Research on the Aggregation and Synchronization of LDDoS Attack Based On Euclidean Distance

Meng Yue
Tianjin Key Lab for Advanced Signal Processing, Civil Aviation University of China, Tianjin, China
Email: myue@cauc.edu.cn

Zhijun Wu and Jin Lei
Tianjin Key Lab for Advanced Signal Processing, Civil Aviation University of China, Tianjin, China
Email: {zjwu, jlei}@cauc.edu.cn

Abstract—**Flow aggregation or time synchronization ensures low-rate denial of service (LDoS) attack flows form an ideal rectangular pulse at the victim to maximize attack efficiency. The differences of end-to-end delay between each host are critical for aggregation or synchronization. A new approach based on Euclidean distance is proposed to avoid the complexity of direct measuring internet end-to-end delay. Using NS2 experiments, the performances of such coordinated attack are shown and compared with uncoordinated attack. Test results prove that an aggregated or synchronous LDoS attack launched by the approach is even more detrimental.**

Index Terms—**low-rate denial of service (LDoS), Euclidean distance, aggregation, synchronization**

I. Introduction

LDoS attack can degrade the capability of the system or severely reduce service quality by subjecting the system to a fairly low-intensity attack traffic, which makes the system inefficient and unstable [1]–[3]. Because of its low-rate characteristic, LDoS attack is more secluded than traditional flooding-based DoS. (Generally, by adjusting the attack parameters, the LDoS attacker can cause different levels damage [4]–[7], ranging from degradation-of-service to absolute denial-of-service). The tradeoff between the "damage" inflicted by an attacker (e.g., waste in bandwidth) and the "consumption" of the attack (e.g., average attack rate) should be considered. At the premise of keeping enough power to cause a large number of packets loss, an aggregated or synchronous LDoS attack (well orchestrated and timed) can save the consumption of each attack host and elude detection of counter-DoS mechanisms [8]–[11].

Generally, there are two attack models [12], [13]: TCP-Congestion-Control-Based and Router-Queue-Management-Based. In this paper, the aggregation and synchronization of LDoS attack are investigated in two models respectively. We begin with describing the characteristics of LDoS attack, then， propose a new Euclidean-Distance-Based approach to ensure aggregation or synchronization. According to the new approach, comparing the performances of aggregated attack and non-aggregated attack, and comparing the performances of synchronous attack and asynchronous attack. Through NS2 experiments the advantages of an aggregated or synchronous LDoS attack have been proved. At the end of paper, we draw a conclusion.

II. Characteristics of LDoS Attack

In essence, an LDoS attacker generates a sequence of false congestion signals to the victim using periodic attack pulses [12], [13]. As shown in Fig. 1, a single source LDoS attack can be modeled by a square waveform. T is the time interval between two consecutive attack pulses, L indicates the time period during which attackers send packets, and R exhibits the peak rate by which attacking flow is sent. This type of attack is named low-rate attack, as L/T is small. If L/T=1, LDoS attack becomes flooding-based DoS.

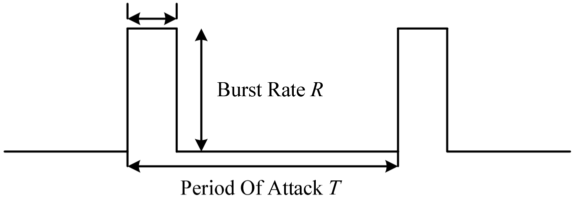


Fig. 1. Single LDoS attack stream.

There are several requirements for successful LDoS attack [12], [14]:

1) Attack period T is appropriate for periodic sending congestion signal and hard to detect.

Manuscript received June 17, 2013; revised December 5, 2013; accepted December 17, 2013.

This work was supported in part by China National Science Foundation under Grant No.61170328 and U1333116, Key Project of Tianjin Natural Science Foundation under Grant No.12JCZDJC20900, and the Fundamental Research Funds for the Central Universities of CAUC under grant 31122013P007, 3122013D007, and 3122013D003.

Corresponding author: Zhijun Wu, Email: zhijun-wu@163.com.

doi:10.4304/jsw.9.7.1854-1861

2) The burst length L is sufficiently long to induce packet loss.
3) The magnitude of the attack peak traffic R is large enough to cause a severe congestion on the link to the victim. When these conditions are satisfied, the legitimate flows will be very low throughputs.

In a distributed scenario, multiple attack sources could low their individual traffic rates further, thereby save the consumption and make the detection even harder[15], [16].

Fig. 2 describes the aggregated LDoS attack. Attack hosts send short attack pulses (For N end-hosts, the rate is $1/N$). If the delay is well calculated, these pulses can aggregate at the victim to form a high rate attack flow.

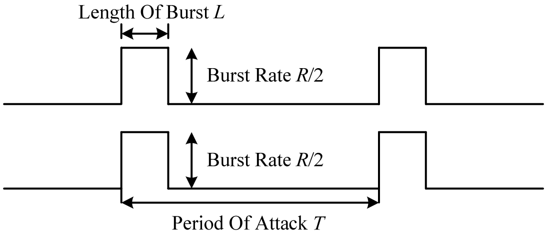


Fig. 2. Multiple LDoS attack streams with low burst rate.

Fig. 3 depicts the synchronous LDoS attack. Attack hosts send long-period attack pulses (For N end-hosts, the period is N times). The attack pulses can synchronous arrive at the victim to form a well-timed attack stream.

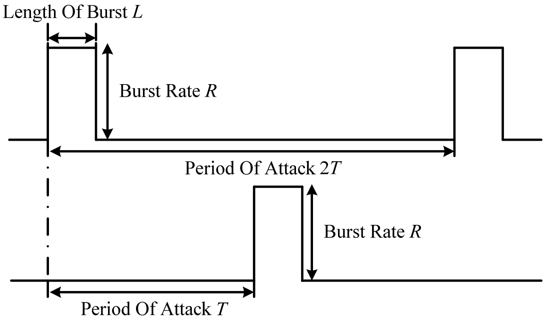


Fig. 3. Multiple LDoS attack streams with long period.

