Transactions on Machine Intelligence 2(1) (2019) 20–32

ISSN Online: 2821-1693

Transactions on Machine Intelligence

Journal Homepage: https://tmachineintelligence.ir/index.php/TMI

TCP Low Rate DDoS Attack Detection

M. R. Razian[1,*]

[1] Iran University of Science and Technology, Tehran, Iran

ARTICLE INFO

Article History:
Received 25 November 2018
Received in revised form
15 February 2019
Accepted 11 March 2019
Available online 13 March 2019

Keywords:
Network Security,
TCP Low rate attack,
DDoS,
Encountering, TCP

ABSTRACT

Undoubtedly one of the more significant attacks on computer networks is distributed denial of service (DDoS). DDoS assaults can be divided into two groups: high-rate attacks and low-rate attacks. In the high-rate DDoS category, the attacker tries to use all of the bandwidth available on the channel by saturating it with packets. While maintaining a low average transmission rate, the attacker conducts a DDoS attack in the low-rate DDoS category (also known as LDDoS). TCP LDDoS is a low-rate DDoS assault in which the attacker takes advantage of the way TCP handles congestion. In this article, we look into a system for stopping a TCP LDDoS attack and suggest a fresh approach. We offer several observations to help distinguish between appropriate behavior and an attack. Our system produces a priority queue of flows, where flows with a high priority are valid and flows with a low priority are suspect. Using the NS2 simulation environment, we assess the suggested system. Results demonstrate that our suggested approach can accurately distinguish between attack flows and genuine flows.

1. INTRODUCTION

Today, many advances have been made in the frontiers of knowledge [1,2]. An intense attack on computer networks is the distributed denial of service (DDoS) attack. Reports shows that DDoS attack is one of the serious attacks in recent years. For launching DDoS attack, attacker uses (or misuses) behavior of existing protocols in different layers of TCP/IP network model. In aspect of rate of average packet sending ratio, DDoS attacks are known in two categories: high rate DDoS and low rate. In high rate DDoS, attacker sends packets high rate in order to filling up bandwidth capacity of legitimate users. In low rate DDoS attack, attacker launch his/her attack so that send his packets low sending average rate but with special pattern. In former, sending packet is one of good evidences of occurring DDoS attack for encountering system. In later because of low average rate, traditional systems can't defend against it. TCP low rate attack is one of the low rate DD0S attacks which exploit the behavior of Transmission Control Protocol (TCP) to launch DDoS attack [3]. Fig. 1 shows a low rate dos flow. A flow is defined by a 5-tuple (Source IP, Source Port, Destination IP, Destination Port, and Protocol) or 4-tuple (Source IP, Source Port, Destination IP, and Destination Port).

* Corresponding Author: razian.mr@gmail.com
Iran University of Science and Technology, Tehran, Iran

http://dx.doi.org/10.47176/TMI.2019.20

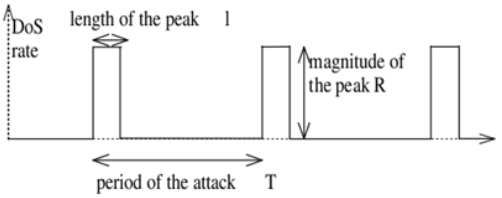


Fig. 1. Low rate dos flow

Different encountering methods have presented in recent years but each one of them has drawbacks so that attacker can launch attack. In this paper we present an approach for defending against LDDoS attack. Our approach is based on LDDoS attack behavior and not based on its pattern. Consider that attacker for launching an intensive attack, need to provide his flows in special time in order to occupy link capacity and cause TCP flows time out. Besides, attacker shouldn't provide his flows in reminder of times, because of average rate of sending packets should be low. This fundamental characteristic builds our approach to encountering against LDDoS attack.

In this paper we present a novel encountering system to identify LDDoS flows. We analyze each input flows to router and find their similarity to the fundamental characteristic of LDDoS attack flows. We present three key observations as fundamental characteristics of LDDoS attack flows:

- TCP flows drastically were been defected
- when loss rate is increasing most of flows outgoing to output link are attack flows
- when loss rate is decreasing most of flows outgoing to output link are benign flows

To the observation, we calculate similarity value of flows to LDDoS attack flows. Each one of this observation can has itself weight in their aggregation. After identifying attack flows, now you can filter then ore apply your desire policy. Now we sort aggregated values: High priority flows are legitimate flow and we can service them more. Low priority flows are suspected to attack flows where we can apply our punishment policies to them.

We evaluate the proposed system employing the NS2 simulation environment. We consider different scenario and challenging condition to evaluate our method. The experiment results show that proposed method is effective for detecting LDDoS attack flows. In following our contributions are listed:

- We extract some criteria and compare different defending system for LDDoS
- We present a novel approach for eliminating weakness in approach of other defense system
- We propose a novel method for detecting LDDoS attacker

Two main advantages of our proposed method are:

- Identifying non feedback based flows such as UDP flows
- Identifying attack flows which haven't deterministic pattern

The rest of paper is organized as follows. We first discuss the related work in Section. In Section**Error! Reference source not found.** we describe our proposed method. Simulation and results are provided in Section**Error! Reference source not found.**. Finally some conclusion is drawn in Section.

2. RELATED WORKS

TCP low rate attack misuse different layers of TCP/IP network model. In physical there is layer Lion attack that is related to attack to cognitive radio device [4]. Low rate attack to protocols which is working in in application layer investigated is different researched [5-7]. TCP Low rate DoS attack were proposed by Kuzmanovic in 2003 which is known as Shrew attack too. Internet2 network is one of destination of TCP low rate DoS attack [8]. In this paper we focused on last category i.e. TCP low rate DoS.

