

Cross-correlation Based Synchronization Mechanism of LDDoS Attacks

WU Zhijun, CUI Yi, YUE Meng, MA Lan, and WANG Lu

Tianjin Key laboratory for Advanced Signal Processing, Civil Aviation University of China, 300300 Tianjin, China

Email: zjwu@cauc.edu.cn, ahakong@sina.com, myue@cauc.edu.cn, mlan@cauc.edu.cn

Abstract—A success Low-rate Distributed Denial of Service (LDDoS) attack is composed of many single sources of Low-rate Denial of Service (LDoS) attacks, which are well-organized in time synchronization to aggregate the attack flow at the end of target router. This paper addresses time synchronization and flow aggregation in LDDoS attacks for the purpose of exploring the attack performance. A cross-correlation algorithm is proposed to guarantee all network-wide distributed attack pulses aggregate at the victim end with a strict time limitation to form a powerful attack pulse. Experiments on the attack performance of LDoS and LDDoS attack are performed in NS-2 simulation platform. Experiment results show that the LDDoS attack effects can be improved significantly by using cross-correlation algorithm to coordinate attack pulses, which obtain better attack performance than many single dependent attack pulses.

Index Terms—LDoS; Low-rate Distributed Denial of Service (LDDoS); Cross-Correlation; Time Synchronization; Flow Aggregation

I. INTRODUCTION

The Denial of service (DoS) attack is an unsolved tough problem in internet for many years. This problem became more serious due to appearance of many variant DoS attacks, which can be divided into two types of attack, which are defined as Flood [1] and Shrew [2]. The Flood DoS attacks send large volume of traffic to throttle the victim, while the Shrew attacks dispatch relative low rate of flows to degrade the target service performance. Hence, the Shrew attack is one kind of low-rate DoS (LDoS) attack [2], which is a interested topic that studied by many researchers world widely.

Present, there is two definitions of low-rate DoS attacks.

A. The First Definition

The first one is shrew attack. This kind of low-rate DoS attack was first found in 2001 and reported by

Aleksandar Kuzmanovic [3] on Sigcomm conference in 2003. This kind of low-rate DoS attacks launch a sequence of cycle pulse with a certain period, width, and amplitude to victim and degrade the quality of service (QoS) at the end of victim without being conscious. This kind of low rate DoS attack is a new type DoS attack.

A low-rate DoS attack with single source is modeled by a square waveform with an attack period of $RTO_{min} + 2RTT$, burst length of L , and the burst rate of R , as shown in Fig. 1.

The model of low rate DoS attacks is a set of three elements $\{R, L, T\}$, in which R is the rate, large enough to induce loss (i.e., R aggregated with existing traffic must exceed the link capacity), L is the duration of scale round trip time (RTT) (long enough to induce timeout but short enough to avoid detection), and T is the period of scale RTO (chosen such that when flows attempt to exit timeout, they are faced with another loss).

Low-rate DDoS has a relatively low data rate to elude being detected. The behavior of low-rate DDoS attack likes a shrew can defeat elephant. Hence, low-rate DDoS attack is called Shrew [3] in early. Because the wave of low-rate DDoS attack is a series square pulses, therefore, someone call low-rate DDoS attack as Pulse DoS (PDoS) attack [4]. The purpose of low-rate DDoS attack is not to tear down the target, but to degrade the quality of service (QoS). So, low-rate DDoS attack has another name of Degrading QoS attack [5].

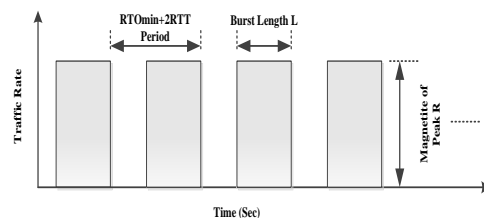


Figure 1. Model of LDoS attack traffic

B. The Second Definition

The second one is actually a Flood type DDoS attack that reported by D. Moore et al. [6] and Yang Xiang [7]. They analyzed the DDoS attacks that contained in CAIDA [8] data set, results show that more than 10000 attack packets per second can achieve a high-rate attack, and 1000 attack packets per second around can only achieve 60% of full attack. Therefore, this is a low-rate

Manuscript received June 17, 2013; revised December 2, 2013; accepted December 17, 2013.

Part of this paper was first appeared in "Research on Time Synchronization and Flow Aggregation in LDDoS Attack Based on Cross-correlation", which is published on the proceedings of The 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2012) that hold in Liverpool, England, UK, 25-27 June 2012.

Corresponding author: Wu Zhijun Email: zjwu@cauc.edu.cn.

DDoS attack. So, they believe that the DDoS attack with a data rate of more than 10,000 attack packets per second is defined as a high-rate DDoS attack, and the DDoS attack with a data rate of 1,000 attack packets per second around is considered as a low-rate DoS attack. Therefore, the MIT Lincoln Laboratory Scenario (attack-free) inside tcpdump dataset was used as the normal network traffic, and the low-rate DDoS attack scenario from CAIDA was used as the DDoS attack traffic for experiments in the publication [7].

Therefore, the two kind of low-rate DoS attack are totally different. Our paper is focus on the first kind of low rate DoS, which is shorten in LDoS, belongs to the shrew attack. It exploits the deficiencies of the minimum RTO of TCP to send out attack packets in short-duration periodic pulses with low average volume traffic in order to throttle TCP throughput.

