ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Use of SDN for Detecting and Mitigating Link Flooding Attack

Prof. Kanchan Varpe, Komal Khandale

RMD Sinhgad School of Engineering, Pune, India

Student, RMD Sinhgad School of Engineering, Pune, India

ABSTRACT: In this paper, we will work on link-flooding attackdefense system, LFADefender that leverages SDN featuresto effectively detect and mitigate LFA. In LFADefender, we studied the proposed a target link selection approach and a congestionmonitoring mechanism to effectively detect LFA, and further propose technique of multiple traffic rerouting method and a maliciousttraffic blocking approach to radically mitigate LFA.In addition, LFADefender has been implemented based onFloodlight, and evaluated on CloudLab with real-worldnetwork typologies. Our evaluation results have shown thatLFADefender could rapidly detect and eliminate LFA with very low performance overhead.

I. INTRODUCTION

1.1Distributed Denial of service attack (DDoS)

DOS is an attack used to deny legitimate users access to a resource such as accessing a website, network, emails, etc. or making it extremely slow.A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resourceDoS is the acronym for Denial of service. This type of attack is usually implemented by hitting the target resource such as a web server with too many requests at the same time. This results in the server failing to respond to all the requests. The effect of this can either be crashing the servers or slowing them down.

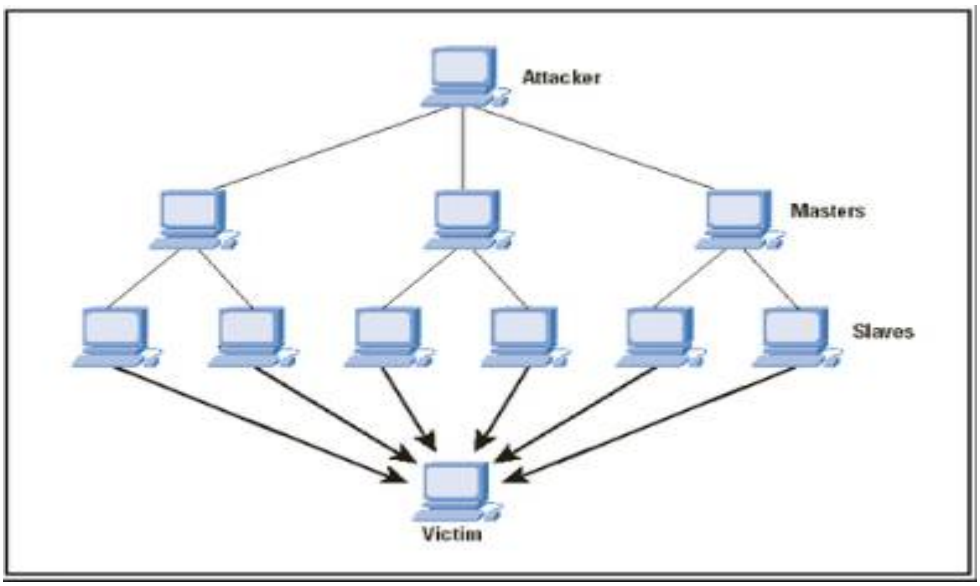

Fig 1.1 DDoS attack

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

1.2Link flooding attacks

A new kind of DDoS attack calledlink-flooding attack (LFA), has surfaced and is already being used by attackers to flood and congest network critical links. LFA is verydifficult to detect since adversaries often utilize large-scale legitimate low-speed flows and rolls target links to isolate target areas forlaunching attacks.