In [9] has proposed a distributed detection system. Detection operations will be done using all routers in protected network thus one of drawbacks of this method is not scalable. In this method, each router should perform detection

operation in its input ports. If an input port found, upstream router is responsible of detecting attack. If an input port not found in affected router, it means that distributed denial of service attack is launching. In this case, DRR (Deficit Round Robin) algorithm mechanism performs for queuing to provide bandwidth allocation and protection between flows. Advantage of this method is pushing the detection of low-rate attacks as close as possible to the attack sources, and it is able to minimize damage to the legitimate TCP flows. Another drawbacks of this system is attack detection based on input ports (and not flows of each input ports), because of it is possible that some legitimate flows exist in detected malicious port. In [10] new classification of low rate DoS attack named Pulsing DoS (PDoS) was proposed. This kind of attack itself is categorized into AIMD-based (AIMD stands for Additive Increase and Multiplicative Decrease) attack and Timeout-based attack .In former attacker send its attack pulse till victim timed out. In latter, value of attack pulse is in way of victim repeatedly do fast recovery. According to this classification shrew attack place in Timeout-based. Besides of this classification, a two-stage detection system proposed to detect PDoS attack. The first stage is based on a wavelet transform used to extract the anomaly of components of the data traffic and ACK traffic. Because PDoS attack causes the rate of incoming traffic to fluctuate more severely and when PDoS attack start, rate of outgoing ACK packet decline. The second stage is to detect change points in the extracted components. This method is unable to detect attack flows and only detect attack flows and only detect occurrence of PDoS attack.

Shevtekar and et al [11] proposed low rate TCP DoS attack detection at edge routers. Mechanism of this method is: A flow with a periodic pattern is considered attack flow if its burst length is greater than or equal to RTTs of other connections with the same server, and its time period (parameter T in Figure 1) is equal to the fixed minimum RTO (1ms). Another flows sent from this server is considered attack flow too. This method is able to detect DoS attack and is unable to detect DDoS attack at all. Aleksandar Kuzmanovic and Edward W. Knightly in [12] investigate existing method proposed for TCP low rate denial of service attack. According to their investigation solutions based on router (in this solutions defense mechanism place in router) such as RED with Preferential Dropping (RED-PD), and A stateless active queue management scheme for approximating fair bandwidth allocation (CHOKe) and solutions based on end host such as randomization of the minRTO parameter, and increase of the initial window size parameter, none of these solutions can completely defend against low rate DoS attack.

In low rate DoS, attacker can tune three parameter (R,L,T) بهarbitrary. In [13], a router-based technique to mitigate reduction of quality (RoQ) attacks has proposed. The RoQ attack does not try to completely denial of service of the legitimate flows, but tries to reduce the quality of service experienced by them. In this type of attacks, attacker will send attack flows with higher time period. For counter measuring against this attack, they form a benign flow table. The benign long-lived flows passing through the router will saved in this table. In this paper a flow that be active for more than two seconds are named long lived flow. Reason of defining this concept is encountering to IP Spoofing (In IP spoofing attacker uses spoofed source IP address and therefore flows constructed with this manner early died). When a packet received in router, if its flow exists in one of records of benign flow table, it will directed to outgoing link otherwise it can be blocked. Advantage of this problem is partially resistant against IP spoofing. In our idea, there exist more short lived flows such as HTTP and DNS packets that this method can detect them as attack flow. Attacker can easily change its flows pattern too.

Some of methods are proposed based on RED (Random Early Detection) algorithm. Zhang and et al. [14] proposed RRED (Robust RED) algorithm that use RED algorithm in its detection mechanism. This method can provide more throughputs in compare to algorithms such as Drop Tail and RED-Preferential Dropping (PD). Main idea of this method is based on behavior of TCP protocol. In flow related to TCP, when packet dropped, next packets of that flow will send with delay (back off of algorithm for avoiding congestion collapse). Consequently, a packet is suspected to be an attacking flow packet if it is sent within a short-range after a packet is dropped. Of course these packets (for legitimate flows) can be left in network (for example placing in intermediates routers queue) and not a packet sent from sender after awareness from congestion condition and consequently flows related to them considered malicious. Another drawback of this method is weakness in detection of unresponsive flow (non-feedback based flows) such as UDP flows as an attack flow. In [15], another RED-based encountering system is proposed. This system using detection of attack source, disrupt attacker traffic. The purpose of this system is detection and blocking attack traffic before entrance of it in traditional RED algorithm. Proposed method is similar to RRED beside of a testing phase for checking incoming flows. This system has drawbacks of previous method too.

Information theory has been used to identify these attacks. Zhiang in [16], employed two information metrics, entropy metric and the information distance metric. These metrics of information theory applied in order to finding difference between normal traffic and attack traffic (They check out traffic from perspective of packet size and IP distribution). First in each router check whether anomaly exist or not. Despite of existence of anomaly, if that is result of local network connected to router, traffic of that network will be blocked, otherwise (if that is not result of local network connected to router) upstream router are responsible of finding attack source. Scalability of proposed system is low because full control of all the routers is necessary.

