Study on Simulated ZMW Attack

Xingman Chen, Yanhui Guo, Qi Li

Beijing University of Post and Telecommunications, Beijing 100876, China;
x-man@bupt.edu.cn

Keywords: ZMW; BGP session; LDoS; BGP table version number; Route flapping

Abstract. ZMW is a BGP-session-targeted LDoS (Low-Rate Denial of Service) attack, which can leave a drastic impact on the network infrastructure. Therefore, it's essential to identify and know the attack. In this paper, we first establish a small-scale and double-link experimental network of BGP on the network simulator GNS3 to study this attack and generate LDoS attack flows by getting the required parameters. Then, we redo ZMW attack on target links through single nodes. We measure the overall effect of ZMW attack by monitoring the data traffic of target links and redundant links, and identify the links with route flapping by gathering the characteristic parameter, BGP table version number, and finally measure the attack efficiency of ZMW with adjusting the lengthen of UDP packet. We study and grasp this attack technology against BGP session, so as to give proper prevention scheme in time, thus effectively ensure the security of network and communication.

Introduction

On the NDSS (Network and Distributed System Security Symposium) in 2007, Zhang, Mao, Wang, have proposed the LDoS attack targeting BGP which is a routing protocol running on the target links in their study [1]. They point out that this attack can contribute to lengthen the time of network convergence and lead to the reset of BGP session. On the NDSS in 2010, Max Schuchard et al. from University of Minnesota have named this attack as ZMW attack after the initials of Zhang, Mao, and Wang in their study [2]. In addition, they have testified that by simulation it can lead to the collapse of the whole internet for several hours if it does ZMW attack on multiple BGP sessions using botnet of 250,000 nodes.

So far, people have studied ZMW attack by mainly using Network Testbed[1] and simulation platform[2]. However, there are mainly two limits here. One is that it's rather expensive to establish a set of testbed and simulation platform. The other is that it's difficult to redo ZMW attack by using NS-2—the network simulator based on discrete event simulation technique, which is widely used in the study on TCP-targeted LDoS attack, because it take no account of the physical properties and therefore loses its authenticity of simulating route. No paper has done the study on ZMW attack by using NS-2 until now. On the other hand, considering that the essence of ZMW attack is LDoS attack, studies have been done by testing LDoS attack flows with time domain[4][5][6] and frequency domain[7][8]. However, with those methods, it needs large quantity of computing resources, and can't locate the specific link with route flapping effectively. And no effective testing method has been achieved so far. At last, the studies on ZMW attack mainly focus on the study and comparison of attacking parameters to get the possibility of resetting BGP session and the time that route table transforms [1], but they haven't weighed the ratio between costs (including rate, time of sending packets and so on) and the impact may lead to (including time period and possibility of resetting BGP session etc.).

In this paper, first, we establish a small-scale BGP experimental network with redundant links by GNS3—the mirrored, open, and convenient network simulator using Cisco IOS. Second, we compute each attacking parameter that is required to form LDoS attack flows, such parameters as pulse length L, attacking period T, and pulse intensity R [3], and then we form the binary pulse flow of UDP. Third, we do ZMW attack on target links by using single-attack nodes, and then measure the overall effect of ZMW attack by monitoring the data traffic of target links and redundant links, and identify and locate the links with route flapping by gathering the characteristic parameters—BGP table version number. At last, we measure the efficiency of the attack caused by the costs of attackers through defining and computing the lengthen of different UDP packets.

Background Introduction

ZMW Attack. ZMW attack is a type of LDoS attack targeting route infrastructure, which is different from Shrew attack. ZMW attack targets the BGP session taking TCP as its transport protocol, and it can form binary pulse flow of UDP by obtaining the attacking parameters like RTT, minRTO and link bandwidth etc. of target BGP session pairs. And then it destroys BGP message in control plane by using the attack flows in data plane, which leads to the loss of packets of KeepAlive message in control plane for repeated transmission. Once the Hold Timer that BGP session pairs stay in BGP session runs out, reset BGP session. The process is shown in Fig .1. And,

$$\mathrm{n} = \mathrm{floor}\left[log_2\left({}^{HoldTimer}/_{minRTO} + 1\right)\right] - 1, \mathrm{n} \in \mathrm{N} \tag{1}$$