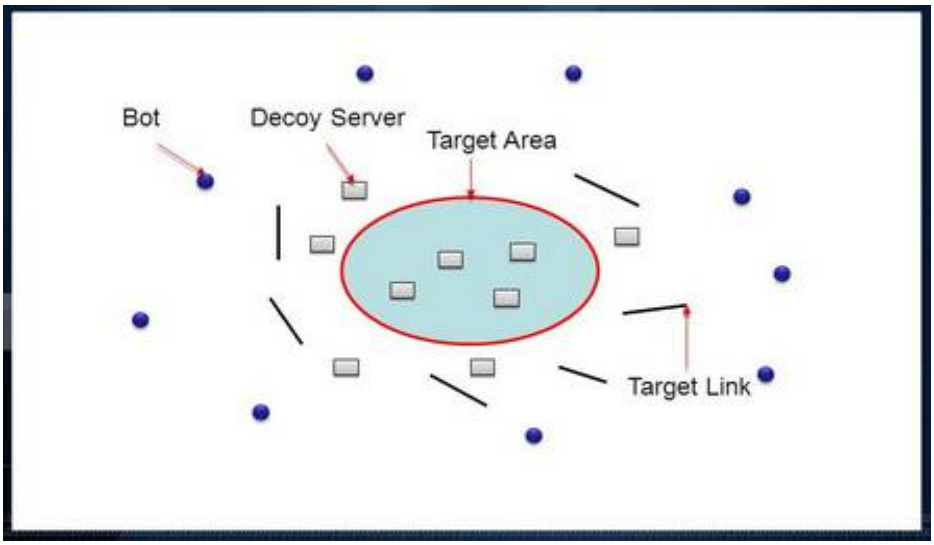

Fig 1.2 Link flooding Attack

1.3SDN

Software-defined networking (**SDN**) technology is a novel approach to cloud computing that facilitates network management and enables programmatically efficient network configuration in order to improve network performance and monitoring. Software-defined networking (SDN) is an architecture purporting to be dynamic, manageable, cost-effective, and adaptable, seeking to be suitable for the high-bandwidth, dynamic nature of today's applications. The SDN controller possesses a global view of a networkthat makes the SDN network more intelligent.

1.4NetworkAnomaly Detection

Network anomaly detection can be roughly divided into two categories: performance related anomalies and security related anomalies. The performance related anomalies include transient congestion, file sever failure, broadcast storms and so on, and security related network anomalies are often due to DDoS attacks that flood the network to prevent legitimate users from accessing the services. Anomaly detection attempts to find patterns in data,which do not conform to expected normal behavior . However, LFA can evade such detection because an attacker instructs bots to generate legitimate traffic to congest target links and the attack traffic will never reach the victim’s security detection system DOS attacks are one of the most serious threats to network security. LFA cuts off critical infrastructure through flooding and congesting critical network links of a target area. It presentstwo unique characteristics that make it very hard to detect and mitigate. First, LFA uses large-scale legitimate low-speed flows to launch attacks. Therefore, traditional anomaly-based IDSes and signature-based IDSes cannot effectively identify those attacks. Secondly, LFA is adaptiveand often changes the target links in real time, easily bypassing the traditional defence mechanisms which are often deployed in fixed locations of networks.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

SDN has several benefits, such as network-wide view, logically centralized control, software-based traffic analysis, and dynamic updating of forwarding rules, which can be leveraged for more effective attack defence.
In this paper, the author proposeLFADefender, a novel LFA defence system, that leverages key features provided by SDN to detect and mitigate LFA. A critical step for a LFA is to find target links. Using SDN technology, LFADefender can easily identify target links that are potentially used by LFA attackers, also they propose a target link selection algorithm based on SDN to find high flow density links that can be exploited as target links by LFA. Also, since LFA floods and congests the target links to cut off the communications from/to a target area, the current approachdetects link congestion through sending a lot of real-time probing packets from the probes deployed inside or outside of a target area. The link congestion monitor can be dynamically deployed at each end of any target link to efficiently capture traffic data and then send them to the SDN controller where they are analyzed to produce a rich, real-time, network-wide view of traffic flows. To demonstrate the feasibility of LFADefender, they give orim-plement four modules including a target link selection mod-ule, a link congestion monitoring module, a traffic rerouting module, and a malicious traffic blocking module.

II. LITERATURE SURVEY

2.0 Towards detecting target link flooding attacks

DDoS attacks have caused very serious damage to enterprise networks. Recently, a new kind of DDoS attack called link-flooding attack (LFA), has surfaced and is already being used by attackers to flood and congest network critical links. LFA attacks are very difficult to detect since adversaries often utilize large-scale legitimate low-speed flows and rolls target links to isolate target areas for launching attacks. To address such a critical security problem, author designs and implement a novel LFA defense system called LFADefender that leverages some key features, such as programmability, network-wide view, and flow traceability, of an emerging network technology, Software-Defined Networking (SDN), to effectively detect and migrate LFA attacks.

2.2The coremelt attack.

Current Denial-of-Service (DoS) attacks are directed towards a specific victim. The research community has devised several countermeasures that protect the victim host against undesired traffic.author presentsCoremelt, a new attack mechanism, where attackers only send traffic between each other, and not towards a victim host. As a result, none of the attack traffic is unwanted. The Coremelt attack is powerful because among N attackers, there are $O(N^2)$ connections, which cause significant damage in the core of the network. they demonstrate the attack based on simulations within a real Internet topology using realistic attacker distributions and show that attackers can induce a significant amount of congestion.

