Cooperative Scenario based Centralized Defense Mechanisms for Low-Rate TCP Attacks

Won-Ho So[O], Sang-Heon Shim*, Kyeong-Eun Han*, Kyoung-Min Yoo*, Soon-Seok Lee**,
Young-Sun Kim**, and Young-Chon Kim*

Dept. of Computer Education, Sunchon National University, Suncheon Korea
* Dept. of Computer Engineering, Chonbuk National University, Jeonju Korea
** ETRI BcN Architecture Team, Daejeon Korea

***Abstract*—The low-rate TCP attack has been reported recently. That is essentially a periodic short burst which exploits the homogeneity of the minimum retransmission timeout (RTO) of TCP flows. It is difficult to identify this sort of attack in BcN (Broadband convergence Network) due to no cooperative defense mechanisms among different networks. In this paper, NCP (Network Control Platform) based centralized defense mechanisms are proposed. Firstly, low-rate TCP attack and the previous defense mechanisms are reviewed. It helps us to find and select reasonable features of them for supporting the proposed mechanism. Secondly, we propose a cooperative defending scenario between NCP as centralized controller and MDRs (Monitoring and Defending Routers). Without adopting defense mechanism to all routers in network, it is possible to effectively protect network resource from low-rate TCP. That is because the attack flows can be filtered at both victim-side and attack side MDRs with cooperative scenario. The performance id evaluated by using ns-2 simulator.**

***Index Terms*—Low-rate TCP, DoS, Network Security, BcN**

I. Introduction

The Internet has been required to provide various services and to evolve into broadband networks due to dramatic increase in the number of users and multimedia traffic volume. This makes network service providers converge their network services on broadband IP based Internet. Specially, BcN (Broadband Convergence Network) related technologies have been introduced and focused at variety of research area. In order to efficiently construct BcN as the next generation network, the requirements such as the quality of service, network survivability, SLA (Service Level Agreement), and network security should be satisfied. The network security will be one of these important components of BcN in the near future [1].

Denial of Service (DoS) attacks consume resources in networks, server clusters, or end hosts, with the malicious objective of preventing or severely degrading service to legitimate users. Example DoS attacks include TCP SYN attack, ICMP flooding, and DNS flood attacks and they generates high volumes of traffic like a sledge-hammer directed at a target victim [2, 3].

In this paper, low-rate TCP attacks called as "shrew attacks," is introduced in point of BcN. This attacks attempt to deny bandwidth to TCP flows while sending at sufficiently low average rate to elude detection by counter-DoS mechanisms. We review the TCP's RTO (Retransmission Time Out) and the previous mechanisms for defending these attacks. And the usage of NCP (Network Control Platform) as a centralized network controller of BcN is considered. Thus we propose a centralized defense mechanism by using cooperative scenario between NCP and other edge routers.

This paper is organized as follows. In Section 2, we show the TCP retransmission timer behavior, low-rate TCP attack, and previous defending mechanisms. The proposed mechanism based on NCP is described in Section 3. In Section 4, we provide simulation results by using ns-2. Finally, we draw conclusions and suggest future work in Section 5.

II. Low-rate TCP Attack and Defenses

A. TCP Timeout Mechanism

TCP Reno uses the following RTO mechanism for congestion control in Internet which is exploited by low-rate TCP DoS attack. Packet loss is detected via either timeout from non-receipt of ACKs, or by receipt of a triple-duplicate ACK. If loss occurs and less than three duplicate ACKs are received, TCP agent waits for a period of retransmission timeout to expire, reduces its congestion window to one packet, and resends the packet. Therefore the performance of TCP connection decreases in throughput due to this waiting time. Allman and Paxson experimentally showed that TCP achieves near-maximal throughput if there exists a lower bound for RTO of one second [4]. Figure 1 shows the behavior of the TCP retransmission timer.