III. How to Implement Aggregation or Synchronization

The differences of network delay from each zombie to victim necessitate aggregation and synchronization. The target of aggregation or synchronization is ensuring that attack flows from diverse zombies follow the desired square wave when arriving at the victim. The desired square wave can maximize attack efficiency and make attack source hard to detect. Assuming that the zombies are not aggregated or synchronous, three problems maybe appeared [17]–[19]:

1) Attacker cannot launch sufficiently high rate to cause congestion.
2) Congestion time is not long enough.
3) It's easier to be detected.

A. End-to-End Delay Analysis

Reference [20] proposes an approach based on timestamp to measure the end-to-end delay, as shown in Fig. 4, choose a controller, which is most close to the victim so that the delay from victim router to controller has minimal effect on aggregation or synchronization. Once the controller C is identified, each delay from zombie to controller can be easily tested (e.g., ICMP/IP timestamp). In Fig. 4, T_{sn} is the zombie sending timestamp, T_{rn} is the controller receiving timestamp, D_n is the delay between zombie to controller. Subsequently, controller can control each zombie to start attacking at opportune moment.

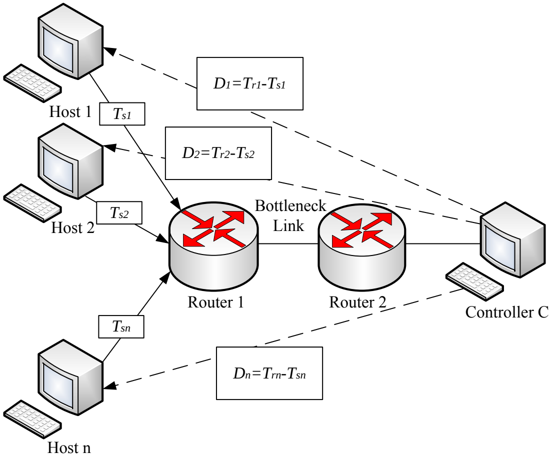


Fig. 4. The approach of implementing aggregation or synchronization

Based on the approach above, the end-to-end delay may be measured in a very simplistic network environment. But it's not adaptive for complex network. In practice, there are two points that should be considered [21], [22]:

1) The path between source node and destination node is always asymmetry, even through it is symmetry, the different queue situations make the end-to-end delay different in the path.
2) The asynchronous clocks in end systems lead to the usage of timestamp to measure end-to-end delay inaccurate. Considering the two issues, there are several existed approaches to measure end-to-end delay, but, generally, they are complex [21], [23].

B. The Approach of Aggregation or Synchronization based on Euclidean Distance

Generally, different zombies send attack pulses with the same attack parameter (T, L, R), as shown in Fig. 2 and Fig. 3. According to the pulse characteristic of LDoS attack, a new approach based on Euclidean distance can be used to keep aggregation and synchronization, thereby avoiding complex measure of end-to-end delay.

For an N-dimensional space, the Euclidean distance is:

$$d(\mathbf{p},\mathbf{q})=\sqrt{(p_1-q_1)^2+(p_2-q_2)^2+\cdots+(p_n-q_n)^2} \quad (1)$$

$\mathbf{p}=(p_1, p_2,..., p_n)$ and $\mathbf{q}=(q_1, q_2,..., q_n)$ are two point sets in Euclidean n-space. Euclidean distance can be seen as the similarity of two signals, the smaller distance $d(\mathbf{p},\mathbf{q})$, the more similar of two signals. To realize the approach based on Euclidean distance, a controller is also chosen closed to the victim, as shown in Fig. 4. The attack packet number from each zombie reached the Controller is sampled as an N dimensions point set.

Choose an attack flow as baseline, the Euclidean distance between baseline and other attack flows can be calculated. According to the Euclidean distance, the start time of each attack pulse can be adjusted dynamically. Repeat calculating the Euclidean distance and adjusting start time until the Euclidean distance is minimal, subsequently the end-to-end delay of each zombie can be confirmed and the aggregation or synchronization can be achieved. The flowchart is shown in Fig. 5:

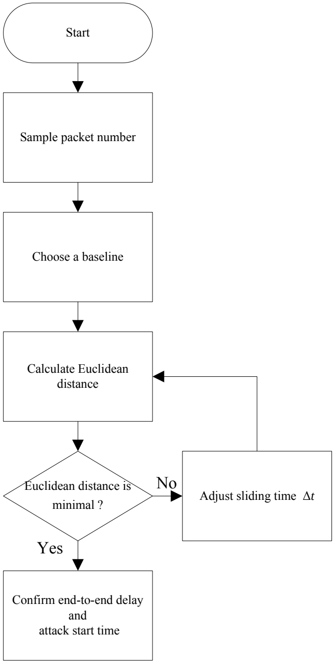

Start
Sample packet number
Choose a baseline
Calculate Euclidean distance
Euclidean distance is minimal ?
No
Adjust sliding time Δt
Yes
Confirm end-to-end delay and attack start time

Fig. 5. Processing flowchart of the Euclidean distance based approach.

As the flowchart shown:

Step1: Sample the received packet number of each attack flow in Controller.

