

A Ratio-Based Control Algorithm for Defense of DDoS Attacks

Sheng-Ya Lin, Yong Xiong, Jyh-Charn Liu⁺

Department of Computer Science,

Texas A&M University

College Station TX 77843-3312

{shengya,yongx,liu}@cs.tamu.edu

Technical Report 2005-1-4

Jan 27, 2005

Abstract

Resource depletion is a universal indicator of Distributed Denial of Service (DDoS) attacks. In this paper, we propose a ratio based control algorithm for detection and throttling of DDoS attacks. We use the sliding mode control (SMC) control theory to formulate and optimize the traffic control conditions for DDoS defense. A cluster-based control model is developed for the environment of an open network at reduced computing cost. The control algorithm is shown to be highly flexible and robust against different types of attack patterns. It can be integrated with different low level detection schemes, so that bandwidth sharing can be implemented using one common framework.

1. Introduction

Distributed denial-of-service (DDoS), since it severely disrupted some public web sites years ago, remains a critical threat to Internet security. By sending a massive amount of packets to a selected target, the DDoS attack is aimed at depleting the computing and communication resources of the victim. The impact of an attack can be classified as disruptive or degrading [6]. It is more difficult to detect a degrading attack than the disruptive one, because it is more difficult to differentiate normal traffic from the hostile traffic when the attack level is low.

Bandwidth depletion can be caused by packet flooding, or by redirect amplification of attack packets. DDoS attacks can be implemented at different protocol levels. In a flooding attack, agents-zombies send large volumes of traffic to the victim to consume the victim system's bandwidth, whereas in amplification attack the broadcast router redirects and amplifies the attack to the victim.

Many *pattern* and *statistics anomaly* based detection techniques have been developed in the literature. The pattern based approach cannot defend the attacks unless the patterns are known *a priori*. The statistics based detection approach needs to effectively manage false alarms, especially when the dynamics of the mixed regular-attack traffic flows are affected by the throttling mechanisms.

In general, normal traffic would be less affected when the DDoS traffic can be contained at proximity of their sources [5]. A prevention based approach using resource accounting was proposed in [18], [19]. Spectral analysis [20], string matching [25], and game theoretic sampling [24], etc. have also been proposed in the literature. The adaptive threshold scheme in [21] measured the mean rate to detect attacks, but it is insensitive to the attacks of low density. Cumulative Sum (Cusum) [21], [23], [28], [29] is a widely adopted algorithm for detection of DDoS traffic. It effectively observes the *change point* of the packet stream to detect DDoS. The hop-count filtering technique [22] utilizes the time-to-live (TTL) value to determine the legitimacy of a packet. This scheme is based on the observation that spoofed IP addresses are generated randomly, thus hard to create the matched TTL value for each of them.

Knowing that attack traffic and normal traffic can be classified into two different types, this idea can be generalized to the notion of ratio-based DDoS detection. Traffic ratio is a good indicator for detection, e.g., MULTOPS [15] albeit it did not consider non-adaptive protocol attacks. The Packet Scores-CLP algorithm [26] used the Conditional Legitimate Probability (CLP) as a score-based filtering approach to throttle packets. By computing the probabilistic distribution of packet attributes during the sampling period, each packet is checked to see if it conforms

to the profile of normal traffic. An attack is detected when changes of the joint distributions of suspicious traffic types exceed some CLP thresholds.

Most detection algorithms are designed for single point detection. When the traffic patterns are stable, a static DDoS detection technique suffices. Without considering the effects of defense mechanisms, the detection scheme may produce excessive false alarms.

Four primary mechanisms have been developed for DDoS defense. *Traceback* provides the victim with the location of the attack source that can be quenched. *Throttling* reduces the suspicious influxes. *Filtering* identifies and prohibits specific types of malicious packets from entering the protected zone, and *reconfiguration* adjusts the network topology to quarantine the attacks. For better performance of defense, the detection and response subsystems should be integrated.

In this paper we propose an area-wide control scheme for ratio based DDoS defense. It is based on a similar observation of the traffic flow imbalance under DDoS attack as the PacketScore, but our approach does not require probabilistic characterization of the traffic flows. To make the solutions practical and robust, we take a non-parametric approach, where the target system is treated as a black box, so that only the system inputs and outputs need to be considered for design of the control system. Based on the Sliding Mode Control (SMC) theory, this scheme can control traffic flows at any protocol layers, because the system under control is treated as a black box. Assuming that a *change point* detection technique such as CuSum is employed, we focus on how to characterize the network dynamics using bandwidth utilization ratio as the control object. The tradeoff between responsiveness and stability of a cluster-based DDoS defense architecture is analyzed.

The remainder of the paper is organized as follows: Section 2 discusses the traffic model and system architecture. Section 3 analyzes the traffic behavior and derives traffic balance equations. Section 4 extends the model from a single node to a cluster and gives an optimal control law aimed at maximizing the total admission ratios. Section 5 gives the simulation results to verify the performance of our control methodology. Section 6 concludes this paper.

2. Ratio-based detection and control of DDoS traffic

Detection and control of DDoS traffic are closely related. Control rules are designed to stabilize the detection and reaction behaviors by packet throttling. An effective detection algorithm must take into account of the queuing and control dynamics when both DDoS attack and its defense function are both engaged. Otherwise, the detection system will tend to give excessive false alarms. And the control decisions need to be made based on detection outcomes, so

that optimal amounts of control adjustment can be delivered to the target system timely.

Ratio based control is not based on direct measurements of the physical system, but based on indirect performance measurements. In formulation of the control objective, we pay attentions to ensure that the optimization process is consistent with the physical phenomenon. The bandwidth ratio can be a real-time time function, or a constant obtained by off-line statistical analysis, and the attribute of the measurement unit can be defined with respect to different protocol layers, or protocol types as needed. The complexity of underlying analysis for multiple flows apparently increases with the number of packet types being controlled. In this work, we only consider a two-traffic-type control problem, which is adequate for defense of DDoS attacks.

Unlike the CLP-based PacketScore that needs continuous update of traffic profile, the ratio-based control is stateless, and distribution free. Ideally, defense of DDoS attack should engage all network nodes to throttle attack traffic, but this is not possible for real world operations. Furthermore, from the analytical viewpoint, it is computationally infeasible to incorporate the dynamics of a large network into one single model in order to solve the stability problem. To balance between solution optimality and practicality, we adopt a *Self-stabilizing Cluster System* (SSC) [1], i.e. Figure 1 as the design basis.