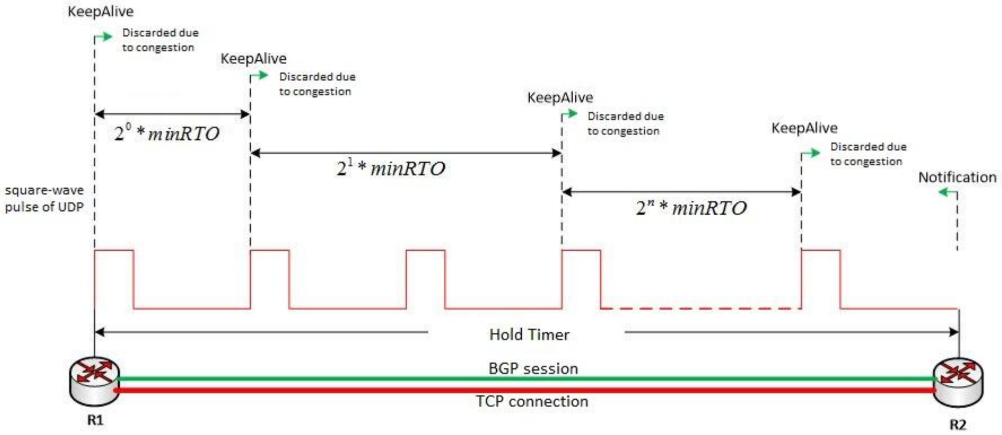

Figure. 1 ZMW attack

The state of route is changed once resetting BGP session. Then BGP route will undo the target links by starting Update to update message, which induces that the router computes its routing table again and the attack flows are led to another path again. Therefore, it eliminates the congestion in target links, BGP session pairs will be formed again, and then the state of route is changed again and so forth. The process is repeated over and over again. As a result, BGP session switches frequently under the state of Up and Down, and Update message is generated frequently as well, which lead to network instability. In general, ZMW is LDoS attack, which targets BGP session in bottleneck links. Thus, the three key factors [3] in LDoS attack are also important for ZMW attack.

BGP Table Version Number. ZMW attack results in reset BGP session, which generates Update message. However, we cannot judge and identify the links whose BGP sessions have been resetted by those Update message. In this paper, we present a way to identify those links by gathering BGP table version number. Providing the current state of routing table, BGP table version has certain relationship with Update message. The increase of BGP table version number definitely results from the generating of Update message; however, generating Update message does not always lead to the increase of BGP table version number, and only with the change of BGP route strategy that is the optimal route, the increase can occur.

As resetting BGP session in the target links, the optimal path of the related two routing devices is inevitably to change, therefore, BGP table version number of those two routing devices, but not that of other routing devices, increases. The fact is that the optimal path is to change twice during the reset of BGP session, so that BGP table version number will be doubled according to the number that the optimal path has changed. Thus, the links with routing flapping can be identified by the sign that BGP table versions of at least two routing devices increase in accordance with the same rule within the same interval.

Attack Efficiency. In order to measure how to get the greatest efficiency with the lowest cost, we have consulted the papers done by other experts [12], and we define attack efficiency as following:

$$\Pi = \frac{Damage}{Cost} = \frac{C_{Receive} - C_{Send}}{{}^{RL}/_{T}} \tag{2}$$

The equation above is the ratio of the loss to the cost of launching ZMW attack. What’s more, in this paper, we define the loss of launching ZMW attack as the difference between sending rate of attackers and receiving rate of receivers for UDP packet. And we define the cost of launching ZMW attack as effective attacking rate, i.e. the ration of product of pulse intensity R and pulse length L to attacking period T. Attack effect is closely related to attack efficiency.

Establish Simulation Experiment

The experiment topology we establish in the network simulator GNS3 is a simple double-link topology containing 4 routing devices, 3 terminal devices, and 7 network segments. With the double-link topology, we can easily detect how the target links and redundant links complement each other in the attack flows for that it will be led to redundant links during the reset of BGP session.