As we found in some defense system, one of phases before encountering against attack sources is notification about attack occurrence. In [17], time-based network traffic features such as duration of time slot, traffic in current time slot, average traffic per time slot, packet inter-arrival time in current time slot, average packet inter-arrival time, number of time-outs in current time slot, number of discarded packets in current time slot, number of connections to the server in current time slot, threshold value for number of packets discarded in a particular time slot has used. This system need to supplement defense system for encountering to TCP low rate denial of service attack.

Zhang and et al in [18] proposed a new metric named CPR (Congestion Participation Rate) for detection of attack flows. Main idea of this system is derived from behavior of TCP congestion control. Legitimate TCP flows tend to eliminate and save network from congestion. Thus they send much lower traffic in congestion condition. It is contrary to behavior of attack flow so that they tend to put network in terms of congestion. CPR parameter determines which flows are sending more traffic in congestion condition and therefore introduce them as attack flows. Main drawback of this system is recognizing unresponsive flows such as UDP flow as an attack flow. In [19], a chaos-based detection system has proposed. This system is based on two assumptions: the major part of today Internet traffic is related to TCP and low rate attack traffic has very low traffic volume. In our opinion this assumptions is not tautology proposition in all network condition. According to these assumptions and using signal processing try to find attack traffic. Given that chaotic systems are sensitive to determined signals (such as attack signal which has determined pattern) have used to detect low rate attack. In [20] an adaptive IP trace back method is presented that differs from packet marking method (method using in trace back). For detecting abnormally traffic in router traffic, entropy variation is applied to measure changes of randomness of flows in a router. After detecting anomaly in victim, the victim will continue operation with pushing back detection system for finding upstream routers caused attack. This method will bypass when attacker mimic a normal behavior.

In recent research, researchers tend to investigate different aspects and results of LDDoS. Zhijun and et al. [21] presents a new method for launching an LDDoS attack. Aggregation of distributed sources in appropriate time (which caused a effective damage impact to victim) is most important in DDoS specially in LDDoS attack. In this paper a cross correlation algorithm is proposed. The purpose of this work is launching an attack with high performance. In [22], a mathematical model for analyzing this attack is presented. This paper presents a network model and attack model and analyze impact of LDDoS on these environment and finally present a strategy to defending against such attack. In [23] impact of LDDoS attack on feedback based system is evaluated. Feedback based systems are which systems need to feedback of other side of relation to perform their next operations (such as TCP, web server). In this paper developed a novel methodology to systematically analyze the impact of LDDoS attack and two problem considered: “1) what is the impact of an low rate DoS attack on a general feedback-control based system and 2) how to conduct a systematic evaluation of the impact of an low rate DoS attack on specific feedback-control based systems”. A result of this real research (research is performed on real servers) shows LDDoS can degrade performance of these types of systems.

Because of using information metric used in some proposed method for describing different characteristics of network traffic, in [25] an empirical evaluation of information metric both for low rate and high rate attack is performed. The main purpose of this work is finding efficiency and effectiveness of several major information metrics: Shannon entropy, Renyi’s entropy, generalized entropy, Kullback-Leibler divergence and generalized information distance.

For presenting a sound and complete defensive system for DDoS attacks, first we should be familiar to different aspect them. In [24] low rate DDoS (LDDoS) attack and flooding DDoS attack has been compared in these criteria: generation principles, mechanism utilizations, behaviors, signatures, and attack performances.

3. PROBLEM SPACE

In previous section we reviewed some of proposed system for encountering to TCP low rate denial of service. As a result we found that these systems have drawbacks which enable attacker to deny service. Some of these drawbacks are:

•Weakness in recognizing non feedback based flows such as UDP flows.

•Constructing their solution based on detecting fixed pattern of attack flows.

•Need to more process and memory resource for encountering against attack.

•Constructing their solution based on escapable assumption.

As we said among describing related works, some establish their encountering system based on specific pattern of TCP LDDoS attack (in term of deterministic statistical attack traffic pattern or fixed attack flows wave form). Already only these types of attack considered and therefore encountering attack were designed to defend against these types of attacks.

4. PROPOSED METHOD

In this section, first we proposed a new approach for encountering against TCP low rate denial of service attack and next we present our encountering system.

A. Approach of proposed system

In previous section we found some drawbacks in proposed solutions. Most important drawback of them was considering fixed pattern of attack flow. In our opinion defender should consider network condition with high level vision. For achievement of an effective approach, we have answered this question: what behaviors attacker should show up to his attack be successful? We find the answer in this manner: Attacker should lead to the loss of TCP packets AND in a short time have a strong presence AND in a short time have an inconspicuous presence. This answer leads us to find some observation. These observations are:

•First observation: Existing more-defected TCP flows in attack condition

•Second observation: When the loss is increasing, many of the attacker flows are in the output queue of victim router.

•Third observation: When the loss is decreasing, many of the benign flows are in the output queue of victim router.

In following we will explain these observations in details.

1. First observation

The purpose of attacker for sending burst traffic is facing TCP flows with packet loss. Using burst traffic, attacker wants to permanently maintain TCP flows in slow start (timeout) phase. This action of attacker causes, in each try of TCP sender for sending packet, packets will be loosed. Thus our first observation formed. We define defected flows as flows which in each try for sending packets, buck of their packets will be loosed in router.

Among all flows, those flows that are less defected are combination of non-feedback based flows (such as UDP flows which don't back off in packet loss condition) and attack flows. Beside of these flows and according to [3], very small percentages of TCP flows utilize available bandwidth and therefore are not more affected. For further evaluation, these three categories of flows are entered to phase of recognizing benign/attack behavior. In formal method can be state that:

F = {include all of flows such that fi is ith flow}

D = {contain all of defected flows}

T = F – D

T is combination of non-feedback based flows and attack flows. At this stage we expect legitimate TCP flows be extracted.