2.3 A Survey of Defense Mechanisms Against Distributed Denial of Service Flooding Attacks

Distributed Denial of Service (DDoS) flooding attacks are one of the biggest concerns for security professionals. DDoS flooding attacks are typically explicit attempts to disrupt legitimate users' access to servicesIn this paper, author explore the scope of the DDoS flooding attack problem and attempts to combat it. Also they categorize the DDoS flooding attacks and classify existing countermeasures based on where and when they prevent, detect, and respond to the DDoS flooding attacks. Moreover, they highlight the need for a comprehensive distributed and collaborative defense approach.

2.4Agile virtualized infrastructure to proactively defend against cyber attacks

DDoS attacks have been a persistent threat to network availability for many years. Most of the existing mitigation techniques attempt to protect against DDoS by filtering out attack traffic. Thisapproach has two components: (1) a correct-by-construction VN migration planning that significantly increases the uncertainty about critical links of

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

multiple VNs while preserving the VN placement properties, and (2) an efficient VN migration mechanism that identifies the appropriate configuration sequence to enable node migration while maintaining the network integrity.

2.5 Deriving traffic demands for operational ip networks: Methodology and experience

Author presents a model of traffic demands to support traffic engineering and performance debugging of large Internet service provider networks. By defining a traffic demand as a volume of load originating from an ingress link and destined to a set of egress links, author can capture and predict how routing affects the traffic traveling between domains.To infer the traffic demands, he proposes a measurement methodology that combines flow-level measurements collected at all ingress links with reachability information about all egress links. Later hediscuss how to cope with situations where practical considerations limit the amount and quality of the necessary data.

2.6An overview of routing optimization for internet traffic engineering

Traffic engineering is an important mechanism for Internet network providers seeking to optimize network performance and traffic delivery. Routing optimization plays a key role in traffic engineering, finding efficient routes so as to achieve the desired network performance. In this survey author review Internet traffic engineering from the perspective of routing optimization. A taxonomy of routing algorithms in the literature is provided, dating from the advent of the TE concept in the late 1990s. author classified the algorithms into multiple dimensions: unicast/multicast, intra-/inter- domain, IP-/MPLS-based and offline/online TE schemes.

2.7 A novel framework for modeling and mitigating distributed link flooding attacks

Distributed link-flooding attacks constitute a new class of attacks with the potential to segment large areas of the Internet. Their distributed nature makes detection and mitigation very hard. This work proposes a novel framework for the analytical modeling and optimal mitigation of such attacks. The detection is modeled as a problem of relational algebra, representing the association of potential attackers (bots) to potential targets. The analysis seeks to optimally dissolve all but the malevolent associations.The framework is implemented at the level of online Traffic Engineering (TE), which is naturally triggered on link-flooding events. The key idea is to continuously re-route traffic in a manner that makes persistent participation to link-flooding events highly improbable for any benign source.

2.8 Towards Mitigating Link Flooding Attack Via Incremental SDN Deployment

Link flooding attack (LFA), as a new type of DDoS attack, can degrade or even cut off network connectivity of atarget area. This attack employs legitimate, low-density flows to flood a group of selected links. Therefore, these malicious flows can hardly be distinguished by traditional schemes. In this paper, author proposes a scheme called Woodpecker. Woodpecker employs centralized traffic engineering based on the upgraded nodes, which can make the traffic balanced enough to eliminate the routing bottlenecks likely to be utilized by the adversaries.

2.9 Header Space Analysis: Static Checking For Networks

Today's networks typically carry or deploy dozens of protocols and mechanisms simultaneously such as MPLS, NAT, ACLs and route redistribution. Even when individual protocols function correctly, failures can arise from the complex interactions of their aggregate, requiring network administrators to be masters of detail.The goal is to automatically find an important class of failures, regardless of the protocols running, for both operational and experimental networks.

2.10CoDef: Collaborative Defense Against Large-ScaleLink-Flooding Attacks

Large-scale botnet attacks against Internet links using low-rate flows cannot be effectively countered by any of the traditional rate-limiting and flow-filtering mechanisms deployed in individual routers. In this paper, author presents a

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

collaborative defense mechanism, called *CoDef*, which enables routers to distinguish low-rate attack flows from legitimate flows, and protect legitimate traffic during botnet attacks. CoDef enables autonomous domains that are uncon- taminated by bots to collaborate during link flooding attacks and reroute their customers' legitimate traffic in response to requests from congested routers.