The 4 routing devices in the topology belongs to 4 AS domains respectively, but with the same model Cisco 7206 and same version 12.4. In this paper, the routing devices interfaces, bandwidth (10M), SNMP, and BGP session are configured, but other parameters all use the default settings with that the sending interval of KeepAlive message is 60s, HoldTimer is 180s. The operating systems of attackers in the 3 terminal devices and targets are all Ubuntu, but that of the traffic monitor is Windows XP. Those three are all deployed in virtual machine (VMware), but belongs to 3 network segments with different Host-only types. They declare through BGP. We launches ZMW attack by using single-attack source, and we take no account of the procedure of selecting the bottleneck links——target links for small-scale BGP experiment network. Thus, in this paper, we assume that target links are R1<->R2, and redundant links are R3<->R4. We obtain the received the amount of bytes in the interfaces of SNMP induction spots of R2 and R4 by SNMP MIB Browser to monitor the traffic.

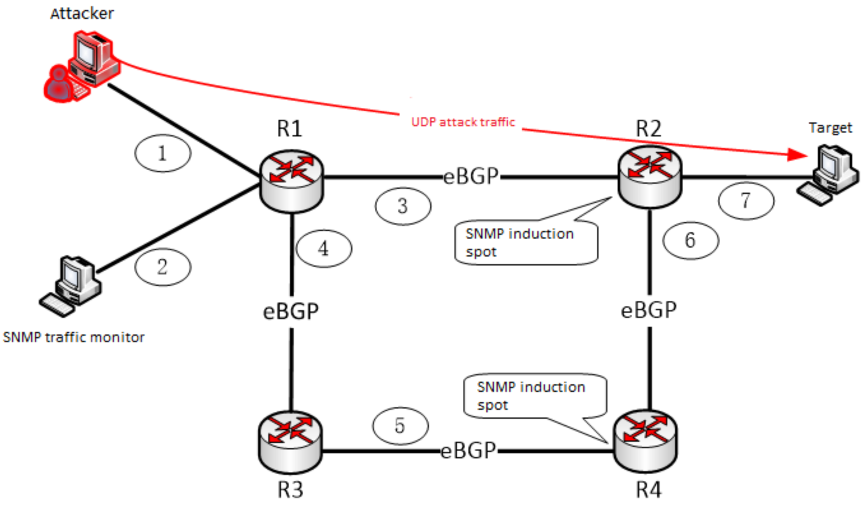

Figure. 2 Simulation experiment topology

Obtain Attacking Parameter

Attacking parameters include pulse length L, attacking period T, and pulse intensity R. L represents the time period that the attacker sends packet at high speed. Only L is large enough, can it result in the loss of packet, and then BGP session taking TCP as its transport protocol can be induced to enter the state of overtime retransmission. And often the best value of L is twice of the largest RTT at different time ($L \sim 2 * \max(RTT_1, RTT_1, \cdots, RTT_1), n \in N$). T, the time interval among attacking pulses, often takes minRTO as its optimal value that is $T \sim$ minRTO. R represents the sending rate of attack flows. And the larger R is, the better, which can lead to network congestion. It is at least larger than the bandwidth of target links, i.e. $R \geq C_{target\_link}$.

In this paper, we obtain minRTO of BGP routing devices in the platform of GNS3 simulation as 300ms by using tcpRtoMin of SNMP MIB Browser. According to Eq.1, when KeepAlive message is retransmitted for the ninth time, it can lead to the reset of BGP session. We employ Iperf tool to obtain the bandwidths of links in different sizes of TCP windows, and the results are shown in Fig .3. As TCP window get larger and larger, bandwidth of target links levels off and is within 1.1-1.2Mbps (As GNS3 is the simulator subject to the properties of the host, the bandwidth can't be up to the real standard—10M, which has no impact on conducting the experiment). Eventually, we note the bandwidth of the links as 1.2Mbps. In this paper, we get the value of RTT of the routes between R1 and R2 by using Wireshark, which is seen in Fig .4, and it is between 10ms to 60ms. The specific parameters of LDoS attack flows are defined as following:

1) Pulse intensity R: 2Mbps (>1.2 Mbps),

2) Attacking period T: 300ms (minRTO),

3) Pulse length L: 100ms (between 40ms and 120ms, i.e. 2*RTT).

Apart from the three essential parameters, there is another variable parameter—UDP packet length. It greatly affects not only the size of sending packets, but the sending interval of packets as well. Different from the former three parameters, it can be decided by the attacker. Therefore, we lay more emphasis on checking the attack efficiency of ZMW attack with different lengths of UDP packets in the latter part of this paper.