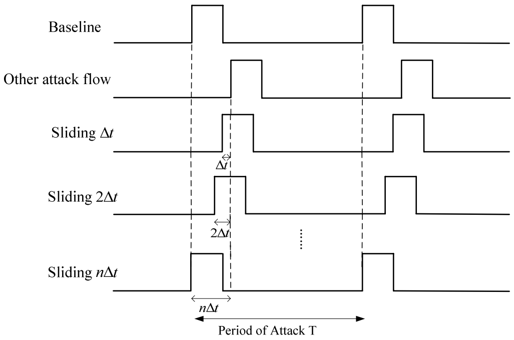
Step2: Choose an attack flow as baseline.

Step3: Calculate the Euclidean distance between baseline and other attack flows respectively.

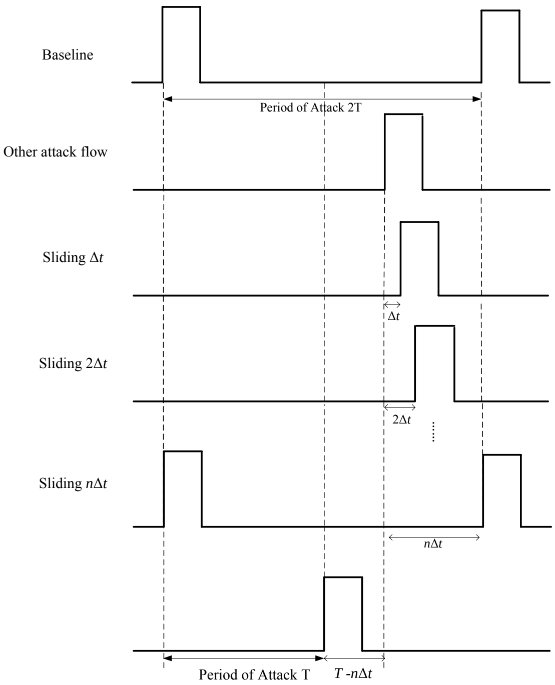
Step4: Adjust attack start time of each attack, and, repeat *Step3*, until each Euclidean distance is minimal.

Step5: According to *Step4*, confirm end-to-end delay of each zombie, and control each attack start at appropriate time.

In Fig. 5, the "sliding time Δt" is the adjusting value of start time before next calculating Euclidean distance. Fig. 6 reveals the adjusting process.



(a) Multiple LDoS attack streams with low burst rate scenario



(b) Multiple LDoS attack streams with long period scenario

Fig. 6. The adjust process of start time.

As shown in Fig. 6 (a), in multiple LDoS attack streams with low burst rate scenario, the final delay $n\Delta t$ between "Baseline" and "Other attack flow" can be achieved after *n* times sliding. That is to say, when the start time of "other attack flow" delay $n\Delta t$, the Euclidean distance is minimal and the LDoS attack is aggregated.

As shown in Fig. 6 (b), in multiple LDoS attack streams with long period scenario, the final delay $n\Delta t$ between "Baseline" and "Other attack flow" can be achieved after *n* times sliding, thereby the Euclidean distance is minimal. So, when the start time of "other attack flow" delay $T-n\Delta t$ (T is attack period), the LDoS attack is synchronous.

IV. Simulating Experiments And Performances Analysis

In this section, performances of aggregation and synchronization attack based on Euclidean distance are analyzed respectively, the results are presented using network simulator NS2.

A. Performances of Aggregated LDoS Attack

Aggregation can low zombie's peak attack rate. To confirm the validity of Euclidean distance used in aggregation, two typical LDoS attacks are simulated below: one is RTO (Retransmission Timeout)-based [10], [12], [16], and the other is RED (Random Early Detection)-based [21]–[25]. The attack performances are compared.

1) Aggregated LDoS Attack based on RTO

NS2 simulations are carried out with the topology shown in Fig. 7. It consists of two routers: Router A (Node 0), Router B (Node 1), two legitimate TCP senders

(Node 3, Node 5), two TCP receivers (Node 7, Node 8), and three UDP LDoS attack sources (Node 2, Node 4, Node 6). TCP Reno is used for the purpose of experiment, which is most vulnerable. The minRTO is set to 1000ms. Test duration is 20s.

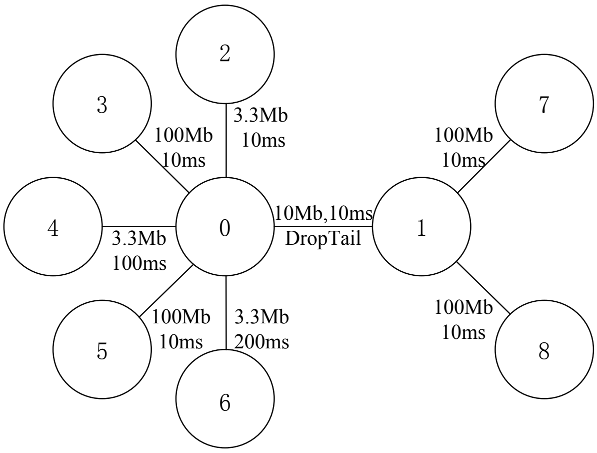


Fig. 7. The RTO-based dumb-bell topology

Link capacity and delay are set as Table I.