B. Low-rate TCP DoS Model

As described in previous section, the loss with retransmission timeout sets the congestion window to 1 and induces the degradation of throughput. For example, consider a single TCP flow and a single DoS stream. Assume that an attacker creates

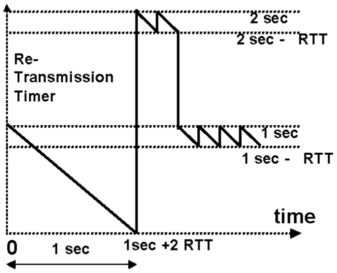


Fig. 1. Behavior of the TCP retransmission timer

1-4244-0574-2/06/$20.00 (C)2006 IEEE

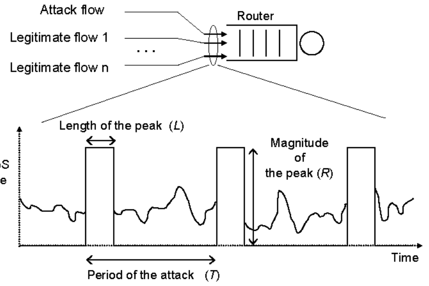


Fig. 2. Square-wave DoS stream

an initial outage at time 0 via a high-rate burst of short duration. Due to this dramatic packet loss, the TCP sender will wait for a retransmission timer of 1 sec to expire and will then double its RTO. If another attack is created between time 1 and 1+2*RTT*, the TCP sender should wait another 2 sec.

Figure 2 shows the “square wave” shrew DoS attacks which transmits bursts of duration *L* and rate *R* in a deterministic on-off pattern that has period *T*. Generally, a successful shrew attack will have rate *R* large enough to induce loss (i.e., *R* aggregated with existing traffic must exceed the link capacity). In addition, *L* should be long enough to induce timeout but short enough to avoid detection. Finally, *T* is set to RTO for TCP flows to exit timeout and to face with another loss.

C. Defending Mechanisms

A defense to this “shrew wave” attack is to randomize the RTO. In doing so, information can still be transmitted while the attacker is waiting and a connection will be able to avoid timing out successively. Randomizing the fixed minimum RTO seems to be an immediate solution, but the main issue is whether such an approach should be adopted. Randomizing also reduce the TCP connection performance in the absence of an attack [5].

In [6], a distributed detection mechanism which uses the dynamic time warping (DTW) method is adopted to robustly and accurately identify the existence of this sort of attack. Once a router detects the attack, it use a fair resource allocation mechanism is used so that the number of affected TCP flows is minimized, and provide sufficient resource protection for the affected TCP flows. This mechanism, however, should be required to be implemented at multiple routers along the path from source to destination.

A novel scheme that does not introduce any modification to the TCP congestion control mechanism and can be implemented at a single edge router [7]. This approach maintains the arrival times of packets at the edge router. The malicious flow detection sub-module of the object module computes the time difference of consecutive packets of each flow. If the average high value of the time difference repeats periodically for the attack flow and its burst length is larger than or equal to the RTTs of other flows, the attack flow will be filtered at victim edge router. This scheme, however, can not protect other flows affected by this attack at intermediate router.

III. Centralized Defense Mechanisms

In this section, we propose the centralized defense mechanisms based on cooperative scenarios. For this goal, we compare previous mechanisms in terms of detection method, attack decision process, attack defense, extra process, and implement cost. Table 1 shows that results.

TABLE 1
Comparison of Previous Mechanisms

Ref. Term	[5]	[6]	[7]
Detection	×	Periodic Burst	Pkt. Arrival
Determining	×	DTW	Arrival Difference
Defense	×	DRR*	Edge Filtering
Extra process	Randomizing	Trace Back	×
Implement	All TCP agents	All Routers	Single Router

* DRR means deficit round robin.

In order to effectively adopt these previous methods to BcN with NCP, we propose a mechanism to satisfy the following requirements. *First*, the centralized controller aggregates the information of attack flows, process to determine where the source of attack is and what kind of the defense methods are available. *Second*, edge router between two different networks only detects the periodic attack pattern and responses to NCP control message by defending attack. *Third*, the cooperative attacks which consist of two or more low-rate DoS sources can be defended. The first and second requirements can be achieved by using NCP and MDR (Monitoring and Defending Router), respectively. Thus if MDR uses available detection methods as described in previous section, we can use throttle scheme at appropriate MDRs, and it also satisfy the third requirement without the implement of key function at all routers.