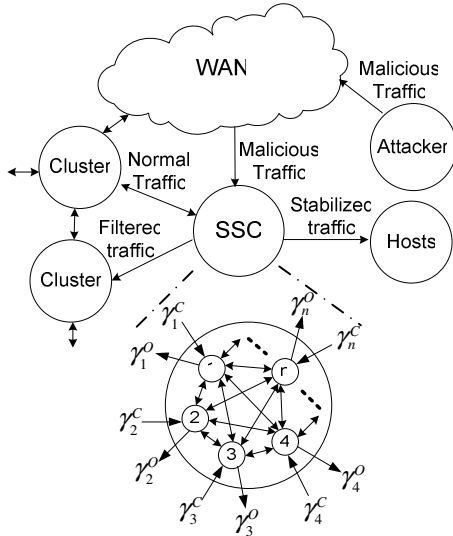


Figure 1. The SSC architecture for defense of DDoS attacks

A network can be divided into an arbitrary number of SSC's. Each cluster is assumed to be independently controlled. Obviously, the effectiveness of DDoS defense is proportional to the number of participating SSCs. In modeling of the control systems, packet traffic is divided into *inter-cluster (external)* and *intra-cluster (internal)* traffic. A cluster is treated as an independent system, where the inter-cluster traffic is the input/output of the system. The sum of external links entering the cluster is treated as one external

variable, so that it is less sensitive to the fluctuation of individual links. Intra-cluster traffic is modeled as system state variables to capture the dynamics of intra-cluster links. This way, it allows easy coupling of clusters, without compromising the accuracy of traffic dynamics.

In this paper, we expand from the threshold based SMC control scheme [1] to a ratio based control scheme. Our work in [1] is a range based control strategy, where traffic rate control is based on an absolute threshold [10], [11]. Unlike packet filtering [7], [8], [9], this technique does not need accurate characterization of the attack traffic, and is consistent with QoS mechanisms [12]. The system dynamics is tailored by the selection of switching function, and its performance is insensitive to parameter and model uncertainty [3].

In this work, we aim at precise control of the bandwidth ratio for two selected traffic types, based on the same traffic model, but a different analysis and optimization approach. The optimization process pays explicit attention to protection of other resources in throttling of hot traffic.

2.1 Full cluster control model

Our node model for defense of DDoS attacks is applicable to sources, targets, or the intermediate network nodes. Traffic under control is divided into two types, and each packet type is allowed to consume up to a fixed ratio of the total capacity. Our first goal is to minimize the impact of DDoS attack within the cluster. As a result, we throttle the inbound traffic to maintain the ratio between traffic types to the target value. Without loss of generality, we assume that the topology in a cluster is a bilateral, fully connected graph consisting of n nodes. If the link between node i and j does not exist, we can simply set throttle variable ρ_{ij} of link L_{ij} to zero in our model.

Nodes in a cluster that need to have more close interactions with another cluster are called edge nodes. Edge nodes can be assigned to the cluster as needed. Nodes that are isolated from other nodes are called inner nodes. An illustration of node N_j and traffic is shown in Figure 2, with their notations given in Table 1. Similar to the node model given in [1], [2], our node model can be applied to local hosts or external nodes.

Table 1. Notations used throughout the node model

symbol	definition
λ_j^{Tk}	The total rate of type k traffic entering N_j
λ_{ij}	The rate of internal traffic from N_i to N_j
λ_{ij}^{IN}	The rate of dispatched traffic in N_i to N_j
λ_{ij}^{Tk}	The internal traffic rate of type k from N_i to N_j
$\gamma_j^{C.Tk}$	The external traffic rate of type k entering N_j

$\gamma_j^{O, Tk}$	The external traffic rate of type k leaving N_j
γ_j^{IN}	The dispatched traffic rate in N_j to the external link
L_j	Outbound inter-cluster link leaving N_j
L_{ij}	One-way intra-cluster link from N_i to N_j
μ_{ij}	The bandwidth of L_{ij}
ρ_{ij}	The throttle level to traffic λ_{ij}^{IN}
φ_j	The throttle level to traffic γ_j^{IN}
X_{ij}^{Tk}	The queue length of type k traffic on link L_{ij}
X_j^{Tk}	The queue length of type k traffic on link L_j
$G_{ij}^{Tk}(X_{ij}^{Tk})$	Utility function for outbound traffic of type k on L_{ij}
$H_{ij}^{Tk}(X_{ij}^{Tk})$	Rejected ratio of outbound traffic $\mu_{ij} * G_{ij}^{Tk}(X_{ij}^{Tk})$
α_{ij}^{Tk}	The percentile of λ_j^{Tk} dispatched to L_{ij}
α_j^{Tk}	The percentile of λ_j^{Tk} dispatched to the external link

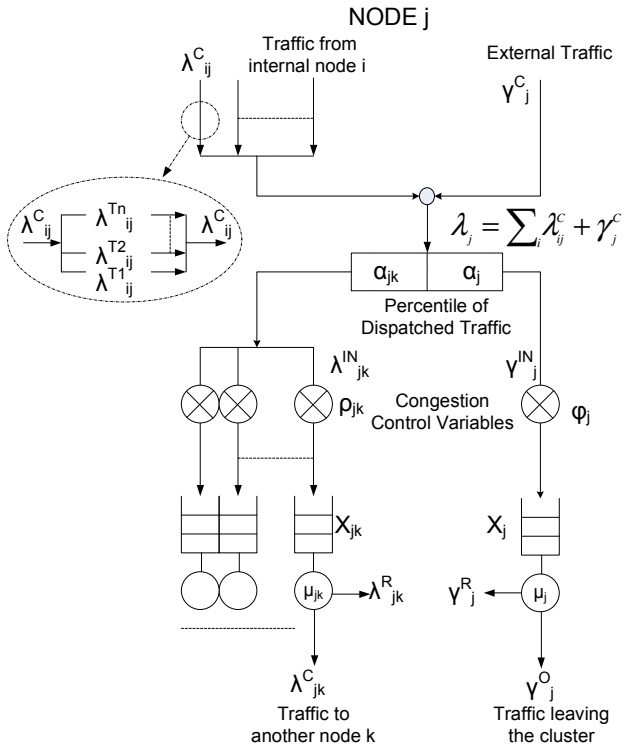


Figure 2. The General Traffic model in a node

3. Balance equations in a node

On the basis of the traffic model, we now discuss the relationship between traffic flows based on four aspects:

packet throttling, intra-cluster routing, queuing dynamics, and traffic output.