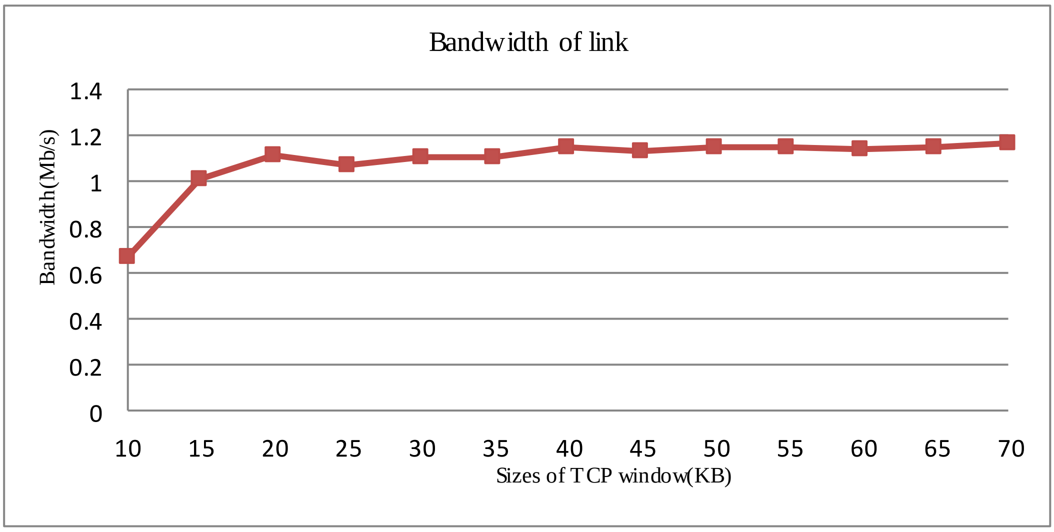

Figure. 3 Bandwidth of target links

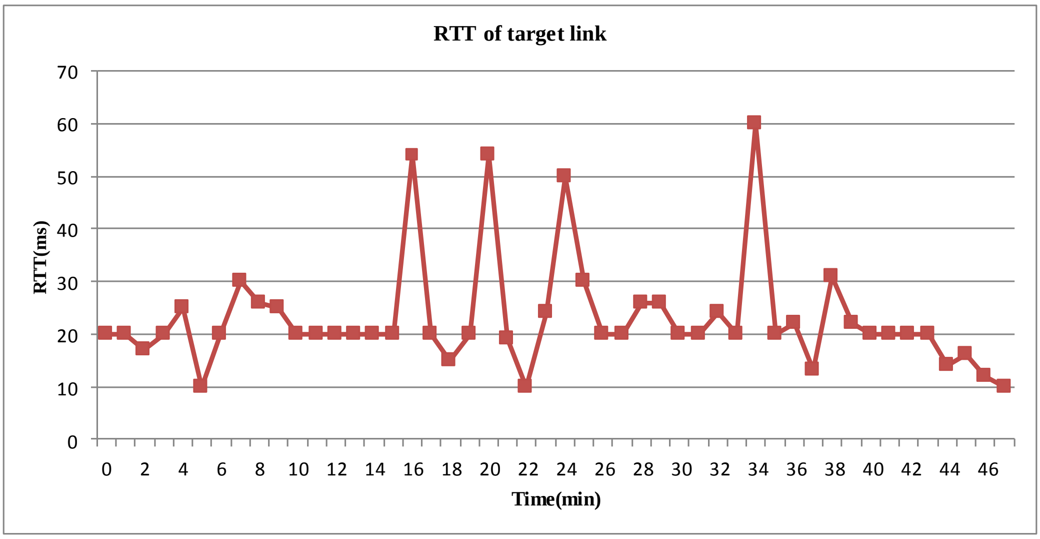

Figure. 4 RTT of Target links

With the obtained attacking parameters and UDP packet length, plus Matlab, we make LDoS attack flows. Then we open the SNMP traffic monitor to monitor the interfaces of R2 in target links and the received traffic data of the induction spots of interfaces of R4 in redundant links. It gathers BGP table version number by operating *show ip bgp summary* on routing devices and the frequency is every other second. Next, it can do ZMW attack to target host in the attacking end, and meanwhile, record the sending rate and receiving rate. We take the amount of received UDP bytes in SNMP induction spot as the overall measurement result of ZMW attack, identify the links with routing flapping by gathering BGP table version number, and measure the impact that different UDP packet lengths have on through attack efficiency.