The following cooperative scenario is important for our proposed defense mechanism. We assume that key components, such as detection, decision, and defense methods, of our mechanism are similar to the previous mechanisms.

The Scenario of NCP based defending Mechanism

Notations: ***M*** is a MDR, $\boldsymbol{P_i}$ and $\boldsymbol{P_o}$ are MDR’s input port and output port, and ***C*** is NCP.

① Low-rate TCP attack is detected at $\boldsymbol{P_i}$ and $\boldsymbol{P_o}$ of an ***M***.
② ***M*** transfers the attack flow information consisting of <5-tuple> and <*T*, *L*, *R*> to ***C***.
③ ***C*** determines the attack pattern and selects ***M***s for traffic throttle by using <5-tuple>.
④ ***C*** decides the defense methods and conducts ***M***s by sending attack flow information and methods to them.
⑤ ***M***s react the attack flow by using information from ***C***.

To describe our mechanism in detail, we can use above scenario as the following example in figure 3. R1, R4, and R5 are MDRs and R2, R3, R6, R7, and R8 are general routers. When R1 detects a periodic attack flow by using <*T*, *L*, *R*> model and packet arrival differentiation (step 1), R1 reports the 5-tuple flow information and <*T*, *L*, *R*> model of attack (step 2). NCP starts the procedure to determine attack pattern, attack source, and defense methods when it receives some attack information from a victim-side MDR or more MDRs (step 3). If NCP can select the attack-side MDR from which attack starts by processing received attack flow of 5-tuple, NCP may use source

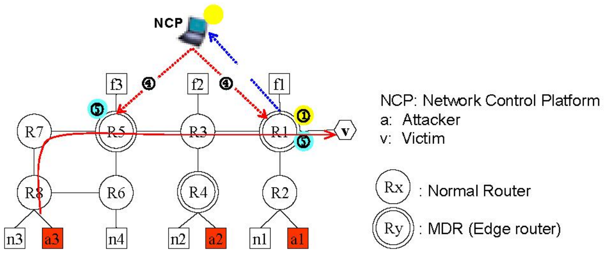


Fig. 3. A scenario for NCB based defending mechanism

throttle method for defending the attack (step 4). It also uses deficit round robin (DRR) scheduling in output buffer. In case of cooperative low-rate attack, NCP can also find the multiple attack sources by using attack information from MDR which is affected by two ore more attack flows. Finally, each MDR which may be the victim-side MDR or other MDRs, can respond to NCP control message by filtering and DRR scheduling (step 5). The following sections describe two types of defending mechanisms such as source filtering scenario approach and hybrid scenario approach.

A. Source Filtering Scenario Approach

This approach uses the flow filtering for attack at two MDRs. One MDR is victim-side router R1 as shown in Figure 3. Another is the first MDR of attack-side router R5. When NCP receives the attack flow information, it can find an attack-side router by using network address of 5-tuple. Thus MDR R1 and R5 can simultaneously throttle the attack traffic by using the information from NCP. With this approach, other normal flows which do not pass R1 but affected by the attack can be protected due to attack flow filtering at both MDRs.

B. Hybrid Scenario Approach

In second approach, we consider flow filtering and DRR scheduling together. In general, routers of Internet use the first-come-first-service (FCFS) scheduling based buffers. This scheduling, however, is not acceptable because of consecutive packet drop under low-rate DoS attack. Thus this is also called as DropTail. On the other hand, DRR uses independent buffer for each traffic flow and legitimate flows are not affected although a specific heavy traffic flow arrives at the router.