Low-rate Distributed DoS (LDDoS) attacks are composed of a number of LDoS attacks, i.e., a cluster of LDoS attacks. An LDDoS attack has significant ability of concealing its traffic because it is like normal traffic extremely. It has the capacity to elude the current anomaly-based detection schemes. The bigger pulse of an LDDoS attack is formed by a few smaller pulses that are sent by many well-organized LDoS attackers. The total attack energy in bigger attack pulse is evenly distributed to each smaller pulse, resulting in decline in the average attack traffic. Therefore, the smaller pulse can be hidden in the normal traffic, i.e., hidden in the attack path. All distributed smaller attack pulses are aggregated at a determined position through different transmission paths within a precise time to generate LDDoS attack pulses [2]. Namely all LDoS attackers working together and forming the time-synchronized and flow-aggregated LDDoS attack, to form an even more devastating attack. Therefore, the mechanism of time synchronization and flow aggregation for LDDoS attacks is useful for defending against LDDoS attacks.

II. RELATED WORKS

There are two methods of organizing LDoS attacks to form LDDoS attacks. In the first method, all the widely distributed LDoS attackers from different domains, they start to launch the attack packets to the victim at the appointed time, and the attack will last for a certain period. This method does not need coordination; all it needs is a range of time [9]. While in the second method, LDDoS is defined strictly by its narrow meaning. This method needs all widely distributed LDoS attacks from different domains well-organized in time synchronization and flow aggregation. It means that all the attack packets from different attackers reach the victim with a strict time limitation for the purpose of enhancing the attack power. This paper focuses on the second situation [10].

Like DDoS attacks, time synchronization and flow aggregation in LDDoS attacks are used to maximize the attack damage. Ying Zhang [11] uses ICMP or IP timestamp request to get the delay variability of the network path between attackers and target link, then the delay can be used to coordinate the attack starting time to

make minimal effect on synchronization. There are some problems in this method. Firstly, it's hard to coordinate the attack pulse since the value of RTT is dynamic. Secondly, RTT can not reflect the shape distinctness among attack pulses. Finally, the shape of attack flows may be distorted during transmission. Even if RTT is exact, it's hard to ensure the pulse peak is superimposed [12] [13]. John C.S. Lui [14] studied the difference between LDoS attack traffic with different period, and how to remain the attack traffic same as the original at the victim router.

In this paper, a cross-correlation approach is proposed to evaluate the result of attack flow superimposition based on the final shape of attack flows.

III. LDDoS ATTACK MODEL

In LDDoS attacks, attacks pulses are split into several ones with much smaller amplitude. These small pulses are sent by different attackers and aggregated at the target end. The attack pulses can be generated through following methods of splitting big pulses.

A. Pulse Peak Multiplicatively Decrease, Attack Period is Unchanged

Even if pulse peaks multiplicatively decreased, the attack period is not changed, as shown in Fig. 2. Supposing that the throughput capacity of the attack target is C , Attackers, named 1 to n , implement LDDoS with an attack period of T and an attack peak of C/n , and each attack pulse can be superimposed at the victim end to form a high rate attack flow with peak C [14] [15].

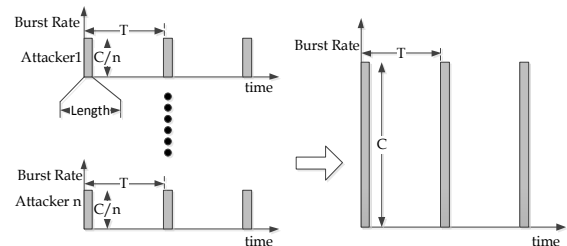


Figure 2. Pulse peak multiplicatively decrease, attack period is unchanged

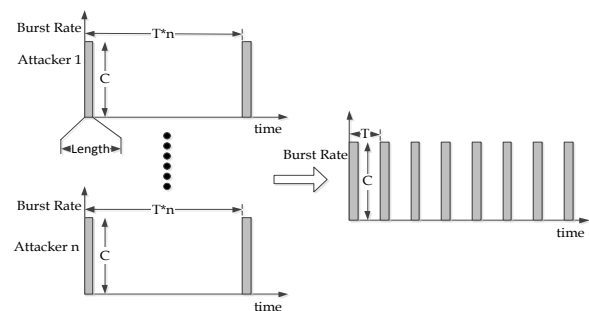


Figure 3. Pulse peak is unchanged, attack period multiplicatively increase

In the case of multiplicatively decreased attack peak, each attack pulse has a good aggregation to form an attack pulse which has enough energy to congest the bottleneck link. Conversely, if the aggregated effect is not ideal, the attack intensity is too small to congest the

bottleneck link effectively. Thus, this form of LDDoS has a highlight requirement for aggregation. Because the single attack pulse intensity is weak and the attack characteristic is not obvious, it's harder to be detected by available counter-DoS mechanism.

B. Attack Period Multiplicatively Increase, Pulse Peak is Unchanged

Pulse peaks are unchanged, but attack cycles multiplicatively are increased, as shown in Fig. 3.

The n attackers are used to implement LDDoS with an attack period $n*T$ and attack peak C . Each attack pulse can be superimposed at the victim end to form a high rate attack flow with period T [14] [15].