III. MOTIVATION

In computer networking ,DDoS attacks have caused very serious damage to enterprise networks. Recently, a new kind of DDoS attack calledlink-flooding attack (LFA), has surfaced and is already being used by attackers to flood and congest network critical links. LFA is very difficult to detect since adversaries often utilize large-scale legitimate low-speed flows and rolls target links to isolate target areas for launching attacks. To address such a critical security problem, author designs and implements a novel LFA defense system called LFADefender that leverages some key features, such as programmability, network-wide view, and flow traceability, of an emerging network technology, Software-Defined Networking (SDN), to effectively detect and migrate LFA. In LFADefender, author proposes a LFA target link selection approach and designs a LFA congestion monitoring mechanism to effectively detect LFA. In addition, author present a multiple optional paths rerouting method to temporarily mitigate links congestion caused by LFA. Author further propose a malicious traffic blockingapproach to radically mitigate LFA.

IV. PROPOSED SYSTEM

The proposed system carries Use of key features of SDN, such as network-wide view,flow traceability, and dynamic reconfiguration, we design the LFA defense system called LFADefender to detect and migrate LFA.Figure 4.1 depicts an overview of LFADefender

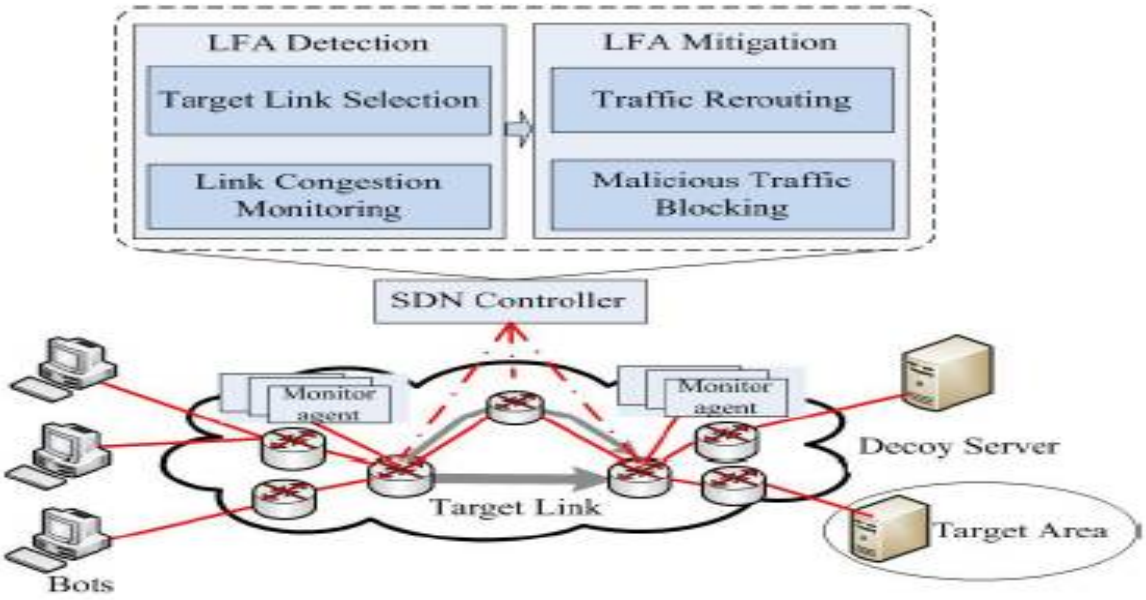

Fig 4.1LFA Defender overview

It consists of four main modules:

1) target link selection,
2) link congestion monitoring,
3) traffic rerouting and
4) malicious traffic blocking.

The target link selection module and link congestion monitoring module to detect LFA. Then, the traffic rerouting and malicious traffic blocking modules are used to mitigate LFA. The target link selection module can communicate with

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

the SDN controller, and obtain flow en-tries in OpenFlow switches from the controller. This module marks the links with high flow density as target links [3] and returns them. The link congestion monitoring module can

retrieve the target links from the target link selection module, and then deploys link congestion monitor agents on these links and reports link states to the SDN controller. The traffic rerouting module is used to mitigate link conges-tion via traffic rerouting. And the malicious traffic blocking module can identify attack traffic through traffic tracing, and tells switches to drop malicious traffic.