Experiment Results

The experiment result is that UDP packet length is 10 Bytes and the overall packets size is 52 bytes, which is shown in Fig .5. Overall, the UDP packet flows between target links and redundant links are complementary to some extent, which accords with the result from ZMW attack. In addition, UDP packet flows are placed in the target links for most of the time that is within $[180s, 180 + n * 60s], n \in N$, and 180 is HoldTimer, 60 is the sending interval of KeepAlive, and n is the times that UDP packet flows sent by attacker staggers KeepAlive message generated by router. Only few UDP packet flows are placed in the redundant links, and their stay time is about 30s that is the time of resetting BGP session.

In the beginning, the optimal path from attacking end and the target host passes the target links, so that the LDoS attack flows sent by attacker are first led to the target links. Therefore, it causes data-plane congestion on R1 router, and then results in control plane congestion of BGP session. In addition, the KeepAlive message R1 sending to R2, and that of retransmission are subject to the constantly loss of packets. If R2 does not receive the KeepAlive message sent by R1 within the holding time, BGP session of R1 will be interrupted. Thus, the network is to compute route table, so that the redundant link become the optimal path and LDoS attack flows are led to the redundant link. As the target link rebuilds BGP session, the optimal path is to change again, and the process is repeated in cycles.

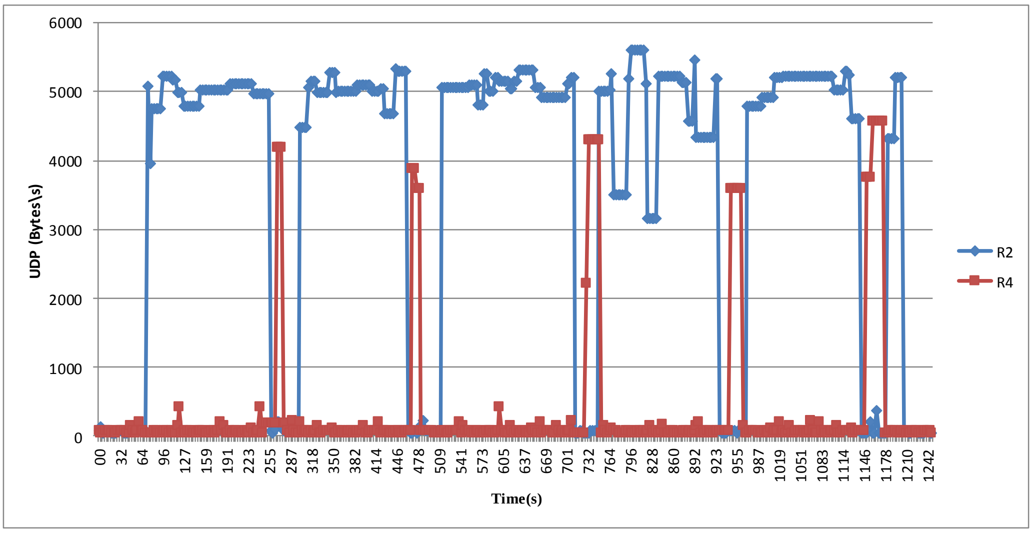

Figure. 5 Amount of received bytes of the induction spots on R2 and R4

Each time after resetting BGP session, we gather BGP table version number by conducting *show ip bgp summary* on every routing device. In this paper, we only gather the variation conditions of BGP table version number as resetting BGP session 5 times, which is shown in Fig .6. We can see that after resetting BGP session every time, BGP table version numbers of R1 and R2 mainly increase by 4 and 6 separately, however, those of R3 and R4 stay the same. As downing BGP session, as for R1, the generated Update message has declared that its optimal paths to network segments 6, 7 in Fig .2 have changed, so that its BGP table version number increases by 2 (1+1). As for R2, similarly Update message has declared that its optimal paths to network segments 1, 2, 4 in Fig .2 have also changed, so that BGP table version number of R2 increases by 3 (1+1+1). However, as for R3 and R4, they have not received any declaration from Update message. As BGP session goes up again, R1 and R2 do the same as above, as a result, always BGP table version number of R1 increases by 4 and that of R2 increases by 6, in the same way, that of R3 and R4 remain the same. We can draw the conclusion that the Update message generated during the reset of BGP session cannot increase all BGP table version numbers of routing devices. Only the optimal paths change, can it increase. Thus, routing flapping can definitely increase BGP table version number, although not all increase of it results from routing flapping. Therefore, we can decide that the links between two routers, which they change according to the same increasing law within almost same time interval (180s, i.e. holding time), have had routing flapping.