TABLE I.
LINK CAPACITY AND DELAY IN RTO-BASED ATTACK

Node	Link Capacity	Delay
(0, 1)	10Mbps	10ms
(2, 0)	100Mbps	10ms
(3, 0)	100Mbps	10ms
(4, 0)	100Mbps	100ms
(5, 0)	100Mbps	10ms
(6, 0)	100Mbps	200ms
(7, 1)	100Mbps	10ms
(8, 1)	100Mbps	10ms

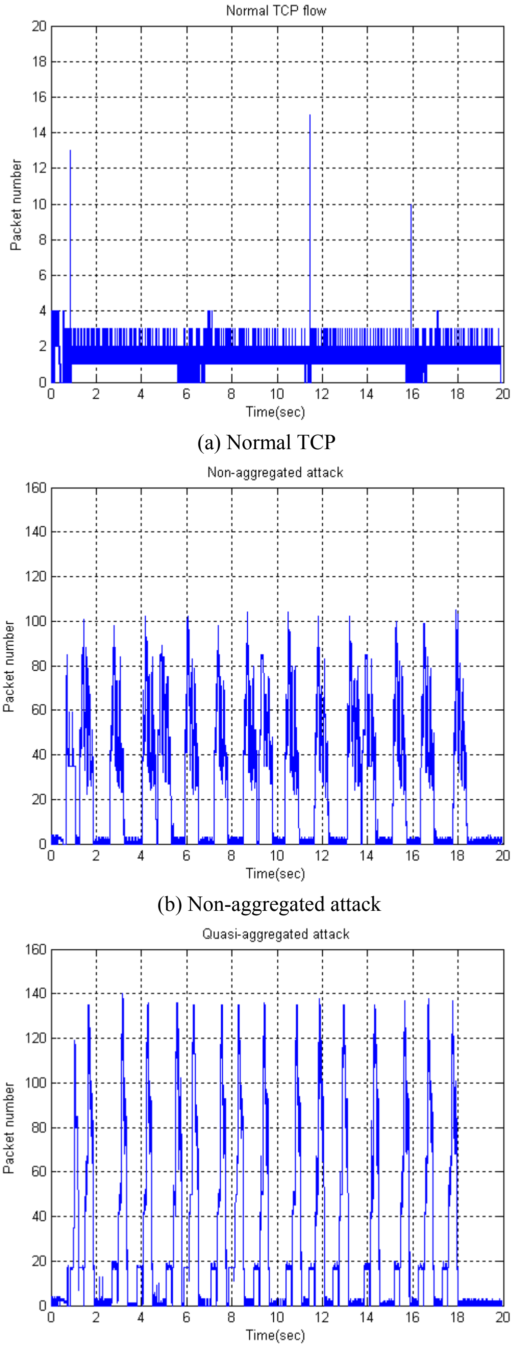
As shown in Table 1, two routers are connected through a bottleneck link of 10Mbps with 10ms delay, other links are 100Mbps, so we set LDoS attack parameters T=1150ms, L=150ms, R=3.3Mbps. All TCP senders and TCP receivers have a one-way delay of 10ms corresponding to Router A and Router B respectively. Delay of each LDoS attack source to Router A is shown as Table 1.

Assuming the delay of each LDoS attack source to the victim Router B is uncertain. It could be tested by the approach based on Euclidean distance. Set sample interval 1ms and sample period 500ms, choose attack flow from Node 2 as baseline, the sliding time Δt =1ms. Define t_p is the delay between Node p and Node 2. The Euclidean distance between Node m and Node n is denoted d(m, n). When t_4=90 Δt =90ms and t_6=190 Δt =190ms, the two Euclidean distances are minimal, namely, $d(2, 4)_{min}$=40.4, $d(2, 6)_{min}$=48.6. It means that Node 4 should start attack 90ms earlier than Node 2, and Node 6 should start attack 190ms earlier than Node 2.

According to these calculated results, attack start time can be set to form an aggregated LDoS attack stream in the victim, this aggregation is named as quasi-aggregated attack. In contrast, if the start time is not well orchestrated, it's named as non-aggregated attack, and, if the delay of all LDoS attack sources to the Router A is set to a fixed value (10ms), it's named as ideal-aggregated attack.

To confirm the effect of aggregated LDoS attack launched by the approach of Euclidean distance. The number of packets arrivals at Router B is sampled with a period of 1ms. Fig. 8 compares the time series patterns:

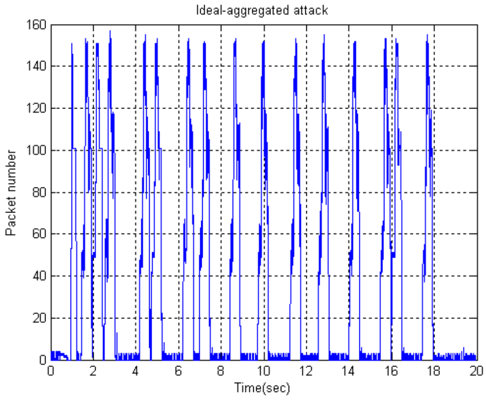
1) Legitimate TCP flows without LDoS attack flows (see Fig. 8 (a)).
2) TCP flows with non-aggregated LDoS attack flows (see Fig. 8 (b)).
3) TCP flows with quasi-aggregated LDoS attack flows (see Fig. 8 (c)).
4) TCP flows with ideal-aggregated LDoS attack flows (see Fig. 8 (d)).