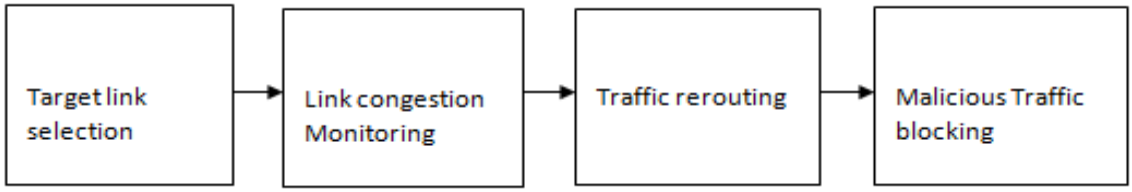

Fig4.2 Proposed System Functions

The four logical stages can be:
1)Target Link Selection: In this stage, our goal is to find target links. We present a target link selection algorithm. We get flow tables from each switch, and then analyze these tables to compute flowpaths, which are the routing paths of each flow. We count the number of flows through each link and the links with high flow density are selected as target links.
2)Link Congestion Monitoring: We design a link conges-tion monitoring module. For all possible target links, link congestion monitoring installs monitor agents at the end of the target links to capture traffic information. Then, the SDN controller gains the network traffic status analyzed and collected by the link congestion monitor agents and determines whether the links are congested.
3)Traffic Rerouting: Once the links are congested, we need to reroute the traffic from the congested target links to other links. For each flow of the traffic, we will find a different routing path to reroute this flow to the new routing path until the target link is not clogged. Since a LFA may simultaneously congest several target links so as to isolate the target area, we design a multiple paths rerouting approach to temporarily mitigate LFA.
4)Malicious Traffic Blocking: In order to radically mitigate LFA, we design a malicious traffic blocking module, which can identify LFA bots and prevent the mali-cious traffic through multiple rerouting and monitor-ingtraceroute packets. The attackers of LFA need to construct link-map and obtain stable target links, hencethey must send a large number of traceroute packets to find the stable routes.

According to the above features, the malicious traffic blocking module can identify LFA bots through malicious flow tracing based on multiple rerouting and the analysis of traceroute packets. Once LFA bots are identified, the malicious traffic blocking module will send block rules to SDN switches so as to drop the traffic from the LFA bots.

A] Detecting link flooding attacks:

- **Crossfire Attack :**

This is one of the reactive version of attack. In the classic Crossfire attack, the attacker has a swarm of bots (or botnet) at his disposal, and seeks to attack a certain area, called the *target area*. The goal is to cut off Internet connectivity to this area. To achieve this, he assigns his bots to send legitimate, low-rate traffic flows towards certainpublic servers, the *decoy servers*. These servers are reached over the same *target links* that connect the target area to the Internet. Thus the bots send traffic along paths that lead to both the decoys and the target, cumulatively flooding the sharedtarget links.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

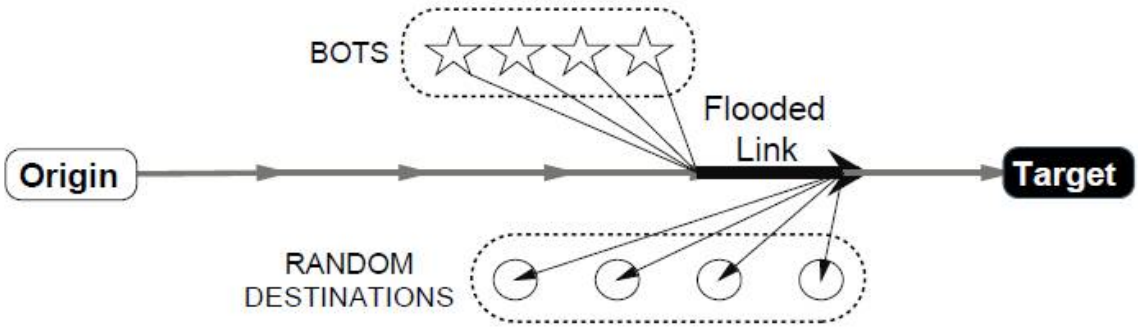

Fig. 4.3 Overview of crossfire attack concept

The most loaded links along the paths from the bots to the servers and from the bots to the targetare flooded. The concept is well illustrated in Fig. 4.3

1) Targetlink selection :

For a LFA adversary, it is essential to build an accurate link-map of network and select effective target links. As for a defender, it is hard to know which link is selected as an attack target. However, in an SDN network, the controller knows the whole network topology, and all the forwarding packets should follow the flow tables stored in OpenFlow switches. Hence, in this section, we propose a target link selection approach based on the analysis of flows in the SDN network, which finds target links by computing the flow density of a link. In Crossfire, the flow density is defined as the number of flows between bots and target-area servers that can be created through that link.
First, we introduce the concept of flowpath. Flow-path represents the forwarding path of each flow in SDN. In our approach, we use Header Space Analysis (HSA) to describe flowpath. By parsing the routing and configuration tables automatically, HSA provides a method to compute forwarding path of packets Based on the flowpaths, we need to compute the flow density of links in the later phase. Note that the link between current hop and next hop has a weight, which depends on the match field of the matched flow entry and the actual hosts in the network.
In the target link selection algorithm, the time complexity depends on the number of OpenFlow switches n, and the average number of flow entries m in the flow tables. Thus,the time complexity of this algorithm is O(nm)