2. Second observation

Among three categories of flows mentioned in above, one category is attack flow. We will present criteria for detecting this category of flows. Attacker essentially should send burst traffic for occurrence of loss in victim flows. Attacker will be ensured that goal of loss occurrence is satisfied when he/she fills link capacity. Therefore in attack time (when loss rate is increasing in router), the high percentage of flows existing in output queue of router are attack flows. Thus the second observation formed.

3. Third observation

For achievement a low rate attack, attacker essentially should be silence after sending burst traffic. In time interval between two bursts (when loss rate is decreasing), the high percentage of flows existing in output queue of router are benign flows (small percentage of flows are attack flows). Thus the third observation formed.

B. Method of acquiring observation

All input flows have Fi counter which show total is sent packet of ith flow. For collecting flows related to first observation, we determine counter Di. Di will be increased if packets of ith flow were loosed. Note that size of loosed packet will be added to Di counter. Then using dividing Di by Fi, defected rate will be yield. This division show that what rate of input packet is loosed in output queue. Whatever the value of this division for a flow be greater, the flow is more defected. For example, if a flow has sent 2048 bytes and 1024 bytes have been lost, defection of rate is 0.5. While if a flow has sent 65536 bytes and 1024 bytes have been lost, defection rate is 0.015. We define counter Si which shows number of presence of ith flow in the time loss is increasing. As Si increases, ith flow is more suspected to be an attack flow. Also we define counter Bi which shows number of presence of ith flow in the time loss is decreasing. As Bi increases, ith flow is more suspected to benign flow. Main problem in extracting these two observations is finding time of increase or decrease of loss in router (We name as decision make component). To achieve this purpose, we define small time interval we named it as snap shot (t snapshot). Then we will count number of loosed bytes for all flows (fi) in t snapshot (lsnapshot). Following equation yields rate of loss: (lsnapshot / tsnapshot). Now by comparing loss rate of each snapshot, we could determine, increasing or decreasing state of system. In this decision maker component, two critical issues exist:

Criteria for declaring state of system (increasing or decreasing state). It is important for our encountering system to determine these two states correctly; because we record number of flow presence in these states and according to this numbers we determine similarity of flows to legitimate or attack flows. We monitor loss rate in each snapshot. In non-attack condition, amount of packet loss is not intermittent in consecutive snapshot. But in attack time, loss rate increases in time of starting attack burst to the end of burst. For sake of simplicity, we consider increasing state if current loss rate is more than previous loss rate and we consider decreasing state if current loss rate is less than previous loss rate.

Determining tsnapshot length. As we defined loss rate in above, finding length of tsnapshot is another important issue. On the other hand, after this time has elapsed, according to router state, output flows place in set of B or S (i.e. Bi or Si counter has been increased). Short duration of snapshot makes decision false and long duration of tsnapshot makes decision process long time.

C. Composition Of observation results

In Fig. 2 architecture of proposed system is depicted. In this figure main component of defending system and their input and output is provided. Output of each observation is a flow table. For first observation (defected flows), we have Defected table; each entry pair of this table shows flow id and rate of its defection. For second and third observation, we have Suspected and Benign table respectively; each entry pair of these tables shows number of presence (i.e. it is a counter) of each flow in desire time (attack time or non-attack time).

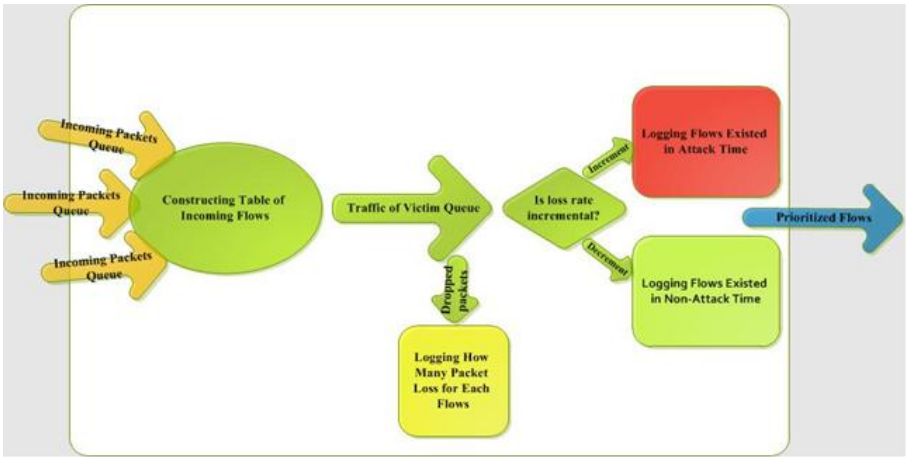


Fig. 2. Architecture of proposed system

We sort defected and benign table ascendant and suspected table descendent (i.e. for example a flow which is more defected and more benign, has bigger index and a flow which is more suspicious has lower index in table). Now it is enough that find summation of index number of each flow in these three tables and then sort result of this addition in descending manner. Indeed this ordered list is our priority queue based on behavior of each flow according to our three observations. As we know, a flow with higher priority takes more services and a flow with lower priority will take less services. We include an example for Fig. 3. For example priority number for flow a1 is: 5 + 2 + 3 = 10 and Priority number for flow l1 is: 8 + 7 + 7 = 10.