(a) Normal TCP

(b) Non-aggregated attack

(c) Quasi-aggregated attack

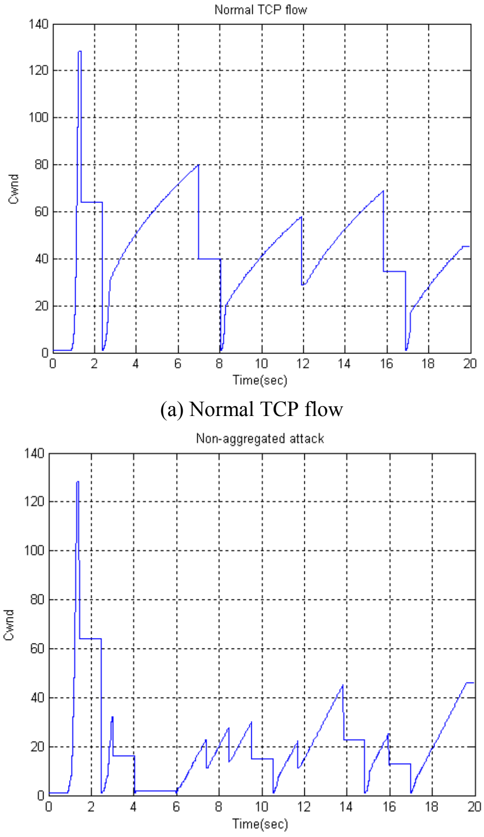


(d) Ideal-aggregated attack

Fig. 8. Comparison of traffic time series patterns

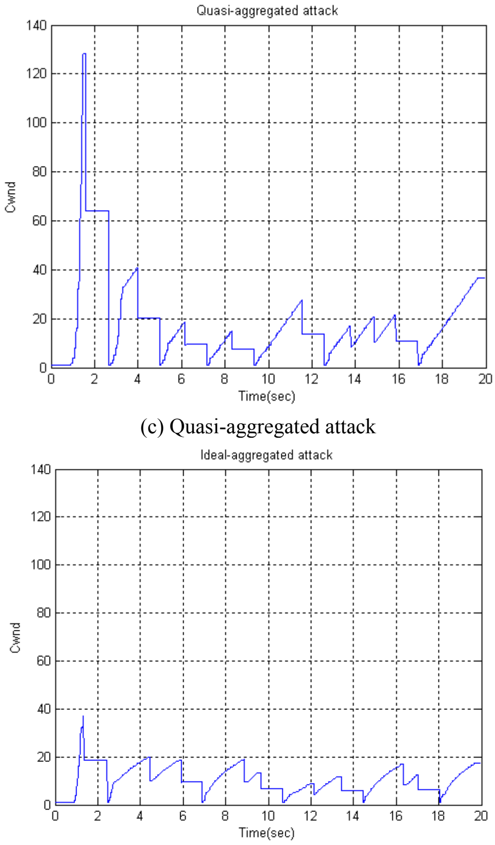
As shown in Fig. 8, normal TCP flows are comparatively smooth. The number of the quasi-aggregated packet is larger than the non-aggregated, and the length of attack pulse implied in the Fig. 8 is narrower and more regular. On the other hand, the ideal-aggregated can provide the best attack, but it's almost infeasible in actual application.

When RTO-based LDoS attack happens, legitimate TCP sender's Cwnd (Congestion Window) is reduced [26-28]. Fig. 9 depicts the Cwnd of node 3. The variation regulation of normal TCP's Cwnd is almost compliance with RTO mechanism (see Fig. 9 (a)). Oppositely, LDoS attack maintains TCP send's Cwnd in a low level. As shown in Fig. 9 (c), the Cwnd of the quasi-aggregated is much smaller than the non-aggregated (see Fig. 9 (b)), and almost identical to the ideal-aggregated (see Fig. 9 (d)).



(a) Normal TCP flow

(b) Non-aggregated attack



(c) Quasi-aggregated attack

(d) Ideal-aggregated attack

Fig. 9. Variation of Cwnd

Fig. 10 depicts the normalized throughput of bottleneck link. As shown in Fig. 10, an ideal-aggregated attack might reduce the throughput to 12.5% of the normal level, to 36.7% by non-aggregated attack and to 18.8% by quasi-aggregated attack. These data illuminate that the performance of the quasi-aggregated is obvious superior to the non-aggregated.

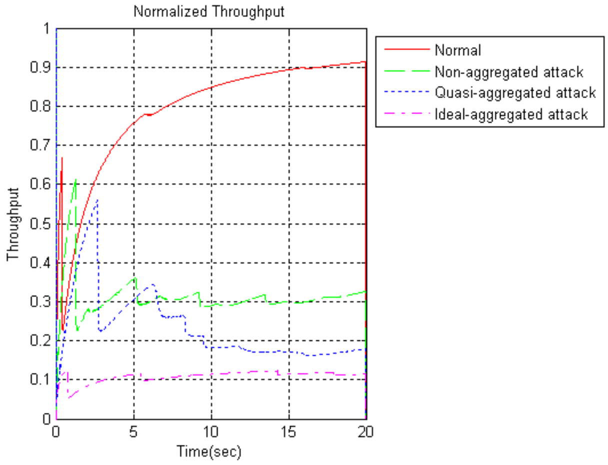


Fig. 10. Normalized throughput in bottleneck link

2) Aggregated LDoS Attack based on RED

In this section, the RED-based LDoS attack is focused. NS2 simulation topology is shown as Fig. 11, where, RED queue management is used. The RED parameters, minimum and maximum thresholds, are tuned to 5 and 15 respectively. The weight parameter is chosen to be 0.002.

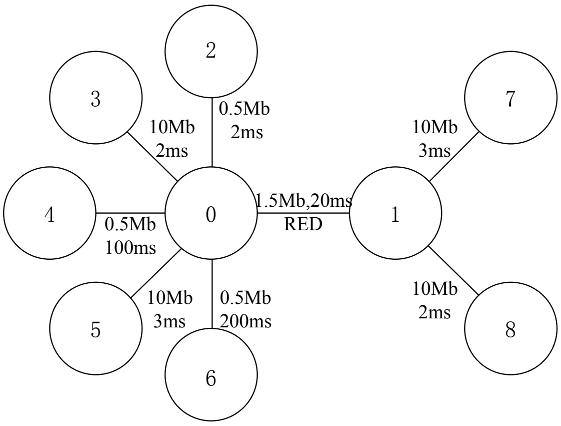


Fig. 11. The RED-based dumb-bell topology

Link capacity and delay are set as Table Ⅱ.