2) Link Congestion Monitoring

When the target links have been found, we need to detect whether they are congested by the LFA. In LFA, adversaries often dynamically change the set of target links and extend the duration of attack almost indefinitely. Continuous link flooding of the same set of target links would lead to the changes of bot-server routes since it would inevitably activate the routers failure detection mechanism [3]. Hence, changing the set of target links can assure attack persistence and enable the attack to remain a pure data-plane attack.
Because of this, we need to dynamically and rapidly deploy monitor agents on the possible target links to detect the LFA. Therefore, we design a congestion monitoring module to detect link congestion.
This link congestion monitoring module runs in the SDN controller, which is responsible for the deployment of agents and the analysis of link congestion. When receiving the target link
information from the target link selection module, the monitoring module installs the link congestion monitor agents at the switches of target links, and when a target link is changed to a non-target link, this module removes the agents immediately. The SDN controller can read and analyze the network data of the link congestion monitor in real time.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Next, we discuss the problems of measurement deviation and deployment of link congestion monitoring :-

➢ **Measurement Deviation** : Packet pair is commonly used in the network measurement. However, cross traffic can randomly enter or leave a probing path, which is called one-hop persistent cross traffic, and results in the deviation. Therefore, in our solution, we use the link congestion monitor agent to sample and measure traffic data, and directly connect the monitor agents with the target links to eliminate the deviation.

➢ **Flexibility and Scalability** : In a LFA, there may exist many target links in a target link set, and an adver-sary periodically selects several flooding target links from the set to confine the attack. According to the features of LFA, our design should be flexible and scalable. On the one hand, we should deploy agents on both ends of a target link, and remove them when they aren't required for saving resources. On the other hand, we should have the ability to provide enough agents for monitoring links. Our link conges-tion monitor agent can meet the two requirements to monitor target link, which is flexible and scalable, and easy to be deployed in OpenFlow switches.

The link congestion monitor agent can gather network traffic information. We use the following link performance metrics to determine whether a link is clogged.

- Packet loss rate, which is increased when a link is clogged.
- RTT (Round-Trip Time), which is also increased be-cause of the queue overflow in a router under link flooding attack.

- Available bandwidth, which is clearly decreased be-cause of a lot of traffic traverses the target links

B] Mitigating link flooding attacks

Our LFA mitigation mechanism consists of traffic rerout-ing module and malicious traffic blocking module. Once link congestion is detected, the link congestion monitoring module will inform the SDN controller to start the traffic rerouting. Meanwhile, the malicious traffic blocking module will identify LFA bots through flow tracing and traceroute packets analysis. When the bots are identified, the SDN controller will send block rules to drop the malicious flows.

1) Traffic rerouting

detected to be congested, we need to find optional links to reroute the partial traffic of the congested links. To mitigate LFA, we propose a multiple optional paths rerouting method. By this method, we can obtain multiple optional links that have sufficient remaining capacity so as to temporally mitigate the target link congestion.

2)Malicious traffic blocking

Traffic rerouting can just temporarily mitigate LFA attacks because the LFA bots can still send malicious traffic and consume the bandwidth resource. Therefore, we further design a malicious traffic blocking module to identify the malicious bots so as to radically mitigate LFA attacks.

C] Link-Flooding Attack Detection and Mitigation

Linkscope [5] employs both end-to-end and hop-by-hop network measurement techniques to capture abnormal link performance degradation for detecting LFA. Compared with Linkscope, our LFADefender leverages the features of SDN to compute flow density and detect possible target links. It does not need to send probe packets from the outside of networks. Furthermore, LFADefender monitors target links dynamically, hence it also does not require complex hop-byhop network measurement to find the congested links.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

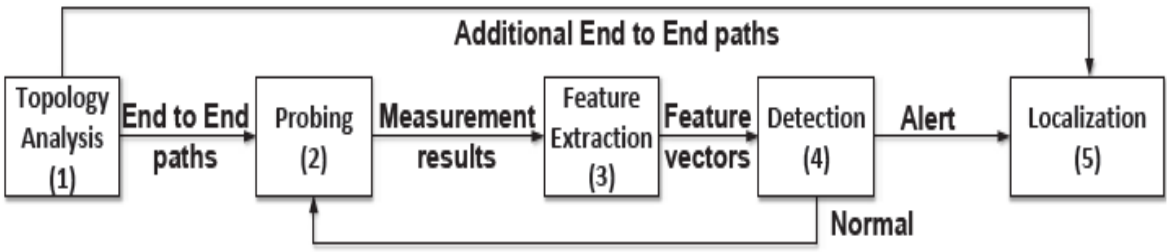

Fig 4.4Major steps for detecting LFA and locating target links/areas.