In the case of multiplicatively increased attack period, the signal attack pulse is high enough to congest the bottleneck link. TCP flows will enter the unstable state even if the aggregated effect is not ideal, and the entire network throughput is affected. However, due to the longer period of signal attack pulses, TCP flows could not be ensured to enter the unstable state continuously if the aggregation of the flows is not ideal. When the interval between the previous attack pulse and the latter is long enough, the victim has the opportunity to recover and enter the stable state. This form of LDDoS has few aggregated requirements. It lengthens the attack period, but the attack pulse intensity is obvious, thereby it is easily detected relatively.

As the Fig. 2 and Fig. 3 show, each attack pulse must comply with certain time series strictly in order to aggregate an ideal LDDoS attack. However, each attacker may distribute in different networks, and the distance between attacker and the attack target is uncertain. Thus, ensuring each attack pulse to be aggregated to form a stronger attack pulse after transmission through different networks has become a difficult technique. If all the single attack pulses cannot be synchronized and aggregated, LDDoS attack will lose its attack characteristics, and attack effect will be degraded seriously.

Fig. 2 and Fig. 3 show that the time synchronization and flow aggregation of LDDoS attack needs a strict timing relationship between all the pulses participated in the attack, i.e. every pulse is closely related to others. Hence, cross-correlation function is used as the solution technique to realize the time synchronization and flow aggregation in this paper. Cross correlation is a standard method of estimating the degree to which two series are correlated [16] [17] [18].

IV. CROSS-CORRELATION ALGORITHM IN LDDoS

A low-rate TCP attack is essentially a periodic burst which exploits the homogeneity of the minimum retransmission timeout (RTO) of TCP flows. Consider a router with capacity C (in bits/s). One form of attack is a periodic square wave as described in [2] [3]. The period of the square wave is denoted by T , which is approximately one second so as to force other TCP flows to enter the retransmission state effectively. Within each period, the square wave has a magnitude of zero except

for l units of time ($l \geq \max\{RTT_i\}$). During this time, the square wave has a magnitude of a normalized burst of R . The average bandwidth of this periodic square wave is Rl/T . Again, the objective of the low-rate attack is that for a short duration l , the attack packets will fill up the buffer of a victim router so it result that packets of any TCP flows are discarded by the router. The packet loss will force, if not all, most TCP flows to enter the retransmission state. And we note that it is considered to be a low-rate TCP attack, whose ratio of has to be small. Otherwise, system administrators can easily detect an attack by its high traffic volume.

The time synchronization and flow aggregation of LDDoS attack is shown in Fig.4.

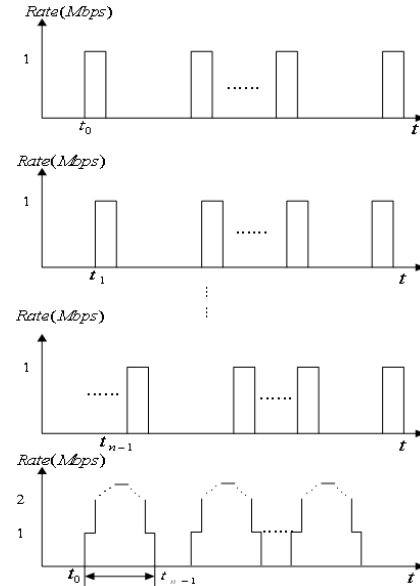


Figure 4. Time synchronization and flow aggregation in LDDoS

In Fig.4, t_0, \dots, t_{n-1} denote the every point of n attack flows arriving at victim. We define the metrics $\Delta\tau = t_{n-1} - t_0$ as the performance of synchronization. Normally, the last time l is about of the order of 100ms, and if $\Delta\tau$ is relatively big for l , it will extend the l and weaken the power of attack aggregation, unlike FDDoS affecting the beginning, it will affect the LDDoS attack all the time.

Consider two LDoS attack series $x(i)$ and $y(i)$, where $i = 0, 1, 2, \dots, N-1$. The cross correlation r between two LDoS attacks series at delay d is defined as [16] [17] [18].

$$r = \frac{\sum_i [(x(i) - m_x) * (y(i-d) - m_y)]}{\sqrt{\sum_i (x(i) - m_x)^2} \sqrt{\sum_i (y(i-d) - m_y)^2}} \quad (1)$$

where, m_x and m_y are the means of the corresponding LDoS attack series. If the cross correlation r above is computed for all delays $d=0, 1, 2, \dots, N-1$, i.e. all the LDoS attack series, the total number is N , participate in the operation of cross correlation, then it results in a cross correlation series of twice the length as the original series.

$$r(d) = \frac{\sum_i [(x(i) - m_x) * (y(i-d) - m_y)]}{\sqrt{\sum_i (x(i) - m_x)^2} \sqrt{\sum_i (y(i-d) - m_y)^2}} \quad (2)$$

Considering the equations (2), when the $y(i)$ series is being slid past the $x(i)$, at each shift the sum of the product of the newly lined up terms in the series is computed.

An LDoS attack from current domain relative to the LDoS attacks from other domain in arrival time with a certain time delay (lead or lag), the cross correlation at each delay is calculated to obtain the maximum correlation at a delay of d , then, one of the two related LDoS attack is shifted the time of d for the purpose of achieving time synchronization and flow aggregation in LDDoS attack.

For convenience, in the following calculations, m_x and m_y are set to zero.

The biggest impact on time synchronization and flow aggregation is that all LDoS attackers are widely distributed in different domains. Each attack pulse cannot reach the attack target at same time after the network transmission due to the networks delay, as shown in Fig. 1 or Fig. 2. Thus, attack pulse can not be effectively aggregated. The cross-correlation algorithm can be applied for estimating the delay between two LDoS attack series.