In this section, we use DRR scheduling at victim-side MDR and attack-side MDR. In [6], DRR is used for defending low-rate attack, but all routers should use this scheduling and it increases the cost of implementation. Although this scheme is adopted, the low-rate DoS attack can not be efficiently defended. Therefore we propose the hybrid scenario approach to use DRR buffers and flow filtering. In this approach, the only victim-side MDR uses the DRR scheduling and other normal router use DropTail. If there is a low-rate attack, NCP reports the defense method including DRR scheduling and attack flow filtering to victim-side MDR and attack-side MDR respectively. In Figure 3, R1 uses only DRR and R5 uses flow filtering with DropTail.

IV. Simulation Results

In this section, ns-2 is used to evaluate the performance of the proposed centralized defense mechanism [8]. Firstly, some short TCP flows are created as the normal traffic and FTP typed three long TCP flows are connected. Then we generate three attacks called as attack 1, 2, and 3, and finally, we trigger defense mechanisms and compare results.

A. Environments

The experiment network topology is shown in Figure 3. We consider three low-rate TCP attacks (Attack1, Attack2, Attack3) and three TCP flows (Flow1, Flow2, Flow3). The latency of each link is 5ms and the capacity of each link is 5 Mb/s. The low-rate attack is a square burst with T=1.0 sec, burst length L = 0.2 sec, burst rate of 5 Mb/s, and R = 1. The low-rate attack uses UDP with packet size of 100 bytes. The packet size of the TCP flow is 500 bytes. In addition, a hundred short TCP connections are created from fives black squares. Each TCP agent is based on TCP Reno.

Simulation time is 20 sec. In order to measure the link utilization of R1-Server1 of 5 Mb/s, we generate the short TCP of 2.082 Mb/s, and use FTP applications for Flow1, 2, and 3. Figure 4 shows the result of that. Flow1, 2, and 3 respectively get 1.073 Mb/s, 1.104 Mb/s, and 0.694 Mb/s in throughput.

We trigger the low-rate DoS attacks by using UDP agents at three different nodes. We know that Attack2 induces higher degradation than others in link utilization of link R1-Server1 through experiments. Therefore we use Attack2 to evaluate mechanisms as shown in Figure 5.

B. Case of Source Filtering Scenario

Figure 6 shows the throughput of link Rl-Server1 when we only use the attack filtering at victim-side MDR. During simulation time, the attack starts from Attack 2 at 1.5 sec and we assume that the start time of attack flow filtering is 10 sec. But the recovery from performance drawback starts from around 16.5 sec. There may be a question why the throughput is still low even after 10 sec. The reason of that is the increased RTO value due to several low-rate attacks from 1.5 sec to 9.5 sec. Though the attack flow filtering is run at MDR from 10 sec, TCP agent's RTO can not be decreased by MDR and NCP.

Figure 7 show the throughput of link R-1Server1 when we apply the source filtering scenario approach at both MDRs. As it is compared to Figure 6, we can notice that the throughput increases after 10 sec when we use the proposed approach. This is because NCP transfer the control message to attack-side