Fig. 4.3 illustrates the major steps in above methodology for detecting LFA and locating target links/areas whenever possible. The first step, involves identifying potential target linksand enumerating a set of end-to-end paths that cover potential target links. Depending on the available resource, we conduct noncooperative Internet measurement on selected paths and Next block describes the measurement method and the corresponding performance metrics. Next Section elaborates on the third and the fourth steps where the feature extraction algorithm turns raw measurement results into feature vectors that will be fed into the detection module for etermining the existence of LFA. If there is no attack, the system will continue the measurement. Otherwise,the localization mechanism, introduced will be activated for inferring the links or areas under attack.

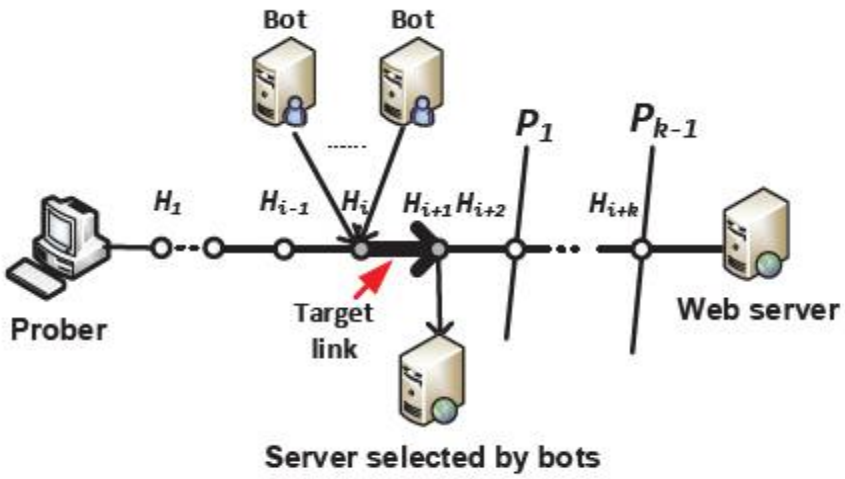

Fig. 4.5Locating the target link

When performance anomaly is detected on a forward path, *LinkScope*tries to locate the target link through two steps. First, based on the hop-by-hop measurement results from mRPT, *LinkScope*knows that the path from *H*1 to *Hi*−1 is not under attack. Second, according to the topology analysis,*LinkScope*will perform measurement on other paths that cover the hops after *Hi*, such as *P*1 going through *Hi*+1 and *Pk*−1 covering *Hi*+*k*.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

V. MATHEMATICAL MODEL

Here, we describe the detailed steps of obtaining theflowpaths in an SDN network. First, we obtain the headerof the head node as the start point of a flowpath. As weknown, SDN controller has the global network view, whichmakes it easy to gain network routing information. So, it iseasy to know the next hop (e.g. switch s1) of this head node.Second, we read the header information of flow tables in s1,convert these information into a binary vector and calculatethe intersection of head node's destination IP address ands1' source IP address. If the result is not an empty set, s1 isadded to the flowpath. Similarly, we need continue to obtainthe next hop of s1, and compare the destination IP of s1 withthe source IP of its next hop (e.g. switch s2). Next, what weneed to do is to repeat the above steps until we find thedestination node, and at the same time, we find a completeflowpath.Based on the flowpaths, we need to compute the flowdensity of links in the later phase. Note that the link betweencurrent hop and next hop has a weight, which depends onthe match field of the matched flow entry and the actualhosts in the network. Some terms are defined as follows:

***W** : the weight of a link;*
***Psrc** : the source IP space of a matched flow;*
***Pdst**: the destination IP space of a matched flow;*
***Q** : the set of all hosts' IPs in SDN;*
and $W = (Psrc \cap Q) * (Pdst \cap Q)$