The paper defines the number of packet that reaches the router as discrete signal sequence, and samples each attack pulse respectively at the victim. Based on one of the attack pulses, the correlation degree of different pulses can be calculated using cross-correlation function. The delay of different signals can also be confirmed. According to the delay, the start time of each attack pulse is adjusted by computing the cross-correlation to aggregate an ideal LDDoS attack flow to the victim.

In the case of multiplicatively decreased pulse peaks, attack pulses are sampled at the victim end, and one of the sample signals is chosen as a baseline. The delay between the baseline and others, denoted as d_1, d_2, \dots, d_{n-1} , can be calculated. Here, n represents the number of attackers. According to the delay, each attacker can be controlled to launch attack pulse at appointed time. Moreover, to minimize the aggregated error, the delay is calculated dynamically by using cross-correlation function, and the calculation will be performed continuously until the aggregated error is small enough.

In the case of multiplicatively increased attack period, the delay between the baseline and others are denoted as $d'_1, d'_2, \dots, d'_{n-1}$, and n represents the number of attackers. Assume the period of the baseline attack pulse is T , other attack pulses can be controlled to start at $T - d'_1, 2T - d'_2, \dots, (n-1)T - d'_{n-1}$ one by one. The start time is adjusted continuously until delay sequence approaches $T, 2T, \dots, (n-1)T$ [19].

The time synchronization and flow aggregation of LDDoS attack can be achieved through the above steps.

V. SIMULATING EXPERIMENTS AND RESULTS ANALYSIS

In this section, the effect of attack by simulation experiment is analyzed and the validity of cross-correlation algorithm used in synchronization and aggregation of LDDoS attack is verified.

A. Experiment Environment

In this paper, the MIT Lincoln Laboratory Scenario (attack-free) inside tcpdump dataset was used as the normal network traffic, and the low-rate DDoS attack scenario from CAIDA was used as the DDoS attack traffic for experiments. Some improvements are made by putting into the information attack period T and attack pulse width L into the CAIDA's data to meet the requirement of LDoS attack.

The experiment environment is based on NS2 platform, and the network topology is shown in Fig. 5.

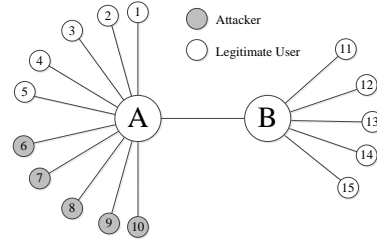


Figure 5. The experiment environment

Fig. 5 shows two routers (node A, node B), five legitimate TCP senders (node 1-node 5), five TCP receivers (node 11-node 15), and five UDP LDDoS attack sources (node 6-node 10). The bottleneck bandwidth between node A and node B is 10Mbps, other links are 100Mbps. Detailed parameters are shown in table 1.

TABLE I. EXPERIMENT PARAMETERS

| | RTT(ms) | Bandwidth(Mb) |
|----------------|---------|---------------|
| Node 1 to A | 10 | 100 |
| Node 2 to A | 50 | 100 |
| Node 3 to A | 100 | 100 |
| Node 4 to A | 150 | 100 |
| Node 5 to A | 200 | 100 |
| Node 6-10 to A | 5 | 100 |
| Node A to B | 50 | 20 |
| Node B to 11 | 10 | 100 |
| Node B to 12 | 50 | 100 |
| Node B to 13 | 100 | 100 |
| Node B to 14 | 150 | 100 |
| Node B to 15 | 200 | 100 |

The LDDoS attack parameters: attack periods $T = 1000\text{ms}$, pulse length $E = 250\text{ms}$, pulse peak $S = 20\text{Mbps}$. In the pulse peak multiplicatively decreased condition, the parameters can be set as: $T = 1000\text{ms}$, $E = 250\text{ms}$, $S = 20\text{Mbps}/5 = 4\text{Mbps}$ [20].

In the attack period multiplicatively increased condition, the parameters can be set as: $T = 1000\text{ms} * 5 = 5000\text{ms}$, $E = 250\text{ms}$, $S = 20\text{Mbps}$. Meanwhile, we sample data flows between node A and node B, then calculate the number of attack packages every 10ms, the number of receiving packages in every second is used to describe attack burst [20].

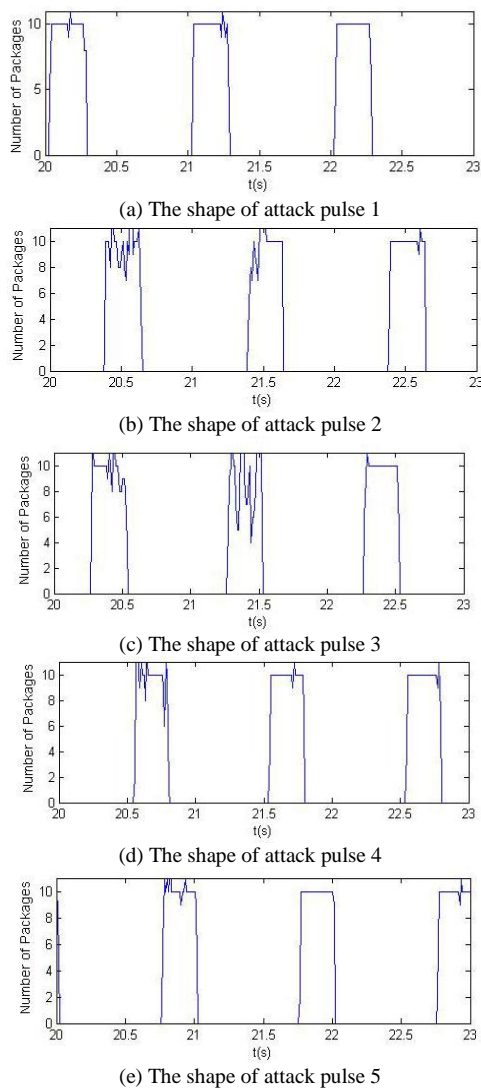


Figure 6. The shape of each attack pulse

The legitimate users will send normal TCP packages until the net flow is stable, and at the 10th second, attackers start to send attack flows, the experiment lasted for 80s.