3.1 Throttling

For node N_j , λ_{ij}^C and γ_j^C are inbound traffic from other internal and external nodes, respectively, and the total traffic entering the node is expressed in ((3.1). Congestion control is accomplished through adjusting throttling variables ρ_{ij} and φ_j . The subscript for each symbol denotes a link from a sender to a receiver.

$$\lambda_j = (\sum_i \rho_{ij} \lambda_{ij}^C) + \varphi_j \gamma_j^C = \Phi \Lambda = \sum_i \lambda_{ij}^{IN,C} + \gamma_j^{IN,C} \quad (3.1)$$

where $\rho_{ij} \in [0, 1]$, $\varphi_j \in [0, 1]$, $\Phi = [\rho \varphi]$, and $\Lambda = [\lambda^C \gamma^C]^T$. Both Φ and Λ are rank-one matrices. If N_j does not have inputs from external links, then φ_j is equal to 0. Symbols λ and γ respectively denote the intra-cluster and inter-cluster traffic, and $\lambda_{ij}^{IN,C}$ and $\gamma_j^{IN,C}$ in (3.1) are packet rates after throttling is in effect.

Packet flows closely affect one another in a cluster, especially when the DDoS attack is active. The relationship between these packet flows is one of the most important indicators for detection of DDoS attack. To represent the relationship between these traffic flows, we use λ_{jk}^{Ti} and γ_j^{Ti} to indicate these types in the link. Their relationship is defined in (3.2).

$$\begin{aligned} \lambda_j(t) &\triangleq \sum_i \lambda_j^{Ti}(t) \\ \gamma_j(t) &\triangleq \sum_i \gamma_j^{Ti}(t) \end{aligned} \quad (3.2)$$

3.2 Packet routing

In a cluster, packets are routed to different outbound paths based on their destination addresses. (3.3) is used to represent the routing relationship between different paths. Here, α_{jk}^{Ti} and α_j^{Ti} are ratios of the input traffic dispatched to other intra-cluster nodes and the external, respectively.

$$\begin{aligned} \lambda_{jk}^{IN,Ti}(t) &\triangleq \alpha_{jk}^{Ti} * \lambda_j^{Ti}(t) \\ \gamma_j^{IN,Ti}(t) &\triangleq \alpha_j^{Ti} * \lambda_j^{Ti}(t) \\ (\sum_k \alpha_{jk}^{Ti}) + \alpha_j^{Ti} &= 1 \end{aligned} \quad (3.3)$$

When $\alpha_j = 0$ it means that a node is not connected to the external link.

3.3 Queuing dynamics

The outbound traffic of a link is a function of its queue length. When the buffer is empty, the departure rate is equal to the arrival rate. When the buffer is not empty, the maximum output rate is upper bounded by the link capacity, and the change rate of queue length is equal to the difference between the output and input rates.

$$\begin{aligned} \dot{X}_k^n(t) &= \lambda_k^n(t) - G_k^n(X_k^n) * \mu_k(t) \\ 0 &\leq \sum_i G_i^n \leq 1 \end{aligned} \quad (3.4)$$

3.4 Output traffic

When the network traffic is heavy, packets would be dropped based on the control laws (3.5). Let $H(\cdot)$ denote the drop rate of the outbound traffic, (3.6) represents the dropped traffic and (3.7) the actual sending rate of the output link to internal nodes.

$$G_k^n(X_k^n(t)) * \mu_k(t) = \lambda_k^{r,n}(t) + \lambda_k^{c,n}(t) \quad (3.5)$$

$$\lambda_k^{r,n}(t) = H_k^n(X_k^n(t)) * G_k^n(X_k^n(t)) * \mu_k(t) \quad (3.6)$$

$$\begin{aligned} \lambda_k^{c,n}(t) &= (1 - H_k^n(X_k^n(t))) * G_k^n(X_k^n(t)) * \mu_k(t) \\ &\triangleq \hat{G}_k^n(X_k^n(t)) * \mu_k(t) \end{aligned} \quad (3.7)$$

(3.8) denotes the actual output rate of the external link.

$$\begin{aligned} \gamma_j^{o,n}(t) &= (1 - H_j^n(X_j^n(t))) * G_j^n(X_j^n(t)) * \mu_j(t) \\ &\triangleq \hat{G}_j^n(X_j^n(t)) * \mu_j(t) \end{aligned} \quad (3.8)$$

Substitute (3.1) into (3.4), we get queue length change on the intra-cluster link in (3.9).

$$\begin{aligned} \dot{X}_k^n(t) &= -\mu_k(t) G_k^n(X_k^n) \\ &\quad + \alpha_k^n * [(\sum_i \rho_i^n \lambda_i^{c,n}) + \varphi_j^n \gamma_j^{c,n}] \end{aligned} \quad (3.9)$$

Similarly, the queue length change on the inter-cluster link can be expressed as below.

$$\begin{aligned} \dot{X}_j^n(t) &= -\mu_j(t) G_j^n(X_j^n) \\ &\quad + \alpha_j^n * [(\sum_i \rho_i^n \lambda_i^{c,n}) + \varphi_j^n \gamma_j^{c,n}] \end{aligned} \quad (3.10)$$

4. Simplified cluster traffic model

The complete cluster control model is a reference to characterize the cluster dynamics comprehensively. To reduce the computing cost, we propose a simplified model in Figure 3 for cluster analysis. We will use a 3-node cluster to make an in-depth study, and the result can be easily modified for different cluster sizes. We assume that no throttling between intra-cluster nodes, i.e. $\rho_{ij}^{rn} = 1 \forall k \in N$. For a three-node cluster, every node is considered intra-clustered, thus

they do not block one another, but handle external DDoS attack together.