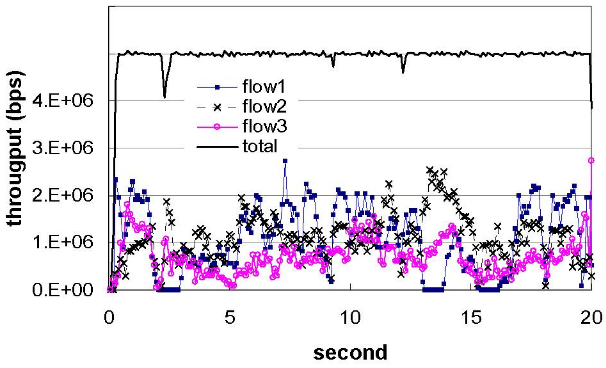


Fig. 4. Traffic volume

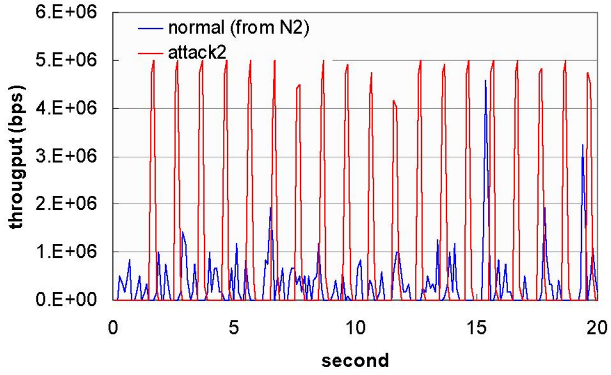
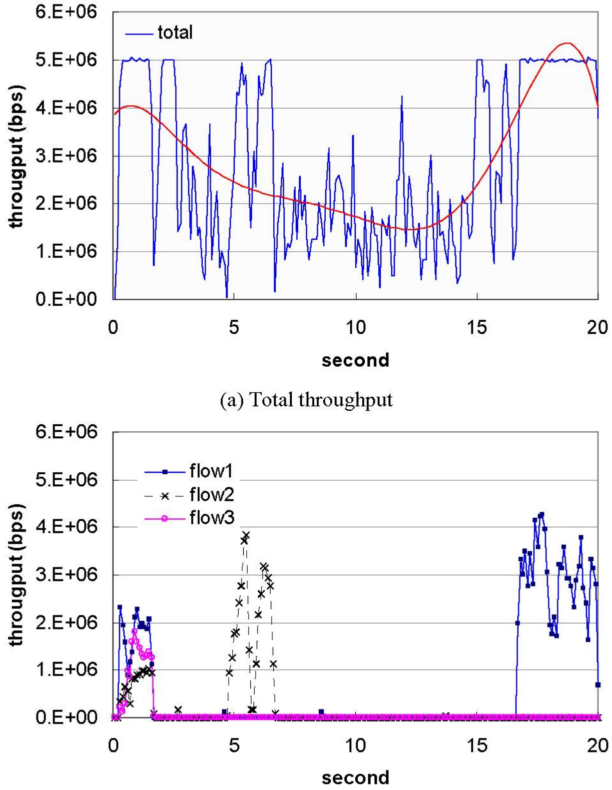
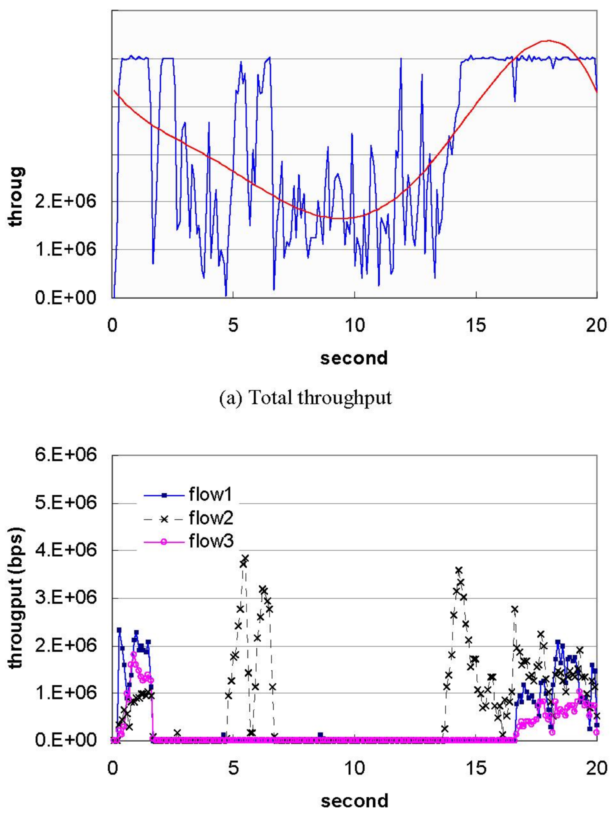