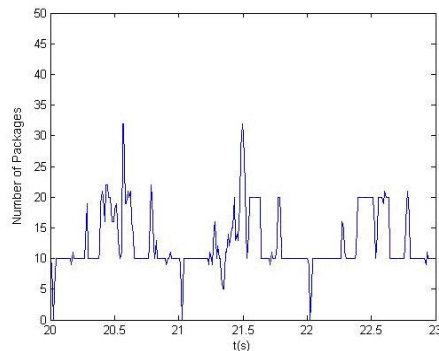


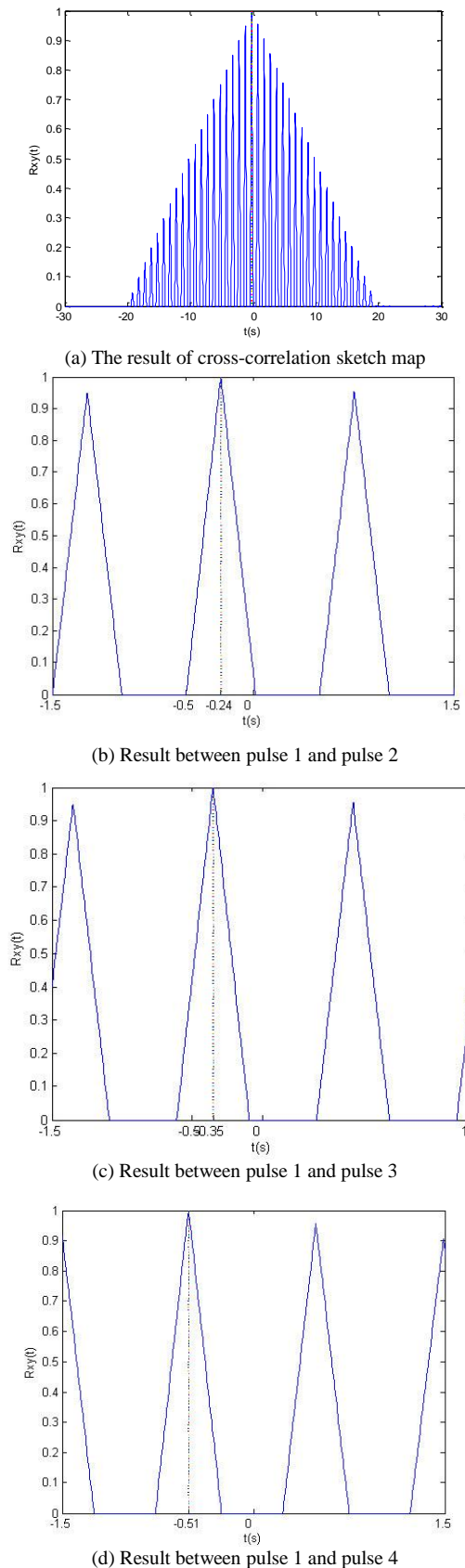
Figure 7. The aggregated pulse when attack pulses are asynchronous

B. Experiments and Results Analysis

Two kinds of experiments have been performed as follows.

a) In the case of multiplicatively decreased attack period, each attack pulse is asynchronous by setting

different delay between attack nodes and router A. The asynchronism may affect the final effect of pulse aggregation. The attack pulse during 20s to 23s is shown in Fig. 6.



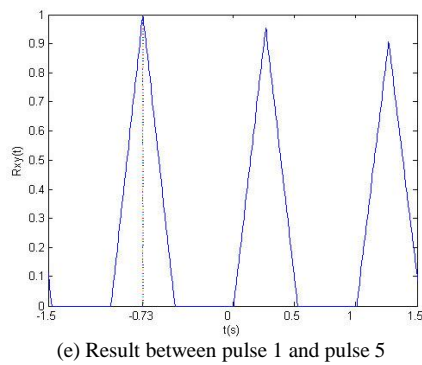


Figure 8. The result of cross-correlation

Because of the difference of phases, the aggregated pulse shape is not ideal, as shown in Fig. 7.

The pulse of attacker 1 is chosen as a baseline and the delay between the baseline and other four attack pulses are calculated by using cross-correlation algorithm. The normalized result is shown in Fig. 8.

The comparison of different delay values for each node and cross correlation value are shown in table 2.

TABLE II. SET DELAY VALUE AND CROSS-CORRELATION VALUE

| | Delay | Cross-correlation value |
|---------------------|-------|-------------------------|
| Pulse 1 and Pulse 2 | 300ms | 240ms |
| Pulse 1 and Pulse 3 | 370ms | 350ms |
| Pulse 1 and Pulse 4 | 690ms | 510ms |
| Pulse 1 and Pulse 5 | 730ms | 730ms |

The delay calculated by cross-correlation algorithm will be used to adjust the start time of every attack pulse, namely, attacker 2 begins attack at 240ms in advance, attacker 3 begins attack 350ms in advance, and attacker 4-5 begin attack at 510ms and 730ms in advance, accordingly. The aggregated attack pulse after adjustment is shown in Fig. 9.