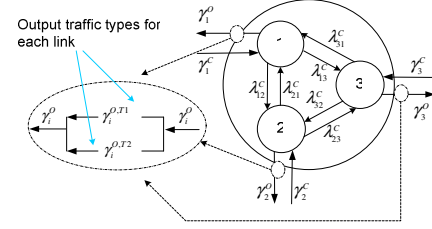


Figure 3. A reduced traffic model for a cluster

Let T_1 and T_2 denote the two types of packet types being controlled on each link, to control their admission ratio, the control object is defined as $\sum_{i=1}^3 \gamma_i^{o,T1} / \sum_{i=1}^3 \gamma_i^{o,T2} = p(t)$, where $p(t)$ is a function that can be represented by spline, wavelet analysis, or other statistical techniques. For simplicity, we assume that $p(t)$ is known. For any node in a cluster, the number of equations is equal to the number of outbound links multiplied by the number of traffic types. For a 3-node cluster, we get six equations for each node. Due to the symmetric topology of the cluster, we just need to analyze one node. Balance equations of other nodes can be derived in a similar manner. For node 1, the equilibrium equations are:

$$\begin{aligned} \dot{x}_{12}^{T1} &= -\mu_{12} G_{12}^{T1} + \alpha_{12}^{T1} (\gamma_1^{c,T1} + \mu_{21} \hat{G}_{21}^{T1} + \mu_{31} \hat{G}_{31}^{T1}) \\ \dot{x}_{12}^{T2} &= -\mu_{12} G_{12}^{T2} + \alpha_{12}^{T2} (\gamma_1^{c,T2} + \mu_{21} \hat{G}_{21}^{T2} + \mu_{31} \hat{G}_{31}^{T2}) \\ \dot{x}_{13}^{T1} &= -\mu_{13} G_{13}^{T1} + \alpha_{13}^{T1} (\gamma_1^{c,T1} + \mu_{21} \hat{G}_{21}^{T1} + \mu_{31} \hat{G}_{31}^{T1}) \\ \dot{x}_{13}^{T2} &= -\mu_{13} G_{13}^{T2} + \alpha_{13}^{T2} (\gamma_1^{c,T2} + \mu_{21} \hat{G}_{21}^{T2} + \mu_{31} \hat{G}_{31}^{T2}) \\ \dot{x}_1^{T1} &= -\mu_1 G_1^{T1} + \varphi_1^{T1} \alpha_1^{T1} (\gamma_1^{c,T1} + \mu_{21} \hat{G}_{21}^{T1} + \mu_{31} \hat{G}_{31}^{T1}) \\ \dot{x}_1^{T2} &= -\mu_1 G_1^{T2} + \varphi_1^{T2} \alpha_1^{T2} (\gamma_1^{c,T2} + \mu_{21} \hat{G}_{21}^{T2} + \mu_{31} \hat{G}_{31}^{T2}) \end{aligned} \quad (4.1)$$

These flow balance equations are similar to those derived in [1], [2] except that throttle variables are moved from input flows to the front of the queue to reduce the effect of packet dispatch. Next, we discuss the new control law to control the ratio between two traffic types.

4.1 The ratio control problem

To reduce the impact of short-term traffic fluctuation, we take the moving average of most recent packets as measured variables of the control and detection system. Knowing that one cannot predict the stochastic behavior of flows, asymptotical control of the ratio is more effective than instantaneous control. Otherwise, any control rule is subject to spontaneous crash due to random inputs. The SMC system consists of *linear* and *switched* laws. The linear control law is derived from the *equivalent control*, which controls the input after it is filtered by a low pass filter. It is based on a continuous control model once the state reaches the switching manifold $s(t)=0$, where $s(t)$ denotes the switching function, one of the important components in SMC. The

construction of the switching function is based on the expected output and the relative degree of the system dynamics. Recall that our control objective is to keep the ratio of two traffic types to a specified value. (4.2) depicts that our goal y is to control the traffic rate of two types to a ratio p . i.e. y is minimized when the ratio of two packet flow types is equal to the specified ratio:

$$\begin{aligned} \gamma_i^{o,T1} &= \mu_i \hat{G}_i^{T1} \text{ (outputrate of type1 in link i)} \\ \gamma_i^{o,T2} &= \mu_i \hat{G}_i^{T2} \text{ (outputrate of type2 in link i)} \\ y &= \sum_{i=1}^3 \gamma_i^{o,T1} - p \sum_{i=1}^3 \gamma_i^{o,T2} \end{aligned} \quad (4.2)$$

where p is the ratio of two traffic types.

In addition, the relative degree of a system is r when the input variable appears after the output function y is differentiated r times [13], [14]. Then we can construct the switching function of an r -degree system using the following equation $s = \sum_{i=0}^{r-2} c_i y^{(i)} + y^{(r-1)}$ [1]. In our model, the relative degree is one, because by (4.3) it shows that the control variable ϕ_i^{Tj} appears after output variable $\gamma_i^{o,Tj}$ is differentiated one time, where $i \in \{1,2,3\}$ and $j \in \{1,2\}$.

$$\begin{aligned} \dot{\gamma}_i^{o,Tj} &= (\mu_i \hat{G}_i^{Tj})' = \mu_i \frac{\partial \hat{G}_i^{Tj}}{\partial x_i^{Tj}} \dot{x}_i^{Tj} = \\ &\mu_i \frac{\partial \hat{G}_i^{Tj}}{\partial x_i^{Tj}} (-\mu_i G_i^{Tj} + \phi_i^{Tj} \alpha_i^{Tj} (\gamma_i^{c,Tj} + \mu_{ki} \hat{G}_{ki}^{Tj} + \mu_{mi} \hat{G}_{mi}^{Tj})) \end{aligned} \quad (4.3)$$

Therefore the switching function used in our cluster model is expressed in (4.4).

$$s = y = \sum_{i=1}^3 \gamma_i^{o,T1} - p \sum_{i=1}^3 \gamma_i^{o,T2} \quad (4.4)$$

Furthermore, we derive the equivalent control law by taking the first derivative of $s(t)$ to be zero. In doing so, we plug (4.4) along with (4.1) into $\dot{s}(t)$ and then obtain (4.5).