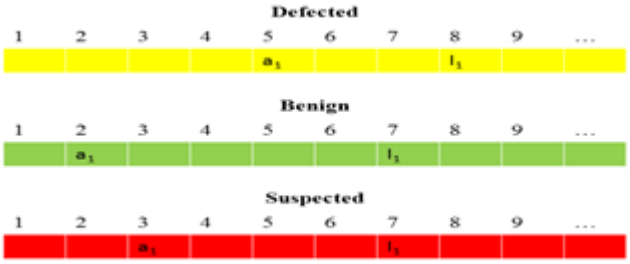


Fig. 3. Composition Of observation results

As in above example showed, priority number of l1 which is a legitimate flow is more than a1 which is an attack flow.

5. SIMULATION AND RESULTS

In this section we first explain studied topology. Then we will design and simulation of our proposed method. In Fig. 4 topology which attacker will misuse it depicted. This topology is known as Dumbbell Topology and usually used for congestion algorithm analysis. In real network a path from sender to receiver has more intermediate nodes (such as intermediate routers). Although for analysis, intermediate node won't be considered and just bottleneck link (link with lowest bandwidth) will be investigated. In depicted topology, link L satisfy these conditions.

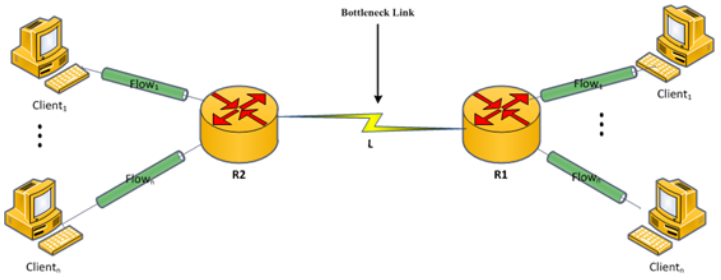


Fig. 4. Topology which attacker will misuse it

For simulation we use NS2, popular network simulator version 2. Implementation of defending system (our proposed method) is performed using AWK programming languages.

D. Experiments

We use topology showed in Fig. 5 as a base scenario for our experiments (Shrew attack used similar topology in their simulation).

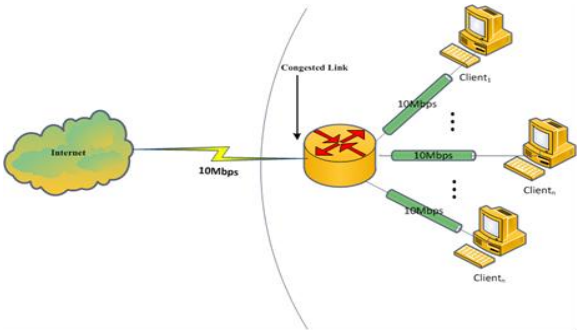
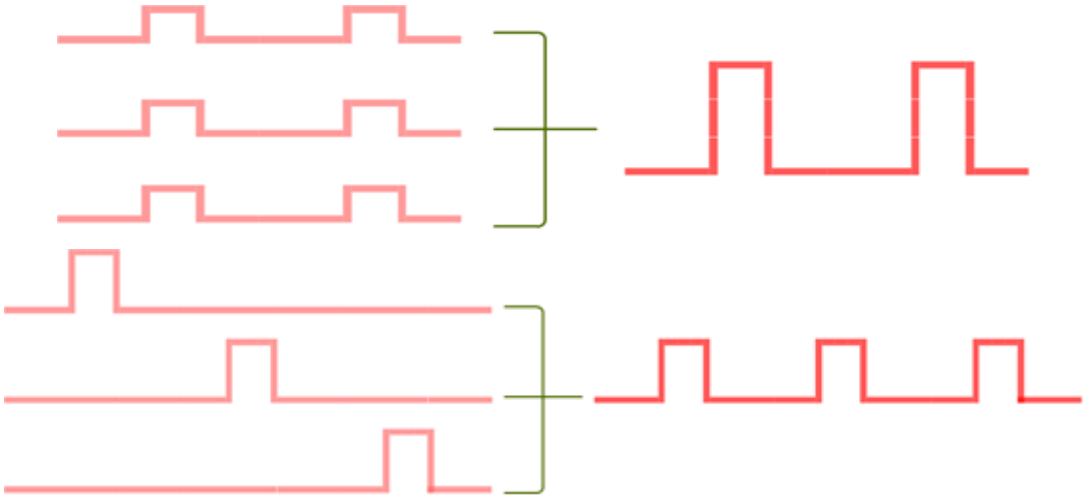


Fig. 5. Scenario for our experiments

LDDoS attack can experience different effectiveness according to flows protocol (example of protocols of a flow is UDP or TCP or etc.). On the other side, performance of encountering system can be differing according to presence of flows with different protocols. Because of these considerations, in this section we will experiment and evaluate various scenarios. TCP low rate DDoS attack traditionally can be done at least with three types of coordination showed is Error! Reference source not found.. For each of these kind we prepare a simulation and get results of them.