TABLE Ⅱ.
LINK CAPACITY AND DELAY IN RED-BASED ATTACK

Node	Link Capacity	Delay
(0, 1)	1.5Mbps	20ms
(2, 0)	10Mbps	2ms
(3, 0)	10Mbps	2ms
(4, 0)	10Mbps	100ms
(5, 0)	10Mbps	3ms
(6, 0)	10Mbps	200ms
(7, 1)	10Mbps	3ms
(8, 1)	10Mbps	2ms

As shown in Table 2, bottleneck link capacity is 1.5Mbps with 20ms delay, other links are 10Mbps, so we can set LDoS attack parameters T=1050ms, L=50ms, R=0.5Mbps.

Similarly, set sample interval 1ms and sample period 500ms, choose attack flow from Node 2 as baseline, the sliding time Δt =1ms. When t_4=102 Δt =102ms and t_6=197 Δt =197ms, the two Euclidean distances are minimal, namely, $d(\mathbf{2},\ \mathbf{4})_{\min}$=106.9, $d(\mathbf{2},\ \mathbf{6})_{\min}$=109.2. It means that Node 4 should start attack 102ms earlier than Node 2, and Node 6 should start attack 197ms earlier than Node 2.

Fig. 12 depicts the variation of average queue size in time series. Clearly, after a short time, normal RED queue size stabilizes, indicating that the system converges to an efficient operating point. However, LDoS attack causes oscillation of queue size, system cannot stabilize in an efficient operating point.

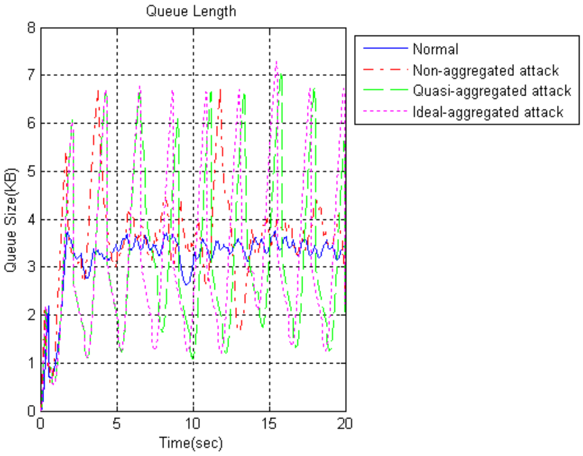


Fig. 12. The effect of RED-based LDoS attack to victim's queue length

As shown in Fig. 12, queue size presents more oscillatory in quasi-aggregated LDoS attack, whose performance is similar with ideal-aggregated, but obvious superior to non-aggregated.

LDoS attack causes the link congestion, so legitimate TCP senders are compelled to lower packet sending rate. Table Ⅲ depicts the number of TCP packets in different conditions. Taking node 3 as example, compared with normal TCP flows, quasi-aggregated attack causes 48.68% packet loss rate, which is close to 51.93% caused by ideal-aggregated attack. However, only 4.25% packet loss rate is obtained in non-aggregated attack.

TABLE Ⅲ.
COMPARISON OF PACKETS IN DIFFERENT TYPES

Node Type	3	5
normal	1787	1662
non-aggregated	1711	1337
quasi-aggregated	917	897
ideal-aggregated	859	894

Queue size oscillation and packet loss lead to the throughput reduction in bottleneck link. Fig. 13 depicts the normalized throughput between Router A and Router B. Compared with normal TCP flows, the throughput is reduced at least 50% in quasi-aggregated attack, the reduction rate is close to ideal-aggregated attack and 38.57% lower than non-aggregated attack. These results confirm that the performance of the quasi-aggregated is obvious superior to the non-aggregated.

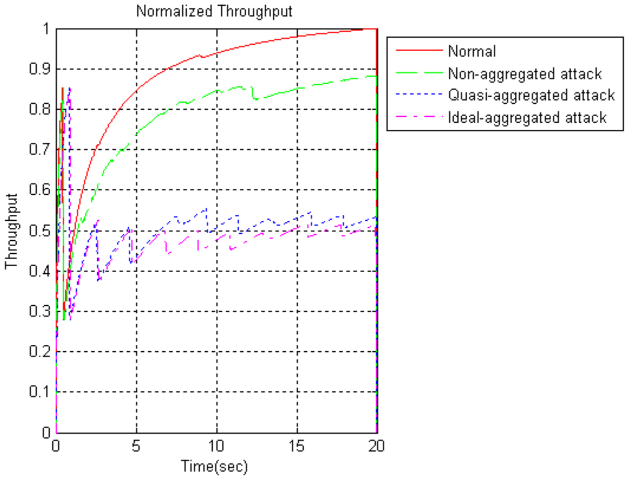


Fig. 13. Normalized throughput in bottleneck link

B. Performances of Synchronous LDoS Attack

Synchronization can extend attack period. As mentioned above, synchronous LDoS attack can provide as excellent attack effects as aggregated attack. For simplicity, only the throughput of bottleneck link, as the most direct reflection of attack performance, is given in this section.

In synchronization scenario, network topology and parameters of RTO-based attack are same as that in Fig. 7. Set attack period T=3450ms, attack length L=150ms， attack rate R=10Mbps. Meanwhile, network topology and parameters of RED-based attack are same as that in Fig. 11. Set attack period T=3150ms, attack length L=50ms， attack rate R=1.5Mbps. Because the synchronous attack requires each attack pulse be difference of a period T, so the final start time of each attack flow should be $(k-1)T-t_p$, k is the number of attackers, T is attack period.

Fig. 14 depicts the throughput of bottleneck link in RTO-based attack. As shown in Fig. 14, the throughput degradation caused by non-synchronous attack is close to that caused by quasi-synchronous attack and ideal-synchronous attack.