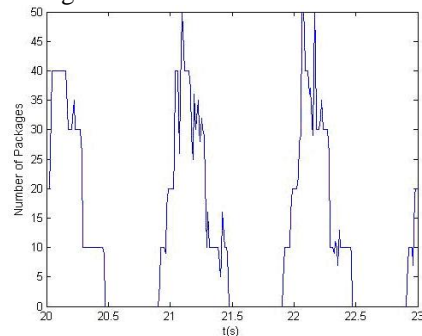


Figure 9. The aggregated pulse after adjustment

Fig. 9 shows period is clearer and its peak is sharper, which is more centralized compared with the attack pulse in Fig. 7. It is clear that the degree of flow aggregation is enhanced after the sending time of attack is adjusted by cross-correlation value.

The result shows that the aggregated pulse is improved after adjustment, although the effect of aggregation is not the best. The throughput of the bottleneck link is shown in Fig. 10.

It can be concluded from Fig. 10 that the attack result after adjust is enhanced, and it is close to the best attack performance of flow aggregation after adjustment.

The delay of each attacker is measured when data are collected after adjustment, and the results are shown in table 3.

For the purpose of enhancing attack pulse, when a time benchmark is selected, the start time of attack pulse has been adjusted to shift a delay time according to the result of cross-correlation, and the superimposition of attack pulse has been completed. If the position of pulse 1 is determined as the baseline, the time shift of pulse 2, pulse 3, and pulse 4 have the delay of 60ms, 10ms, 200ms, and 5ms individually.

b) In the case of multiplicatively increased attack period, Fig. 11 shows the cross-correlation value between the baseline pulse and other four pulses. The delay of between pulse 1 and other pulses are as follows.

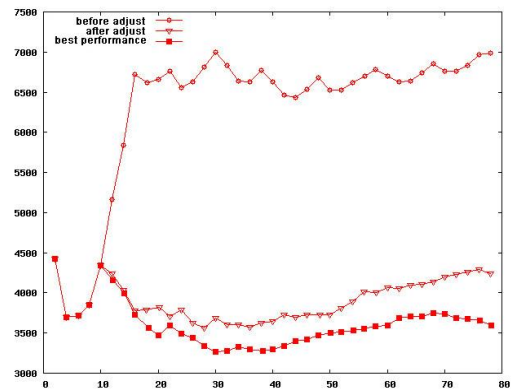


Figure 10. Attack performance before and after adjust

TABLE III. THE DELAY AFTER ADJUSTMENT

| | The delay after adjustment |
|---------------------|----------------------------|
| Pulse 1 and Pulse 2 | 60ms |
| Pulse 1 and Pulse 3 | 10ms |
| Pulse 1 and Pulse 4 | 200ms |
| Pulse 1 and Pulse 5 | 5ms |

(i) pulse 1 and pulse 2 is 0.3900.

(ii) pulse 1 and pulse 3 is 0.5200.

(iii) pulse 1 and pulse 4 is 1.5900.

(iv) pulse 1 and pulse 5 is 4.8500.

The set delay and the cross-correlation value are described correspondingly in table 4.

TABLE IV. SET DELAY VALUE AND CROSS-CORRELATION VALUE

| | Delay | Cross-correlation value |
|---------------------|--------|-------------------------|
| Pulse 1 and Pulse 2 | 300ms | 390ms |
| Pulse 1 and Pulse 3 | 700ms | 520ms |
| Pulse 1 and Pulse 4 | 1690ms | 1590ms |
| Pulse 1 and Pulse 5 | 4730ms | 4850ms |

According to the delay value calculated by cross-correlation algorithm, the attack pulses are adjusted respectively as follows.

(i) attacker 2 delays its start time is 1000ms - 390 ms = 610ms.

(ii) attacker 3 delays its start time is 2000ms - 520ms = 1480ms.

(iii) attacker 4 delays its start time is 3000ms - 1590ms = 1410 ms.

(iv) attacker 5 delays its start time is 4000ms - 4850ms = -850ms.