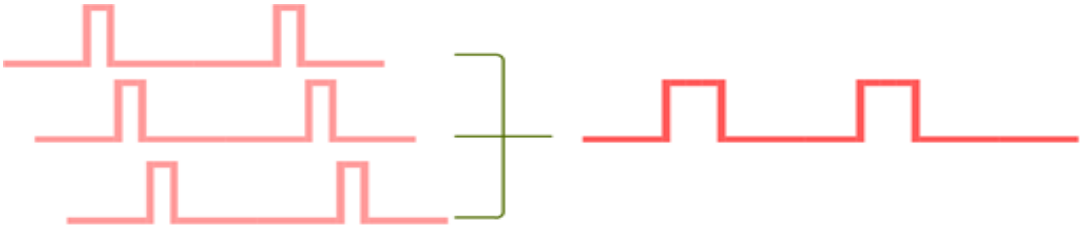


Fig. 6. Different types of DDoS attacks

1. First Case Study

In this experiment, TCP flows, UDP flows and attack flows are as incoming flows and are outgoing to special destination (victim link). The purpose of this experiment is evaluation of correctness of proposed method in presence of legitimate UDP flows.

Table 1. Flows characteristics

Flow ID	Properties	Start time	Finish time
FTP1	-	0	50
FTP2	-	0	50
CBR1	Rate:5Mbps	0	50
CBR2	Rate:5Mbps	0	50
Attack1	Rate:10Mbps; burst period:1s; period length: 200ms	0	50
Attack2	Rate:10Mbps; burst period:1s; period length: 200ms	0	50
Attack3	Rate:10Mbps; burst period:1s; period length: 200ms	0	50

In Fig. 7 results of logging defected flow is depicted. This chart show that how much a flow is recognized defected by proposed system (In all figures vertical axis is flow label and horizontal axis is tensity of Defected/Legitimate/ Suspicious/Priority).

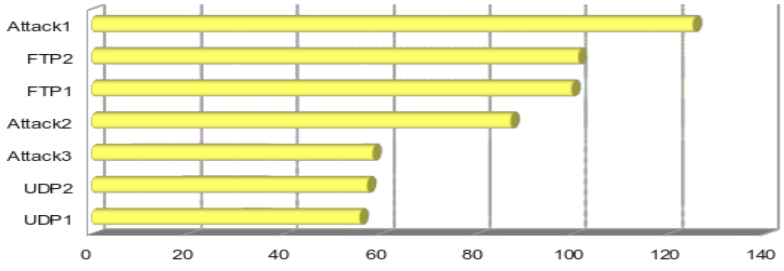


Fig. 7. Defected flow

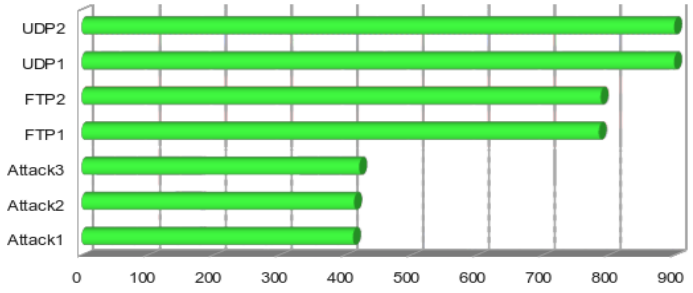


Fig. 8. Legitimate flow

In Fig. 9 results of logging suspicious flow is depicted. This chart show that how much a flow is recognized suspicious by proposed system.

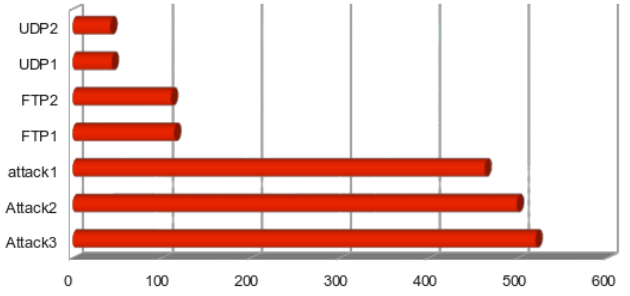


Fig. 9. Suspicious flow

Now we aggregate results of three observations. Fig. 10 show that flows related to attack flows are in lower priority and flows related to legitimate flows placed in higher priority. This result states that our system is capable of detecting legitimate UDP flows from attack UDP flows. We repeated this simulation for each states of attack showed in fig … and in all three state we get correct result.

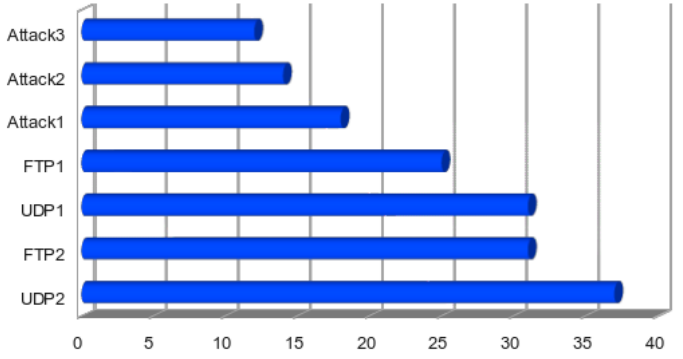


Fig. 10. Priority

2. Second Case Study

In this experiment, TCP flows, UDP flow, HTTP flow and attack flows are as incoming flows and are outgoing to special destination (victim link). The purpose of this experiment is evaluation of correctness of proposed method in presence of legitimate UDP flows. Flows characteristics are provided in Table 2.

Table 2. Flows characteristics

Flow ID	Properties	Start time	Finish time
FTP1	-	0	50
FTP2	-	0	50
CBR1	Rate:5Mbps	0	50
HTTP	Rate of connection creation:15connection per second	0	50
Attack1	Rate:10Mbps; burst period:1s; period length: 200ms	0	50
Attack2	Rate:10Mbps; burst period:1s; period length: 200ms	0	50
Attack3	Rate:10Mbps; burst period:1s; period length: 200ms	0	50

In Fig. 11 results of logging defected flow is depicted. This chart show that how much a flow is recognized defected by proposed system.