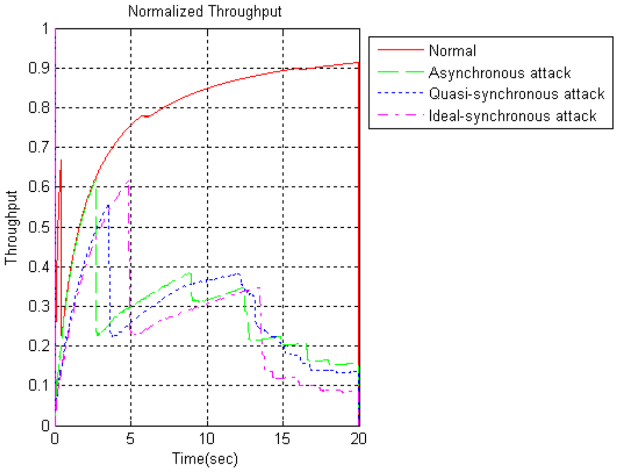


Fig. 14. Throughput in RTO-based synchronous LDoS attack

At the premise of keeping attack rate R sufficiently large, if the delay of each LDoS attack source is small, the performances of asynchronous attack and synchronous attack are almost same. The reason is that TCP sender will gradually increase its throughput every RTT (Round Trip Time) without attack pulse [25], [26]. In our experiments, despite zombies are asynchronous, the interval between two consecutive attack pulses is still not long enough to provide sufficient RTTs for TCP senders to absolutely resume from congestion.

Fig. 15 depicts the throughput of bottleneck link in RED-based attack. Clearly, Compared asynchronous attack, the throughput of quasi-synchronous attack reduced 15% in our experiment.

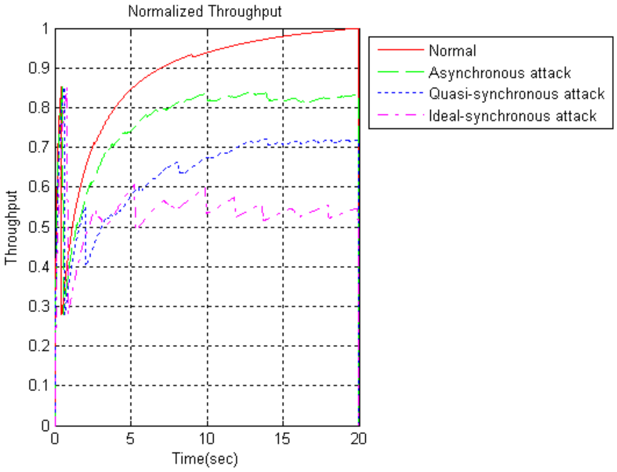


Fig. 15. Throughput in RED-based synchronous LDoS attack

As shown in Fig. 15, the performance of RED-based attack is more vulnerable to synchronization, because the attack period is smaller than the time interval of router queue recovery. The quasi-synchronous attack makes the router be over-load and under-load state alternately, and the router queue size cannot stabilize [25]. When the router is attacked, the router sends congestion signal to legitimate end system, and the legitimate end system will adjust packet sending rate according to TCP congestion control mechanism(e.g., Slow Start or Fast Recovery), which is a feedback to aggravate the oscillation of router queue, so the throughput is degraded.

V. Conclusions

In this paper, we discuss the approach based on Euclidean distance to realize aggregation or synchronization. Furthermore, according to the proposed approach, NS2 experiments are implemented. We launch aggregated and synchronous LDoS attack by adjusting the delay of each link, and compare the attack performances in two models: RTO-based attack and RED-based attack. Test results confirm that our approach is effective and simple, and the aggregated or synchronous attack is flexible from multiple end-hosts, further degrade the throughput by lower individual attack flow rate. In future work, we plan to test the approach in test bed for a deeper analysis of the aggregated or synchronous LDoS attack to better understand the behavior of such attack and propose some approaches to detect and defend against LDoS attack.

References

[1] A. Kuzmanovic and E. W. Knightly, “Low-rate TCP-targeted denial of service attacks and counter strategies,” IEEE/ACM Transactions on Networking, Aug, 2006, 14(4):683-696.

[2] A. Dainotti, F. Gargiulo, L. I. Kuncheva, A. Pescapè, C. Sansone, “Identification of Traffic Flows Hiding behind TCP Port 80,” 2010 IEEE International Conference on Communications (ICC), 2010: 1-6.

[3] V. Kumar, P. Jayalekshmy, G. Patra, R. Thangavelu, “On remote exploitation of TCP sender for low-rate flooding denial-of-service attack,” IEEE Communications Letters, Jan, 2009, 13(1): 46-48.

[4] M. Guirguis, A. Bestavros, I. Matta, “Exploiting the transients of adaptation for RoQ attacks on Internet resources,” ICNP 2004, Oct 5-8, 2004:184-195.

[5] M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, “Reduction of quality (RoQ) attacks on internet end-systems,” in Proc. 24th Annual Joint Conf. IEEE Computer and Communications Societies (INFOCOM 2005), Mar, 13-17, 2005, 2:1362-1372.

[6] M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, “Reduction of quality (RoQ) attacks on dynamic load balancers: Vulnerability assessment and design tradeoffs,” in Proc. 26th IEEE Int. Conf. Computer Communications (INFOCOM 2007), May, 6-12, 2007: 857-865.

[7] M. Guirguis, A. Bestavros, and I. Matta, “On the impact of low-rate attacks,” in Proc. IEEE Int. Conf. Communications, 2006 (ICC ’06), Jun, 2006, 5: 2316-2321.

[8] Jelena Mirkovic, Peter Reiher, “A taxonomy of DDoS attack and DDoS defense mechanisms,” ACMSIGCOMM Computer Communication Review, Apr, 2004, 34(2):39-53.

[9] G. Yang, M. Gerla, and M. Y. Sanadidi, “Defense against low-rate TCP-targeted denial-of-service attacks,” in Proc. IEEE Symp. Computers and Communications (ISCC’04), Alexandria, Egypt, Jul. 2004: 345-350.