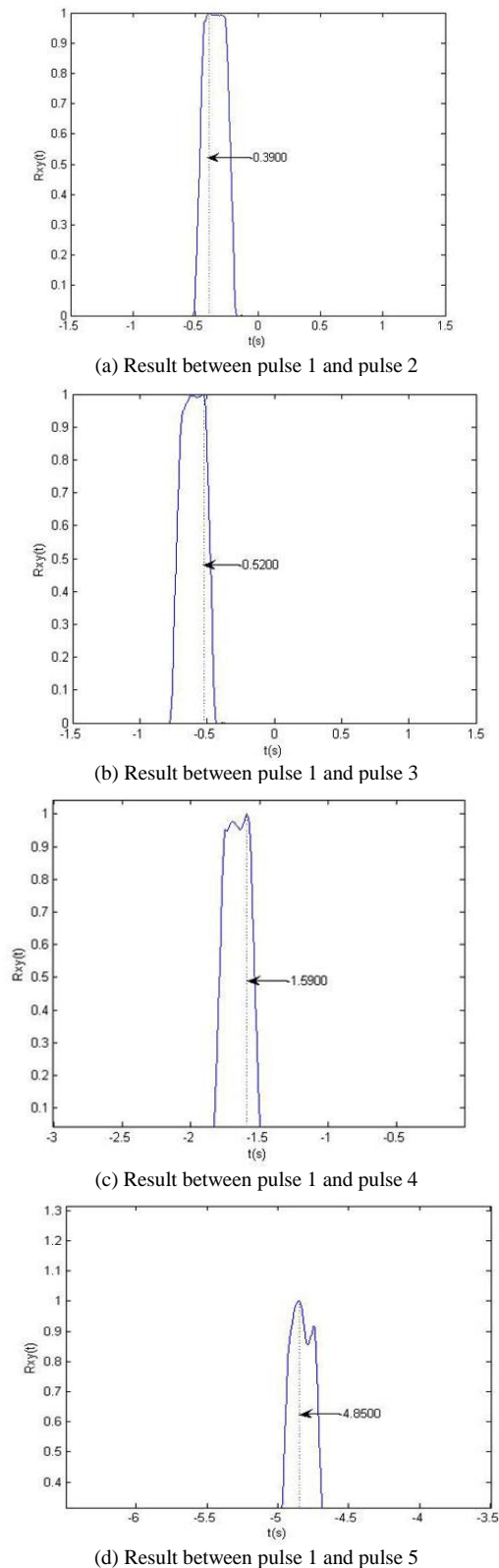


Figure 11. The result of cross-correlation

Fig. 12 shows that the aggregated attack pulse before adjustment is indistinct in its period although its peak is obvious. Since the adjustment, the aggregated attack pulse can not only keep the value of peak, but also enhance the periodicity of pulse. It's clear that the period is about 1s.

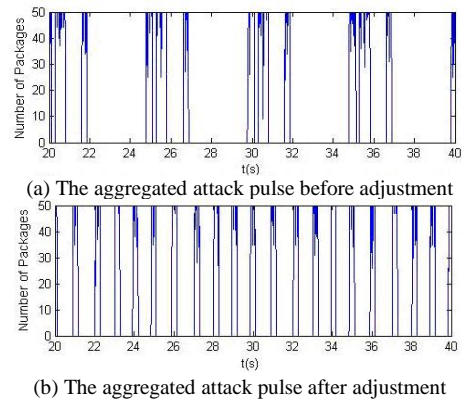


Figure 12. The aggregated pulse before and after adjustment

Equally, the adjusted aggregated attack performance is closer to the best attack performance, as shown in Fig. 13.

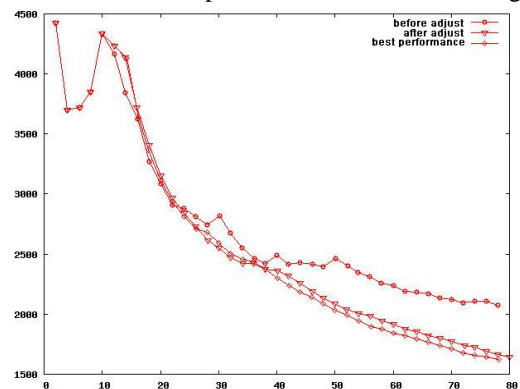


Figure 13. Attack performances before and after adjustment

More experiment results are shown in table 5.

TABLE V. THE PERFORMANCE OF CROSS-CORRELATION USED IN DIFFERENT FORM OF LDDoS

| Peak decrease, Cycle unchanged | | Peak unchanged, Cycle multiplicative increase | |
|---------------------------------|--------------------------------|---|--------------------------------|
| Throughput (kbps) Before adjust | Throughput (kbps) After adjust | Throughput (kbps) Before adjust | Throughput (kbps) After adjust |
| 4496 | 4224 | 1605 | 1482 |
| 4993 | 4036 | 1673 | 1589 |
| 5292 | 4030 | 2120 | 1497 |
| 5237 | 4082 | 1428 | 1477 |
| 7098 | 4325 | 2819 | 2078 |
| 5053 | 4414 | 2595 | 1629 |
| 4881 | 4098 | 1464 | 1580 |
| 4590 | 4023 | 1917 | 1878 |
| 4834 | 4030 | 2279 | 1555 |
| 4420 | 4293 | 1993 | 2238 |

According to the experiment results above, the delay of each attack pulse is calculated by cross-correlation algorithm, and then the degree of synchronization and aggregation of the attack flows are improved by adjusting the sending time of each attack pulse, thereby the attack performance improved.

Compared the proposed approach with the RTT-based method [11] [14], result shows that the proposed approach needs less computation time and resource spent on calculation of IP timestamp, the good performance on time accuracy is obtained.

VI. CONCLUSION

Time synchronization and flow aggregation are two critical aspects for successful LDDoS attacks. In this paper, a cross-relation algorithm is proposed to realize the time synchronization and flow aggregation in LDDoS attack. The experimental results show that this algorithm works effectively and stably. This proposed algorithm can improve (or match the various requirements of) the LDDoS attack effectiveness by effectively adjusting the value of time delay. As the proposed algorithm can increase the time correlation between two LDDoS attack traffic, it can effectively increase the attack performance.

This research tries to explore the generation mechanism of LDDoS attack. It will be helpful to detect and defense against LDDoS attack in future research.

ACKNOWLEDGMENT

This work is financially supported by the China National Science Foundation (No. 61170328 and U1333116), Tianjin Natural Science Foundation (No. 12JCZDJC20900), and the Fundamental Research Funds for the Central Universities of CAUC under grant 31122013P007, 3122013D007, and 3122013D003.