$$\begin{aligned} \dot{s}(t) &= (\sum_{i=1}^3 \dot{\gamma}_i^{o,T1} - p \sum_{i=1}^3 \dot{\gamma}_i^{o,T2} - \dot{p} \sum_{i=1}^3 \gamma_i^{o,T2}) \\ &= C^T \Phi + D \end{aligned} \quad (4.5)$$

$C = [C_1, C_2, C_3, C_4, C_5, C_6]^T$ $\Phi = [\phi_1^{T1}, \phi_2^{T1}, \phi_3^{T1}, \phi_1^{T2}, \phi_2^{T2}, \phi_3^{T2}]^T$, where Φ is a control vector that contains all admission variables. The elements of vector C and D are respectively expressed in (4.6) and (4.7)

$$\begin{aligned} C_1 &= \mu_1 \frac{\partial \hat{G}_1^{T1}}{\partial x_1^{T1}} \alpha_1^{T1} (\gamma_1^{c,T1} + \mu_{21} \hat{G}_{21}^{T1} + \mu_{31} \hat{G}_{31}^{T1}) \\ C_2 &= \mu_2 \frac{\partial \hat{G}_2^{T1}}{\partial x_2^{T1}} \alpha_2^{T1} (\gamma_2^{c,T1} + \mu_{12} \hat{G}_{12}^{T1} + \mu_{32} \hat{G}_{32}^{T1}) \\ C_3 &= \mu_3 \frac{\partial \hat{G}_3^{T1}}{\partial x_3^{T1}} \alpha_3^{T1} (\gamma_3^{c,T1} + \mu_{13} \hat{G}_{13}^{T1} + \mu_{23} \hat{G}_{23}^{T1}) \\ C_4 &= -p \mu_1 \frac{\partial \hat{G}_1^{T2}}{\partial x_1^{T2}} \alpha_1^{T2} (\gamma_1^{c,T2} + \mu_{21} \hat{G}_{21}^{T2} + \mu_{31} \hat{G}_{31}^{T2}) \\ C_5 &= -p \mu_2 \frac{\partial \hat{G}_2^{T2}}{\partial x_2^{T2}} \alpha_2^{T2} (\gamma_2^{c,T2} + \mu_{12} \hat{G}_{12}^{T2} + \mu_{32} \hat{G}_{32}^{T2}) \\ C_6 &= -p \mu_3 \frac{\partial \hat{G}_3^{T2}}{\partial x_3^{T2}} \alpha_3^{T2} (\gamma_3^{c,T2} + \mu_{13} \hat{G}_{13}^{T2} + \mu_{23} \hat{G}_{23}^{T2}) \end{aligned} \quad (4.6)$$

and

$$\begin{aligned} D &= \mu_1 \frac{\partial \hat{G}_1^{T1}}{\partial x_1^{T1}} (-\mu_1 G_1^{T1}) + \mu_2 \frac{\partial \hat{G}_2^{T1}}{\partial x_2^{T1}} (-\mu_2 G_2^{T1}) \\ &+ \mu_3 \frac{\partial \hat{G}_3^{T1}}{\partial x_3^{T1}} (-\mu_3 G_3^{T1}) - p \mu_1 \frac{\partial \hat{G}_1^{T2}}{\partial x_1^{T2}} (-\mu_1 G_1^{T2}) \\ &- p \mu_2 \frac{\partial \hat{G}_2^{T2}}{\partial x_2^{T2}} (-\mu_2 G_2^{T2}) - p \mu_3 \frac{\partial \hat{G}_3^{T2}}{\partial x_3^{T2}} (-\mu_3 G_3^{T2}) \\ &- \dot{p} (\mu_1 \hat{G}_1^{T2} + \mu_2 \hat{G}_2^{T2} + \mu_3 \hat{G}_3^{T2}) \end{aligned} \quad (4.7)$$

4.2 Optimization of equivalent control law

When $\dot{s}(t) = 0$, the equivalent control vector $\hat{\Phi}_{eq} = [\hat{\phi}_1^{T1}, \hat{\phi}_2^{T1}, \hat{\phi}_3^{T1}, \hat{\phi}_1^{T2}, \hat{\phi}_2^{T2}, \hat{\phi}_3^{T2}]$ can be obtained as the optimized solution of the continuous component by solving (4.8). As a heuristic choice, our objective is to maximize the admission variables (1: all packets accepted, 0: no packets accepted), which is subject to two constraints. Firstly, $\dot{s}(t) = 0$ is a necessary condition to derive the equivalent control law. Secondly, the values of admission variables must fall within the range 0 to 1. This can be modeled as a linear optimization problem where the objective function is a linear combination of all input variables. In summary, we formalize this problem to (4.8).

$$\begin{aligned} &\text{Maximize } \sum_{m=1}^6 \Phi[m] \\ &\text{Subject to } \begin{cases} C^T \Phi + D = 0, & i \in \{1,2,\dots,6\}, \\ \Phi[i] \in [0, 1] \end{cases} \end{aligned} \quad (4.8)$$

(4.8) can be solved by using linear programming solvers, such as Matlab optimization toolbox [16] or Ip solver [17]. To guarantee the value of the final controlled throttle variable within 0 and 1, we will adaptively adjust parameters of the switched component for maintaining the control law within a sensible range, as it will be explained shortly.

For the control object to reach its equilibrium, i.e., the expected bandwidth ratio between the two traffic types, one

must drive the control dynamics from any initial state to the *sliding mode*, and make it stay on the switching surface $s(t)=0$. The η -reachability condition $s(t)\dot{s}(t) \leq -\eta|s|$ guarantees that $s(t) = 0$ as $t \rightarrow \infty$ [3][4]. To satisfy this condition and to reduce system uncertainties, the control law (4.9) combines $\hat{\varphi}_i^{Tm}$ with discontinuous component $k_i^{Tm} \text{sgn}(s)$, where $m \in \{1,2\}$ and $i \in \{1,2,\dots,6\}$, when applying the trajectory of $s(t)$ onto the sliding surface.