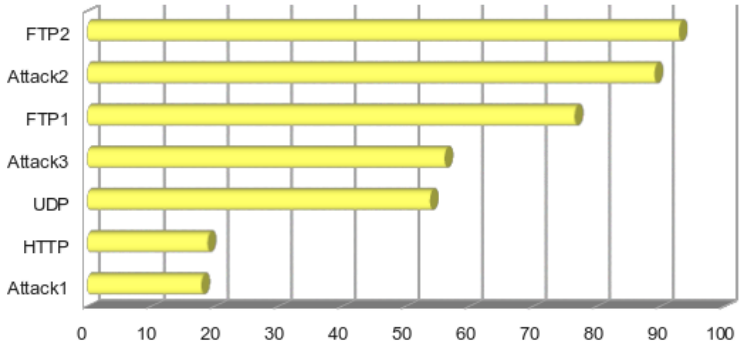


Fig. 11. Defected flow

In Fig. 12 results of logging legitimate flow is depicted. This chart show that how much a flow is recognized legitimate by proposed system.

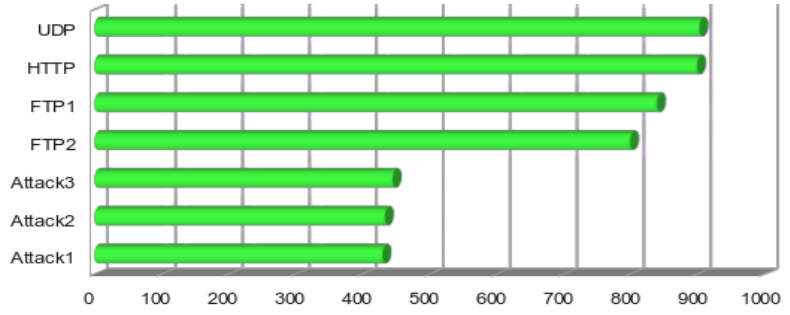


Fig. 12. Legitimate flow

In Fig. 13 results of logging suspicious flow is depicted. This chart show that how much a flow is recognized suspicious by proposed system.

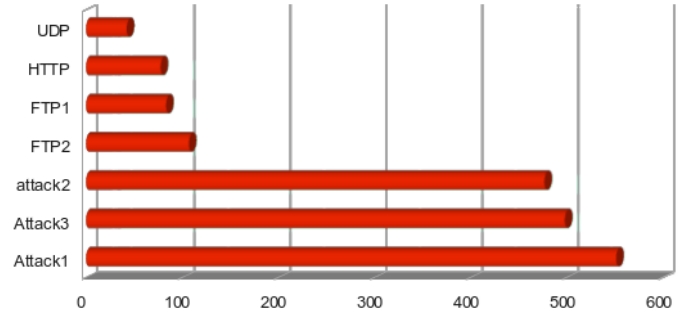


Fig. 13. Suspicious flow

Now we aggregate results of three observations. Fig. 14 show that flows related to attack flows are in lower priority and flows related to legitimate flows placed in higher priority. This result states that our system is capable

of detecting legitimate HTTP flows from attack flows. We repeated this simulation for each states of attack showed in Error! Reference source not found. And in all three state we get correct result.

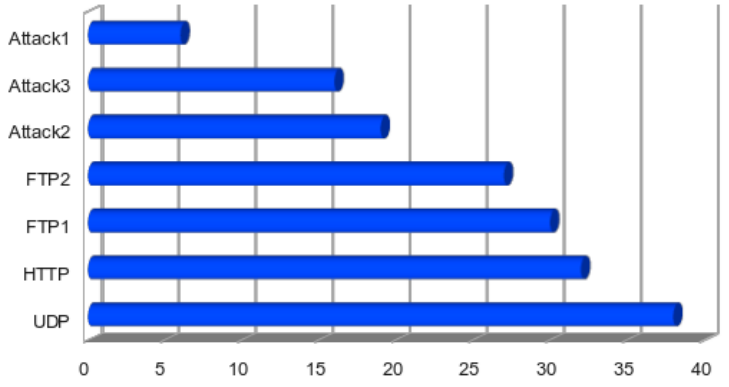


Fig. 14. Priority

6. CONCLUSION

We proposed an encountering system against TCP Low rate Distributed Denial of Service (LDDoS) attack. Traditional methods suffer from some weakness such as recognizing non feedback based flows (e.g. UDP flows) as attack flows, constructing their solution based on detecting fixed pattern of attack flows, need to more process and memory resources for encountering against attack and constructing their solution based on escapable assumption. We presented a new approach to detect TCP LDDoS attack. Our approach uses three fundamental observations which attacker has to perform them. These fundamental observations are: existing more-defected TCP flows in attack condition, when the loss is increasing many of the attacker flows are in the output queue of victim router and when the loss is decreasing many of the benign flows are in the output queue of victim router.

