows
52	Fraction of dst port $>$ 1024 for incoming UDP flows
53	# of distinct TTL values for incoming UDP flows
54	Entropy of TTL values for incoming UDP flows

Table 3: Features extracted for UDP flows

ICMP：

#	Feature Description
55	# of incoming ICMP flows
56	Fraction of ICMP flows over total incoming flows
57	# of outgoing ICMP flows
58	Fraction of ICMP flows over total outgoing flows
59	Fraction of symmetric incoming ICMP flows
60	# of asymmetric incoming ICMP flows
61	# of distinct src IP for incoming ICMP flows
62	Entropy of src IP for incoming ICMP flows
63	Bytes per incoming ICMP flow
64	Bytes per outgoing ICMP flow
65	# of packets per incoming ICMP flow
66	# of packets per outgoing ICMP flow
67	# of distinct TTL values for incoming ICMP flows
68	Entropy of TTL values for incoming ICMP flows

Table 4: Features extracted for ICMP flows

对9-12,43-46,63-67计算字节数和每个流包数的中位数，对8,14,16,18,20,42,48,50,54,62,68计算熵。
算法部分就没有了，也没讲怎么分类。

实验部分

从公网中抓正常流量，利用hping3构造异常流量，在构造的SDN中进行实验，计算：Accuracy,Precision,RecallF值，ROC
本文：主要了解了一些可用于特征提取的特征集，还有一个用于攻模拟攻击的工具：hping3