There are three hosts in the source IP space and two hostsin the destination space so that we can figure out the weightcontributed by the flow 1 is 6, which means that there aresix flows that can be created through the link. Hence, theflow density of a link can be defined as follows: supposingthat there are N flowpaths throughout the link L andeachflowpath has a source IP space Pisrc and a destination IPspace Pidst on L, the flow density D of L can beexpressedas:

$$D = \sum_{i=1}^{N} W_i = \sum_{i=1}^{N} \{(P_{isrc} \cap Q) * (P_{idst} \cap Q)\}$$

In SDN, there are two kinds of flows: proactive flow andreactive flow. Proactive flows are installed on switches inadvance and can be added/deleted by the network administratoraccording to the situation of the network, whilereactive flows are inserted into switches in real time bythe SDN controller and can only exist 5s. In addition, theproactive flow has a higher priority than the reactive flow.Therefore, taking into account the priority, survival timeand removal of the two flow tables above, when selectingtarget links by computing flowpaths and the flow density,we perform the target link selection algorithm in a certaintime interval.

$$D = \sum_{i=1}^{N} W_i = \sum_{i=1}^{N} \{(P_{isrc} \cap Q) * (P_{idst} \cap Q)\}$$

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

$$D = \sum_{i=1}^{N} W_i = \sum_{i=1}^{N} \{(P_{isrc} \cap Q) * (P_{idst} \cap Q)\}$$

VI. CONCLUSION

In this paper, we have studied a link-flooding attack defense system, LFA Defender that leverages SDN featuresto effectively detect and mitigate LFA. In LFA Defender, we studied the proposed a target link selection approach and a congestionmonitoring mechanism to effectively detect LFA, and furtherpropose technique of multiple traffic rerouting method and a maliciousstraffic blocking approach to radically mitigate LFA.In addition, LFA Defender has been implemented based onFloodlight, and evaluated on CloudLab with real-world network typologies. Our evaluation results have shown thatLFADefender could rapidly detect and eliminate LFA with very low performance overhead.

REFERENCES

[1] Lei Xue, XiapuLuo, Edmond WW Chan, and Xian Zhan. Towards detecting target link flooding attack. In 28th Large Installation System Administration Conference (LISA14), pages 90–105, 2014.
[2] AhrenStuder and Adrian Perrig. The coremelt attack. In ComputerSecurity–ESORICS 2009, pages 37–52. Springer, 2009.
[3] FidaGillani, Ehab Al-Shaer, Samantha Lo, Qi Duan, MostafaAmmar, and Ellen Zegura. Agile virtualized infrastructure toproactively defend against cyber attacks. In Computer Communications(INFOCOM), 2015 IEEE Conference on, pages 729–737. IEEE,2015.
[4] AnjaFeldmann, Albert Greenberg, Carsten Lund, Nick Reingold,Jennifer Rexford, and Fred True. Deriving traffic demands foroperational ip networks: Methodology and experience. IEEE/ACMTransactions on Networking (ToN), 9(3):265–280, 2001.
[5]Ning Wang, Kin Hon Ho, George Pavlou, and Michael Howarth.An overview of routing optimization for internet traffic engineering.IEEE Communications Surveys & Tutorials, 10(1):36–56, 2008.
[6] Christos K Liaskos, VasileiosKotronis, and XenofontasDimitropoulos.A novel framework for modeling and mitigatingdistributed link flooding attacks. In IEEE INFOCOM, 2016.
[7] Lei Wang, Qing Li, Yong Jiang, and Jianping Wu. Towardsmitigating link flooding attack via incremental sdn deployment.In Computers and Communication, pages 397–402, 2016.
[8]Xin Hong Wang, Fu Qiang Liu, and Guang Xing Wang.Te routingalgorithm to minimize maximum link utilization. Mini-microSystems, 2005
[9] PeymanKazemian, George Varghese, and Nick Mckeown. Headerspace analysis: static checking for networks. pages 113–126, 2012.
[10] TinaTsou, Pedro Aranda, HaiyongXie, Ron Sidi, Hongtao Yin,and Diego Lopez. Sdni: A message exchange protocol for softwaredefined networks (sdns) across multiple domains. 2012.
[11]Xin Hong Wang, Fu Qiang Liu, and Guang Xing Wang.Te routing algorithm to minimize maximum link utilization.Mini-microSystems, 2005
[12]TeemuKoponen, Martin Casado, Natasha Gude, and Jeremy Stribling. Distributed control platform for large-scale production networks, 2014
[13] Seungwon Shin, Phillip A Porras, VinodYegneswaran, Martin W Fong, GuofeiGu, and Mabry Tyson. Fresco: Modular composable security services for software-defined networks. In NDSS, 2013.