[10] Yu. Chen and K. Hwang, “Collaborative detection and filtering of shrew DDoS attacks using spectral analysis,” Journal of Parallel and Distributed Computing, Sep, 2006, 66(9): 1137-1151.

[11] Yu. Chen, K. Hwang, and W.-S. Ku, “Collaborative detection of DDoS attacks over multiple network domains,” IEEE Trans. Parallel Distrib. Syst., Dec, 2007, 18(12): 1649-1662.

[12] A. Kuzmanovic and E. Knightly, “Low-rate TCP-targeted denial of service attacks (The shrew vs. the mice and elephants),” in Proc. ACM SIGCOMM’03, Karlsruhe, Germany, Aug, 2003: 75-86.

[13] Sarat S, Terzis A, “On the effect of router buffer sizes on low-rate denial of service attacks,” ICCCN 2005, 17-19, Oct, 2005: 281-286.

[14] Yang Xiang, Ke Li, and Wanlei Zhou. “Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics,” IEEE Transactions on Information Forensics and Security, Jun, 2011, 6(2): 426-437.

[15] G. Yang, M. Gerla, and M. Y. Sanadidi, “Defense against low-rate TCP-targeted denial-of-service attacks,” in Proc. IEEE Symp. Computers and Communications (ISCC’04), Alexandria, Egypt, Jul, 2004: 345-350.

[16] Luo X, Chang R, “A New Detection Scheme for a Class of TCP-targeted Denial-of-Service Attacks,” Network Operations and Management Symposium, April 3-7, 2006: 507-518.

[17] Sun. Haibin, J. C. S. Lui, and D. K. Y. Yau, “Distributed mechanism in detecting and defending against the low-rate TCP attack,” Computer Networks, Sep, 2006, 50(13): 2312-2330.

[18] V. Anil Kumar, P. S. Jayalekshmy, G. K. Patra, and R. P. Thangavelu, “On Remote Exploitation of TCP Sender for Low-Rate Flooding Denial-of-Service Attack,” IEEE Commun. Lett., Jan, 2009, 13(1): 46-48.

[19] G. Maciá-Fernández, J. E. Díaz-Verdejo, and P. Garcia-Teodoro, “Evaluation of a low-rate DoS attack against application servers,” Comput&Security, Dec, 2008, 27(7-8): 335-354.

[20] Y. Zhang, Z. M. Mao, and J. Wang, “Low-Rate TCP-Targeted DoS Attack Disrupts Internet Routing,”. In Proc. 14th Annual Network & Distributed System Security Symposium, 2007.

[21] Sue B Moon. “Measurement and analysis of end-to-end delay and loss in the internet,” Department of Computer Science, University of Massachusetts at Amherst, MA, February, 2000: 9-45.

[22] Shih-Yang Yang, Jiun-Ting Jiang, Po-Zung Chen. “OOPProPHET: A New Routing Method to Integrate the Delivery Predictability of ProPHET-Routing with OOP-Routing in Delay Tolerant Networks,”. Journal of Computers, Vol 8, No 7 (2013), 1656-1663, Jul 2013.

[23] O. Gurewitz, I. Cidon and M. Sidi. “One-way delay estimation using network-wide measurements,” IEEE Transactions on Information Theory, Jun, 2006, 52(6): 2710-2724.

[24] Yongsheng Li. “QoS Multicast Routing Algorithm Based on Crowding Ant Colony Algorithm,”. Journal of Computers, Vol 8, No 10 (2013), 2711-2718, Oct 2013.

[25] A. Shevtekar and N. Ansari, “A Router-Based Technique to Mitigate Reduction of Quality (RoQ) Attacks,” Computer Networks, Apr, 2008, 52(5): 957-970.

[26] A. Shevtekar, K. Anantharam, and N. Ansari, “Low rate TCP denial-of service attack detection at edge routers,” IEEE Commun. Lett., Apr, 2005, 9(4): 363-365.

[27] Changwang Zhang , Jianping Yin , Zhiping Cai , Weifeng Chen, “RRED: robust RED algorithm to counter low-rate denial-of-service attacks,” IEEE Commun. Lett., May, 2010, 14(5): 489-491.

[28] Chin-Ling Chen, Chia-Chun Yu. “Performance Evaluation of Active Queue Management Using A Hybrid Approach,”. Journal of Computers, Vol 7, No 5 (2012), 1196-1203, May 2012.

Meng Yue was born in The Hebei province, China at July, 1984. He received the M.A., degree in communication and information system from Civil Aviation University of China in 2009.

He is currently with College of Electronics & Information Engineering Civil Aviation University of China, Tianjin, China. In 2008, he studied in China Education & Research Network Engineering Center, Tsinghua University, China. His research was initially focused on information security and cloud computing, with special focus on denial of service attacks, intrusion detection, and defense.

Zhijun Wu was born in The Xinjiang Uygur Autonomous Region, China at May, 1965. He received the B.A. and M.A., degrees in electronics engineering from Xidian University, China, in 1988 and 1996 individually, and the Ph.D. degree in information security from Beijing University of Posts & Telecommunications, China, in 2004.

He is a professor in the department of Electronics & Information Engineering, Civil Aviation University of China. He is a supervisor of Ph.D candidates in the fields of Communication and Information System at Tianjin University, China, and of Information Security at Beijing University of Posts & Telecommunications, China. From 2004 to 2006, he worked as a post-doctoral in China Education & Research Network Engineering Center, Tsinghua University, China, where he was involved in several research network security projects. His research was initially focused on Information Hiding but he is currently working on computer and network security, with special focus on denial of service attacks, intrusion detection, and reliable protocol design.

Jin Lei received the M.E. degree in information security from University of Electronic Science and Technology of China, Chengdu, China. His research interests include information security.