Fig. 5. Attack2 traffic pattern



(a) Total throughput

(b) Throughput per each flow
Fig. 6. Filtering at victim-side MDR



(a) Total throughput

(b) Throughput per each flow
Fig. 7. Source filtering scenario approach

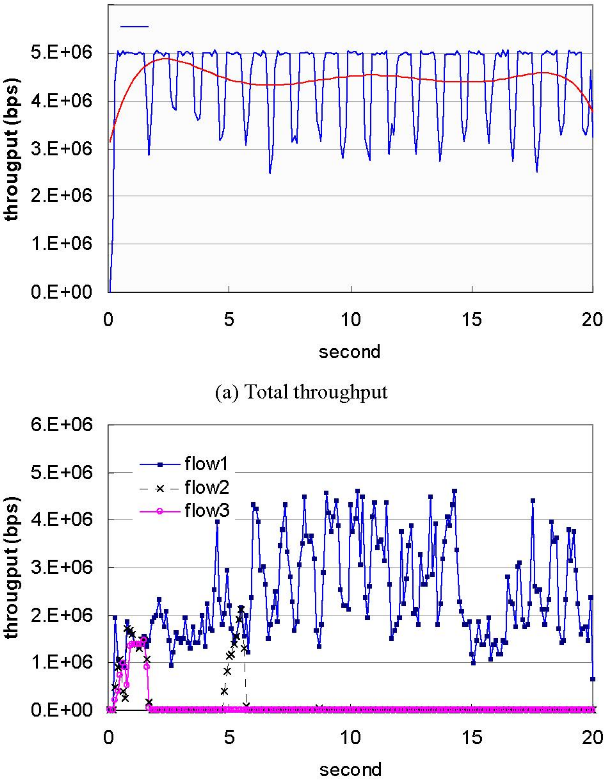
MDR R4 to filter Attack 2 at 10 sec and Flow 2 and Flow 3 traffic can arrive at Server 1 without serious packet dropping. In this case, however, we also notice that the decreased RTO value can not modified by our approach just after 10 sec. In addition, all most of short TCP flows are not affected by the low-rate attack due to short connection life cycle. Thus the link throughput average is about 1.5 Mb/s even under attack.

C. *Case of Hybrid Scenario*

Figure 8 shows the throughput of flows when all MDRs use only DRR scheduling. Because the victim-side MDR use DRR scheduling, Flow 1 has good performance than Flow 2 and 3. In addition, the total data rate of Flow 1 and short TCP flows can increase to 5 Mb/s when there is no attack burst traffic in R1. On the other hand, Flow 2 and Flow 3 can not use network resource of link R3-R1. Thus their performance is near zero. While the victim-side MDR R1 and attack-side MDR R4 have implemented the defense mechanism, R3 as a normal router can not react to any type attack. This notes that only DRR mechanism usage is not enough to control the low-rate DoS attack.

The hybrid scenario approach used mechanism shows its performance in Figure 9. NCP may decide the reasonable defense method for each MDR. It sends the control message of DRR to R1 and reports attack flow filtering to R4. As MDR R4 starts filtering at 10 sec, its effect increases the throughput of Flow 2 and Flow 3. This notes that the attack source throttle at attack-side MDR is very important to defend even low-rate DoS attack. The DRR scheduling can not be the key method for defending as well. Thus if we use a centralized controller like NCP and a few MDRs, the low-rate DoS attack can be efficiently defended in BcN.

Figure 10 shows the value of RTO during low-rate attack and defending time. The RTO is 1 sec under normal state due to no dramatic packet loss. In case of only DRR usage, the RTO values of Flow 2 and Flow 3 except Flow 1 increase continuously. For Flow 2, a sequence is 1, 2, 4, 1, 2, 4, 8, and 16. In case of Flow 3, RTO's value is changed from 1 to 2, 4, 8, and 16 without any withdraw. This means that we can not efficiently support the attack defense without attack flow filtering at attack-side MDR. When we apply the hybrid scenario approach to same simulation environment, All RTO's values of Flows can be finally withdrawn as shown