REFERENCES

- [1] Yogesh Chaba, Yudhvir Singh, and Preeti Aneja. Performance Analysis of Disable IP Broadcast Technique for Prevention of Flooding-Based DDoS Attack in MANET. *Journal of Networks*, Vol. 4, No. 3, pp. 178–183, May 2009.
- [2] Aleksandar Kuzmanovic and Edward W. Knightly. Low-Rate TCP-Targeted Denial of Service Attacks and Counter Strategies. *IEEE/ACM Transactions on Networking*, Vol. 14, No. 4, August, 2006, 14(4), pp. 683–696.
- [3] Kuzmanovic A, Knightly E W.. Low-rate TCP-targeted denial of service attacks. *Proceedings of ACM SIGCOMM 2003, Karlsruhe, Germany*, 2003, pp. 75–86.
- [4] Luo X P, Rocky K, Chang C. On a new class of pulsing denial-of-service attacks and the defense. *Network and Distributed System Security Symposium (NDSS'05)*, San Diego, CA, USA, 2005.
- [5] Guirguis M, Bestavros A, Matta I. Bandwidth stealing via link targeted RoQ attacks. *Proc 2nd IASTED International Conference on Communication and Computer Networks*, Cambridge, MA, 2004.
- [6] D. Moore et al., Inferring Internet denial-of-service activity, *ACM Transactions. Computer. System.*, vol. 24, no. 2, pp. 115–139, 2006.
- [7] 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*, Vol. 6, No. 2, June 2011, pp. 426–437.
- [8] CAIDA, 2010 [Online]. Available: <http://data.caida.org/datasets/security/ddos-20070804/>
- [9] Kumar, V., Jayalekshmy, P., Patra, G., Thangavelu, R., On remote exploitation of TCP sender for low-rate flooding denial-of-service attack, *IEEE Communications Letters*; 2009, 13(1) pp. 46–48.
- [10] Efstathopoulos, P., Practical study of a defense against low-rate TCP-targeted DoS attack; 2009. *ICITST 2009. International Conference for Internet Technology and Secured Transactions*, 2009 pp. 1–6.
- [11] Y. Zhang, Z. M. Mao and Jia Wang, Low-Rate TCP-Targeted DoS Attack Disrupts Internet Routing, *In Proc. 14th Annual Network & Distributed System Security Symposium*, 2007 pp. 1–15.
- [12] Zenghui Liu, Liguang Guan, Attack Simulation and Signature Extraction of Low-Rate DoS; *2010 Third International Symposium on Intelligent Information Technology and Security Informatics (IITSI)*, 2010 pp. 544–548.
- [13] Xiaodong Xu, Xiao Guo, Shirui Zhu; A queuing analysis for low-rate DoS attacks against application servers; *2010 IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS)*, 2010 pp. 500–504.
- [14] John C. S. Lui, Defending against Low-rate TCP Attack: Dynamic Detection and Protection, Presentation, CSE Dept. CUHK.
- [15] M. Guirguis, A. Bestavros, and I. Matta, Bandwidth Stealing via Link-targeted RoQ Attacks, *Proceedings on Communication and Computer Networks (CCN 2004)*, November 8–10, 2004, Cambridge, MA, USA, PP. 438–427
- [16] Yanxia Wang, Yan Ma, Qixin Chen. A Method of Line Matching Based on Feature Points. *Journal of Software*, Vol. 7, No. 7, pp. 1539 – 1545, July 2012.
- [17] Zhi-jun Wu, Minghua Wang, Haitao Zhang, Xingchen Liu. Correlation-based Detection of LDDoS Attack. *Journal of Networks*, Vol. 7, No. 10, pp. 2341 – 2348, October 2012.
- [18] T. Hayashi, A Class of Zero-Correlation Zone Sequence Set Using a Perfect Sequence, *IEEE Signal Processing Letters*, 2009, 16(4), pp. pp. 331–334
- [19] Changwang Zhang, Jianping Yin, Zhiping Cai, and Weifeng Chen, RRED: robust RED algorithm to counter low-rate denial-of-service attacks; *IEEE Communications Letters*, 2010, 14(5) pp. 489–491.
- [20] G. Macia-Fernandez, J. E. Diaz-Verdejo, and P. Garcia-Teodoro, Mathematical Model for Low-Rate DoS Attacks Against Application Servers, *IEEE Transactions on Information Forensics and Security*; 2009, 4(3) pp. 519–529.

Zhijun Wu, was born in Xinjiang Province, China, at May 1965. He received B.S and Master degree in Signal Processing from Xidian University, Xian City, China, in 1988 and 1993 individually, and Ph.D in Cryptography from Beijing University of Posts & Telecommunications, Beijing City, China, in 2004.

He is Professor in Civil Aviation University of China (CAUC). His main research field is network and information security.

Yi Cui was born in Fujian Province, China, in 1988. He is a graduated student in Civil Aviation University of China. His interesting area is network security.

Meng Yue was born in Hebei Province, China, in 1983. He is a Lecturer in Civil Aviation University of China. His interesting area is network security.

Lan Ma was born in Xinjiang Province, China, in 1966. She is an associate professor in Civil Aviation University of China. Her research area is intelligent system and control.

Lu Wang was born in Henan Province, China, in 1986. He is a graduated student in Civil Aviation University of China. His interesting area is network security.