We evaluated proposed method with different type of challenging scenario to verifying correctness of it. Results showed that our proposed method is able to detecting LDDoS attack flows and distinguish between legitimate flows (TCP, UDP, and HTTP) and attack flows. For future work we want to present additional observation and additional method to acquiring data of these observations.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] Seryasat, O. R., & Haddadnia, J. (2017). Assessment of a novel computer aided mass diagnosis system in mammograms. Biomedical Research, 28(7), 3129-3135.
[2] Seryasat, O. R., & Haddadnia, J. (2018). Evaluation of a new ensemble learning framework for mass classification in mammograms. Clinical breast cancer, 18(3), e407-e420.
[3] Kuzmanovic, A., & Knightly, E. W. (2003). Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants. In Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications (pp. 75-86). ACM. doi:10.1145/863955.863966
[4] Hernandez-Serrano, J., León, O., & Soriano, M. (2011). Modeling the lion attack in cognitive radio networks. EURASIP Journal on Wireless Communications and Networking, 2011, 2. doi:10.1155/2011/242304
[5] Maciá-Fernández, G., Díaz-Verdejo, J. E., García-Teodoro, P., & de Toro-Negro, F. (2007). LoRDAS: A low-rate DoS attack against application servers. In International Workshop on Critical Information Infrastructures Security (pp. 197-209). Springer, Berlin, Heidelberg. doi:10.1007/978-3-540-89173-4_17
[6] Maciá-Fernández, G., Díaz-Verdejo, J. E., García-Teodoro, P., & de Toro-Negro, F. (2007). LoRDAS: A low-rate DoS attack against application servers. In International Workshop on Critical Information Infrastructures

Security (pp. 197-209). Springer, Berlin, Heidelberg. doi:10.1007/978-3-540-89173-4_17
[7] Yang, J. S., Park, M. W., & Chung, T. M. (2013, June). A Study on Low-Rate DDoS Attacks in Real Networks. In Information Science and Applications (ICISA), 2013 International Conference on (pp. 1-4). IEEE. doi:10.1109/ICISA.2013.6579418
[8] Delio, M. (2001). New breed of attack zombies lurk [R/OL].
[9] Sun, H., Lui, J. C., & Yau, D. K. (2004). Defending against low-rate TCP attacks: Dynamic detection and protection (pp. 196-205). IEEE.
[10] Luo, X., & Chang, R. K. (2005). On a New Class of Pulsing Denial-of-Service Attacks and the Defense. In NDSS.
[11] Shevtekar, A., Anantharam, K., & Ansari, N. (2005). Low rate TCP denial-of-service attack detection at edge routers. IEEE Communications Letters, 9(4), 363-365. doi:10.1109/LCOMM.2005.1413635
[12] Kuzmanovic, A., & Knightly, E. W. (2006). Low-rate TCP-targeted denial of service attacks and counter strategies. IEEE/ACM Transactions on Networking (TON), 14(4), 683-696. doi:10.1109/TNET.2006.880180
[13] Shevtekar, A., & Ansari, N. (2008). A router-based technique to mitigate reduction of quality (RoQ) attacks. Computer Networks, 52(5), 957-970. doi:10.1016/j.comnet.2007.11.015
[14] Zhang, C., Yin, J., Cai, Z., & Chen, W. (2010). RRED: robust RED algorithm to counter low-rate denial-of-service attacks. IEEE Communications Letters, 14(5). doi:10.1109/LCOMM.2010.05.091407
[15] Razian, M. R. TCP Low Rate DDoS Attack Detection.
[16] Xiang, Y., Li, K., & Zhou, W. (2011). Low-rate DDoS attacks detection and trace back by using new information metrics. IEEE transactions on information forensics and security, 6(2), 426-437. doi:10.1109/TIFS.2011.2107320
[17] Mathew, R., & Katkar, V. (2011). Software based low rate dos attack detection mechanism. International journal of computer applications, 20(6), 14-18. doi:10.5120/2439-3285
[18] Zhang, C., Cai, Z., Chen, W., Luo, X., & Yin, J. (2012). Flow level detection and filtering of low-rate DDoS. Computer Networks, 56(15), 3417-3431. doi:10.1016/j.comnet.2012.07.003
[19] Wu, Z. J., Lei, J., Yao, D., Wang, M. H., & Musa, S. M. (2013). Chaos-based detection of LDoS attacks. Journal of Systems and Software, 86(1), 211-221. doi:10.1016/j.jss.2012.07.065
[20] Baskar, M., Gnanasekaran, T., & Saravanan, S. (2013). Adaptive IP traceback mechanism for detecting low rate DDoS attacks. In Emerging Trends in Computing, Communication and Nanotechnology (ICE-CCN), 2013 International Conference on (pp. 373-377). IEEE. doi:10.1109/ICE-CCN.2013.6528526
[21] Wu, Z., Cui, Y., Yue, M., Ma, L., & Wang, L. (2014). Cross-correlation based synchronization mechanism of lddos attacks. Journal of Networks, 9(3), 604. doi:10.4304/jnw.9.3.604-611
[22] Luo, J., Yang, X., Wang, J., Xu, J., Sun, J., & Long, K. (2014). On a mathematical model for low-rate shrew DDoS. IEEE transactions on information forensics and security, 9(7), 1069–1083. doi:10.1109/tifs.2014.2321034
[23] Tang, Y., Luo, X., Hui, Q., & Chang, R. K. (2014). Modeling the Vulnerability of Feedback-Control Based Internet Services to Low-Rate DoS Attacks. IEEE Trans. Information Forensics and Security, 9(3), 339-353. doi:10.1109/TIFS.2013.2291970
[24] Wu, Z., Li, G., Yue, M., & Zeng, H. (2014). DDoS: Flood vs. Shrew. JCP, 9(6), 1426-1435. doi:10.4304/jcp.9.6.1426-1435
[25] Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2015). An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. Pattern Recognition Letters, 51, 1-7. doi:10.1016/j.patrec.2014.07.019