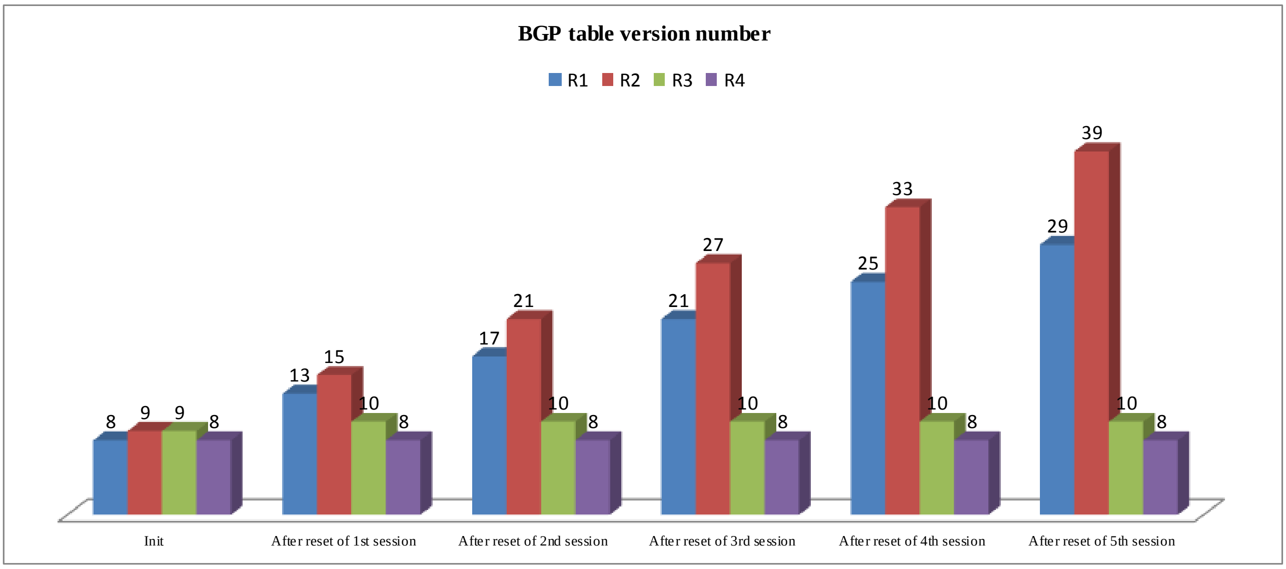

Figure. 6 Variation conditions of BGP table version number

At last, without changing the other three attacking parameters, in this paper, we launch ZMW attack by changing UDP packet length (Binary LDoS attack flows need to be remade each time UDP packet length changes here). Meanwhile, we record the sending rate and receiving rate with different UDP packet length and then calculate its attack efficiency according to Eq.2. The result is shown in Fig .7, and we can see that as UDP packet length increases, attack efficiency decrease gradually. As R is 2Mbps, L is 100ms and T is 300ms, the longer UDP packet length is, the attack is less effective, which is justified by that the time of resetting BGP session has been prolonged and the possibility of resetting has been lowered etc. And the cause is that the shorter UDP packet length is, the sending interval of packet is shorter, and then the sending frequency of attacking packet is faster. Thus, the Buffers of entrance and exit on router will be filled soon; as a result, the generated Keep Alive message constantly loses its packets on the Buffer of exit, and the receiving rate on receiving end is declined. Eventually, the difference between sending rate and receiving rate has been bigger and bigger, which leads to that attack efficiency is rather high. Although UDP packet length is quite long, it can also fill the Buffer of entrance immediately, but it cannot greatly affect the Buffer of exit. As a result, KeepAlive message will not lose easily, and attack efficiency will be lowered in this way. In addition, from Fig .7, we can see that attack efficiency decreases sharply within 10 Bytes to 50 Bytes, and after that, attack efficiency has a gentle decrease for that the longer UDP packet length is, the possibility of resetting BGP session is smaller.