Next, we discuss the control law of SSC for stabilizing the ratio of two traffic types. Construction of the control law is based on the theory in [3] [27], for $i \in \{1,2,3\}$,

$$\begin{cases} \varphi_i^{T1} = \hat{\varphi}_i^{T1} - k_i^{T1} \text{sgn}(s) \\ \varphi_i^{T2} = \hat{\varphi}_i^{T2} + k_i^{T2} \text{sgn}(s) \end{cases} \quad (4.9)$$

where k_i^{T1} and k_i^{T2} are design parameters and $\text{sgn}(\cdot)$ is the signum function defined as $s * \text{sgn}(s) = |s|$. Note that the sign of the switched component of the control law in two traffic types is opposite for driving the traffic ratio to the target value rapidly. By substituting control law (4.2) into (4.9), we can prove that the trajectory of s will converge to the switching manifold $s(t) = 0$. The control law satisfies the η -reachability condition because $s(t)\dot{s}(t) = -(\sum_{i=1}^6 k_i^{T1} + p \sum_{i=1}^6 k_i^{T2})|s| \leq -\eta|s|$, where $\eta > 0$. This is a stronger condition than the right hand side to be zero because it guarantees that the output trajectory will reach the switching surface within a finite time, not infinite.

5. Design and Simulation

5.1 Design of adaptive parameters K_i^{T1} and K_i^{T2}

We need to design k_i^{T1} and k_i^{T2} in (4.9) such that the admission level of a traffic type falls within the range of [0, 1]. Two cases, $\text{sgn}(s) > 0$ and $\text{sgn}(s) < 0$, need to be carefully considered. We first analyze k_i^{T1} , and then k_i^{T2} based on its complementary property with respect to k_i^{T1} .

Case 1: $\text{sgn}(s) > 0$, i.e. $\varphi_i^{T1} = \hat{\varphi}_i^{T1} - k_i^{T1}$

$$\begin{cases} \text{condition 1: } 0 \leq \varphi_i^{T1} \leq 1 \Rightarrow \hat{\varphi}_i^{T1} \geq k_i^{T1} \geq \hat{\varphi}_i^{T1} - 1 \\ \text{condition 2: } k_i^{T1} > 0 \end{cases}$$

In order to satisfy both conditions, k_i^{T1} must be within the range of 0 and $\hat{\varphi}_i^{T1}$ i.e. $k_i^{T1} \in (0, \hat{\varphi}_i^{T1}]$, so that $0 \leq \varphi_i^{T1} \leq 1$. As a heuristic choice, we expect the switched component adaptive and proportional to the equivalent control $\hat{\varphi}_i^{T1}$ i.e., $k_i^{T1} = k * \hat{\varphi}_i^{T1}$, where $k \in (0,1]$ is called the *range parameter* that defines the dynamic range of the control actions.

Case 2: $\text{sgn}(s) < 0$, i.e. $\varphi_i^{T1} = \hat{\varphi}_i^{T1} + k_i^{T1}$

$$\begin{cases} \text{condition 1: } 0 \leq \varphi_i^{T1} \leq 1 \Rightarrow -\hat{\varphi}_i^{T1} \leq k_i^{T1} \leq 1 - \hat{\varphi}_i^{T1} \\ \text{condition 2: } k_i^{T1} > 0 \end{cases}$$

Again, these two conditions dictate the range of k_i^{T1} so that $k_i^{T1} \in (0, 1 - \hat{\varphi}_i^{T1}]$. Let k_i^{T1} be the ratio of $1 - \hat{\varphi}_i^{T1}$, then $k_i^{T1} = k * (1 - \hat{\varphi}_i^{T1})$, where $k \in (0,1]$. In summary, (5.1) represents our design for adaptive selection of the parameters.

$$\begin{cases} \text{sgn}(s) > 0 \Rightarrow k_i^{T1} = k * \hat{\varphi}_i^{T1}, k_i^{T2} = k * (1 - \hat{\varphi}_i^{T2}) \\ \text{sgn}(s) < 0 \Rightarrow k_i^{T1} = k * (1 - \hat{\varphi}_i^{T1}), k_i^{T2} = k * \hat{\varphi}_i^{T2} \end{cases} \quad (5.1)$$

where $k \in (0,1]$ and $i \in \{1,2,3\}$.

5.2 Experiment evaluation

We evaluated the performance of our scheme using simulation. In the first experiment, we regard the whole cluster as the control object, without considering states of individual links. The target ratio of two traffic types in a 3-node cluster is set to be 0.5 for the whole cluster, without considering individual links. That is, the bandwidth utilization of type 1 traffic should be half of that of type 2 traffic at the three output links of the cluster. In the simulation, packets have the same size, and the bandwidth of each link is equal to 10^5 packets/sec. External traffic sources are randomly generated using six independent random number generators. The ingressive packet rate is bounded between $[0.7-1.3] * 10^4$ for node 1, $[0-1] * 10^4$ for node 2, and $[0.5-2] * 10^4$ for node 3. Packets have random paths, but a packet must leave the cluster after it visited all nodes. Packet throttling is based on (4.9), where $\hat{\varphi}_i^{T1}$ and $\hat{\varphi}_i^{T2}$ are derived by using (4.8), and k_i^{T1} and k_i^{T2} are calculated using (5.1). The range parameter k is set to be 0.6 in the whole study. By plugging the value of above parameters into (4.9), we obtain the computed admission rate φ_i^{T1} and φ_i^{T2} used for the current controlling decisions. The simulation results are given in Figure 4 and Figure 5, respectively, where in Figure 4 the ratio of the total output rates between type-1 and type-2 traffic is about 50%, with some instantaneous fluctuation. However, considering the cumulative ratios between the two types of traffic, the control performance appears to be right on target, i.e., 50%, except for the short initial period, see Figure 5.