(a) Total throughput

(b) Throughput per each flow

Fig. 8. Simple DRR at all routers

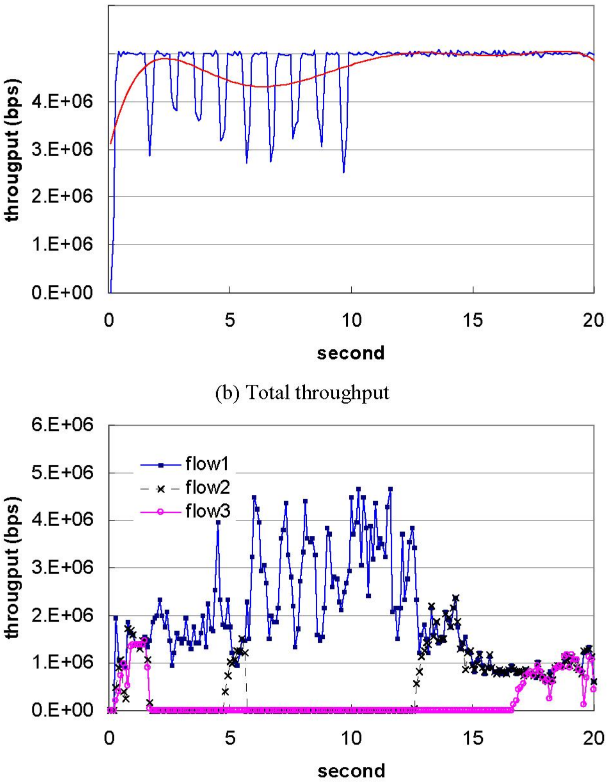
V. Conclusions

In this paper, we review the low-rate TCP attack reported recently and propose the cooperative scenario based centralized defense mechanisms for BcN platform. For this goal, firstly various mechanisms are compared. And we define the role of MDR and NCP for cooperative defending procedure. MDR should detect the periodic attack patterns and report the information about attack flow to NCP. NCP determines attack source and defense methods by using received information from MDRs. Thus all network routers do not have to implement defense method and the processing overhead can be reduced. In addition, attack-side MDR also can be controlled to filter the attack flow, and there is no dramatic decrease in throughput of legitimate flows. The proposed mechanism, therefore, can defend the low-rate TCP attacks more effectively than the previous mechanisms in BcN environment.

References

[1] Y.S. Kim, "Technological Issues and Prospect of BcN," Telecommunication Technology Association, 2005

[2] J. Mirkovic, J. Martin, and P. Reiher, Computer Science Department, UCLA "A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms," Technical report #020018.



(b) Total throughput

(b) Throughput per each flow

Fig. 9. Hybrid scenario approach

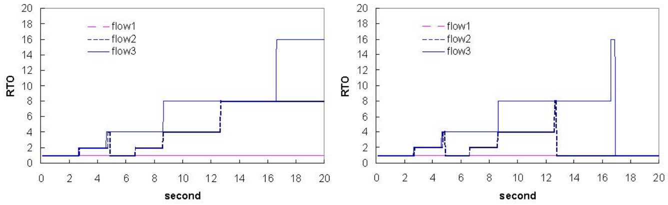


Fig. 10. Behavior of RTO timer in case of DRR and Hybrid scenario

[3] J. Mirkovic, "D-WARD:Source-End defense Against Distributed Denial-of-Service Attacks", Ph.D Thesis 2003.

[4] A. Kuzmanovic and E. Knightly, "Low-rate TCP-targeted denial of service attacks," *In Proc. ACM SIGCOMM*, Karlsruhe, Germany, August 2003.

[5] G. Yang, M. Gerla, and M. Y. Sanadidi, "Randomization: Defense against Low-Rate TCP-targeted Denial-of-Service Attacks," *in Proc. IEEE Symposium on Computers and Communications*, July 2004, pp. 345-350.

[6] H. Sun, J. C. S. Lui, and D. K. Y. Yau, "Defending Against Low-rate TCP Attacks: Dynamic Detection and Protection," *in Proc IEEE Conference on Network Protocols (ICNP2004)*, Oct. 2004, pp. 196-205.

[7] Shevtekar, K. Anantharam, and N. Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," *IEEE Communications Letters*, Vol. 9, No. 4, April 2005.

[8] UCB/LBNL/VINT Network Simulator [online]. Available: http://www.isi.edu/nsnam/ns/