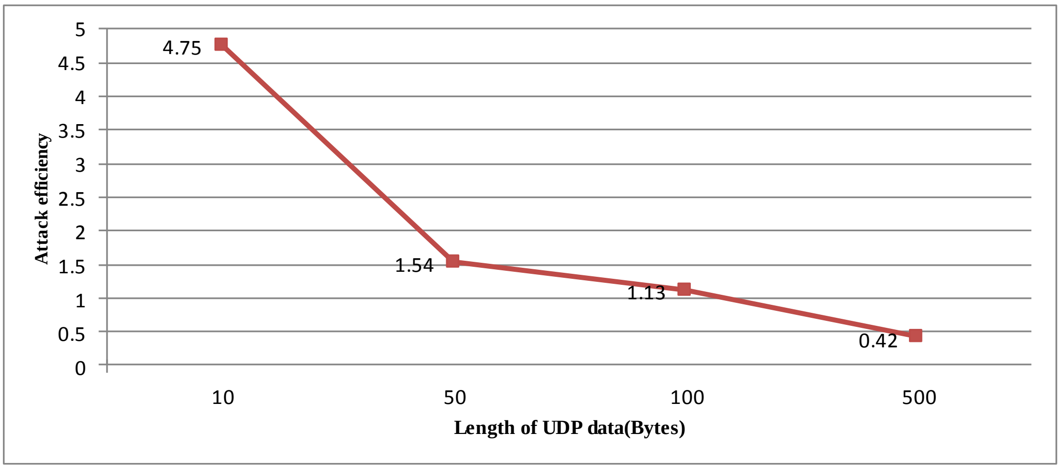

Figure. 7 Attack efficiency with different UDP packet length

Conclusion

In this paper, we build double-link topology in GNS3 and obtain the required attacking parameters to make UDP attack flows, and then to redo ZMW attack; eventually, the routing flapping can be achieved. It is the first to introduce two parameters that are BGP table version number and attack efficiency. By the former parameter, the links with routing flapping can be identified effectively; and the latter one can measure the impact that ZMW attack has left on with different UDP packet lengths. Our future study will devote to enlarge the experiment scale and examine more attacking parameters to expand the study scope.

Acknowledgements

This work is supported by *National Natural Science Foundation of ChinaProject* (61302087, 61401038).

References

[1] Y. Zhang, Z. M. Mao, and J. Wang: *Low-rate TCP-targeted DoS attack disrupts internet routing*. In NDSS. The Internet Society, 2007.

[2] Max Schuchard, Eugene Y. Vasserman, Abedelaziz Mohaisen: *Losing Control of the Internet-Using the Data Plane to Attack the Control Plane*. NDSS 2010.

[3] A. Kuzmanovic and E. W. Knightly: *Low-Rate TCP-Targeted Denial of Service Attacks.* In Proc. ACM SIGCOMM, 2003.

[4] Sun H, Lui J C S, Yau D K Y: *Distributed mechanism in detecting and defending against the low-rate TCP attack*. Computer Networks[J]. The International Journal of Computer and Telecommunications Networking, 2006, 50(13): p.2312-2330.

[5] Kwok Yu-Kwong. Tripathi R, Chen Yu, et al. HAWK: *Halting anomalies with weighted choking to rescue well-behaved TCP sessions from shrew DDoS attacks*[C]// Proceeding of Internet Conference on Computer Networks and Mobile Computing. Zhangjiajie, China, 2005: p.423-432.

[6] Luo Xiaopu, Chan Edmond W W, Chang Rocky K C. Vanguard: *A new detection scheme for a class of TCP-targeted denial-of-service attacks*[C]//Proceeding of the 10th IEEE/IFIP Network Operations and Management Symposium. Cannada, 2006: p.507-518.

[7] X Luo and RKC Chang: *On a New Class of Pulsing Denial-of-Service Attacks and the Defense*. In NDSS, San Diego, CA., 2005, p.2-5.

[8] Chen Y, Hwang K. Collaborative: *Detection and filtering of shrew DDoS attacks using spectral analysis*[J]. Journal of Parallel and Distributed Computing, 2006, 66(9):1137- 1151.

[9] Information on http://www.gns3.net.

[10] Information on http://www.cisco.com/en/US/tech/tk365/technologies_tech_note.shtml.

[11] Information on http://www.networkworld.com/understanding-bgp

[12] Guirguis M, Bestavros A, Matta I. Exploiting the Transients of Adaptation for RoQ Attacks on Internet Resources. June 2004.