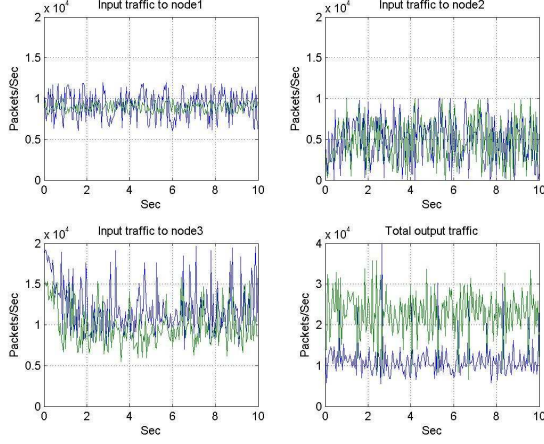


Figure 4. Input and output traffic traces in each node

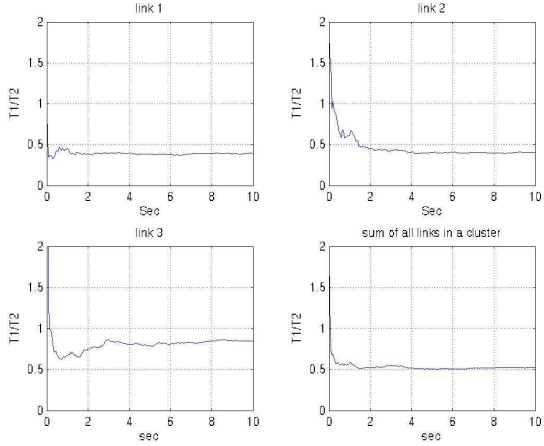


Figure 5. The cumulative ratio of traffic types in the cluster

5.3 Control of single link

In the second experiment, we treated each link as an independent control system, using slightly modified control rules. For the external (outbound) link of node i , $s_i = \gamma_i^{O,T1} - p_i \gamma_i^{O,T2}$ is the switching function for the link to maintain the traffic ratio, and then we use (4.9) for obtaining the control law. The switching function S in (4.9) is replaced by s_i , which means the control goal is determined by the independent link. Similarly, we also use s_i instead of S in (5.1) to acquire k_i^{T1} and k_i^{T2} . For obtaining the optimized admission rate $\hat{\Phi}_{eq}$, we rewrite (4.5)-(4.7) as (5.2) for each link.

$$\begin{aligned} \dot{s}_i(t) &= E_i \Phi + F_i \\ E_i &= [C_i \ C_{i+3}] \\ \hat{\Phi}_i &= [\hat{\phi}_i^{T1}, \hat{\phi}_i^{T2}] \\ F_i &= \mu_i \frac{\partial \hat{G}_i^{T1}}{\partial x_i^{T1}} (-\mu_i G_i^{T1}) - p_i \mu_i \frac{\partial \hat{G}_i^{T2}}{\partial x_i^{T2}} (-\mu_i G_i^{T2}) \end{aligned} \quad (5.2)$$

where C is defined in (4.6), $\hat{\phi}_i^{T1}$ and $\hat{\phi}_i^{T2}$ are defined in (4.8) and $i \in \{1, 2, 3\}$. Hence, $\hat{\Phi}_{eq}$ can be computed by plugging parameters of (5.2) into (4.8) to obtain its optimal value. After receiving $\hat{\Phi}_{eq}$, k_i^{T1} and k_i^{T2} , we can substitute them into the modified (4.9) and then secure admission variables φ_i^{T1} and φ_i^{T2} .

The first row of Figure 6 shows the instantaneous measurement of traffic ratios on the three links. The second row of Figure 7 shows that when taking cumulative average of the traffic ratio, it asymptotically converges to the target value 0.5.

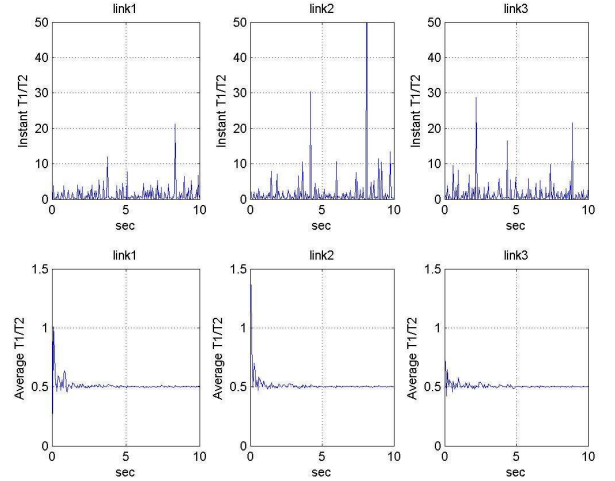


Figure 6. Traffic ratio control to inter-cluster links

We note that a larger value of range parameter k lowers the chance of saturating the controller, but it comes at a price of high level of oscillation. Figure 7 shows the time trace of the admission levels, in terms of the percentile of inbound packets, based on the second experiment. Given the cluster traffic inputs, the control system, the controller adjusts the throttling/admission levels dynamically.

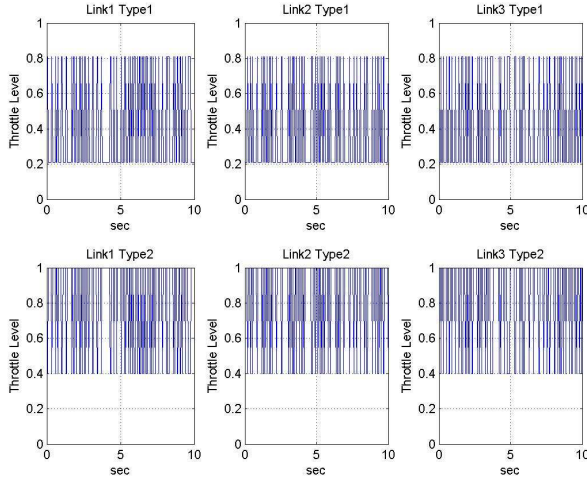


Figure 7. Admission levels on each link for each type when $k = 0.6$ and target traffic ratio is 0.5

5.4 Pushback using admission indicator

Admission level is designed for direct traffic throttling in the two experiments mentioned above. It was found that the admission level is also an effective indicator for detection of traffic ratio changes. We can use them to notify upstream packet sources to throttle their outbound traffic, based on the pushback concept mechanism [30] [31]. The source uses a *multiple-increase-multiple-decrease* (MIMD) rule to adjust its packet flow increase or decrease ratio based on the feedback signals. That is, given the current traffic level μ at each adjustment, the traffic flow increases to $(1+c)\mu$ or decreases to $(1-c)\mu$, where c is a constant. Figure 8 and Figure 9 describe the algorithm corresponding to the cluster and source respectively. Here, adm_type1_linkq denotes the expected admission level of traffic type 1 in outbound link q , and $score(.)$ is a user-designed routine using admission levels of same type as arguments for computing and performing binary traffic pushback. In our simulation, we set $r1=1.1$ and $r2=0.8$, where type-1 traffic is adjusted in sources according to the signal from the cluster, and type-2 traffic is assumed to be a reliable one that need not be adjusted. Figure 10 shows the time traces of the traffic sources after the control is applied, where the controlled traffic has the large yet relatively slow swinging shapes. The cluster admission levels under this control scheme are plotted in Figure 11, and the ratio between the two types of traffic is plotted in Figure 12. Comparing to plots in Figure 5 and Figure 12, the new results have slightly degraded yet excellent asymptotic stability. The ratio between type1 and type2 traffic still converges to the target value 0.5.

```

cluster_algo
for each sampling time
  if score(adm_type1_linkq) >= score(adm_type2_linkq)
    where q ∈ {1,2,3}
  then
    signal = 1
  else
    signal = 0
  send(signal)

```

Figure 8. Control algorithm used in the cluster

```

source_algo
for every fixed period
  receive(signal)
  if (signal)
  then
    rate(type1) = rate(type1) * r1, where r1 > 1
  else
    rate(type1) = rate(type1) * r2, where r2 ∈ [0,1)

```

Figure 9. MIMD algorithm used at the source

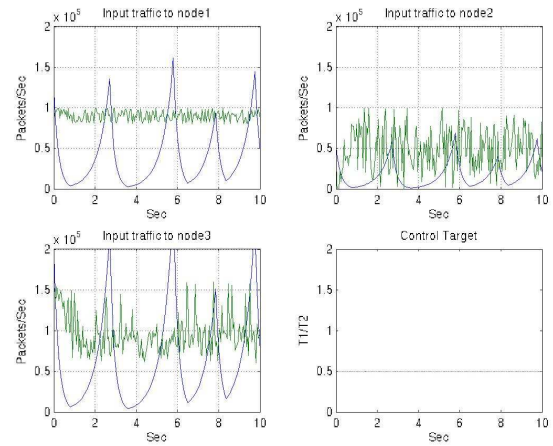


Figure 10. Source control using pushback

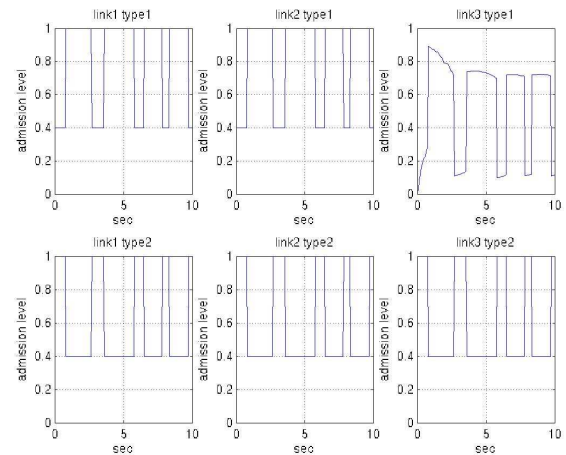


Figure 11. Cluster admission levels for type-1 and -2 traffic

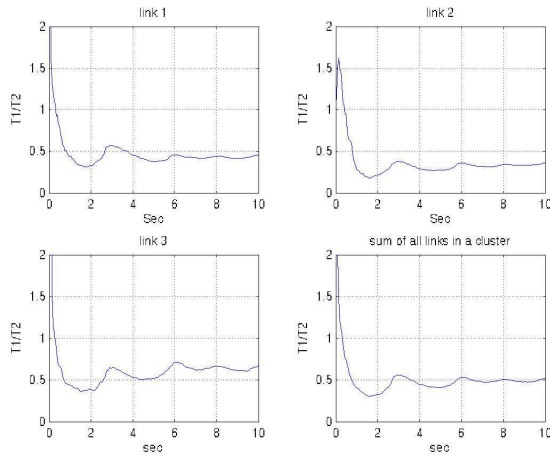


Figure 12. The ratios of two traffic types on each link, and for the whole cluster, when the target value is 0.5

6. Conclusion

In this paper, we proposed a ratio based model using SMC for detection and control of DDoS attack. To solve this multiple input, single output system, we applied both control theory and linear optimization techniques to derive the ratio control laws. Knowing that the admission level is a relative measurement, the switched component of the control law is made adaptive according to the current throttling ratio. We derived the feasibility criteria for design of the adaptive switched law, and guaranteed the range of control variables to satisfy their constraints.

Our design is simple, and can be applied to different levels of control. The cluster level control has excellent asymptotic stability in converging to the target ratio value. It was modified for independent link level control to achieve similar performance. When the admission level of the cluster is used as a DDoS detection indicator for sources, we also achieve similar performance with some expected slight degradation in stability. It is well known that delay is a major concern for any feedback control systems [32], [33], [34]. We tested but did not report the effect of delays due to space limit. It was found that the control performance remains highly stable when the delay is as high as one second or more, more than enough to address the cross US continent delays in most cases.

References

- [1] Yong Xiong, S. Liu, P. Sun, "On the defense of the distributed denial of service attacks: an on-off feedback control approach", *IEEE Transactions on Systems, Man, and Cybernetics, Part A* 31(4), 2001, pp. 282-293.
- [2] Janusz Filipiak, *Modeling and Control of Dynamic Flows in Communication Networks*, Springer-Verlag, Berlin Heidelberg, 1988.
- [3] C. Edwards and S. K. Spurgeon, *Sliding Mode Control - Theory and Applications*, Taylor & Francis Inc, Bristol, PA, 1998.
- [4] Jean-Jacques Slotine and Weiping Li. *Applied Nonlinear Control*. Prentice Hall, Englewood Cliffs, N.J. 1991.
- [5] J. Mirkovic, G. Prier, P. Reiher, "Source-end DDoS defense", *In Proceedings of Second IEEE International Symposium on Network Computing and Applications*, April 2003.
- [6] Jelena Mirkovic and Peter Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms", *ACM SIGCOMM Computer Communication Review*, Volume 34, Issue 2, 2004, pp. 39 - 53.
- [7] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial-of-service Attacks which employ IP Source Address Spoofing", <http://www.ietf.org/rfc/rfc2827.txt>, 2000.
- [8] J. Li, J. Mirkovic, M. Wang, P. Reiher, and L. Zhang, "SAVE: Source Address Validity Enforcement Protocol," *In Proceedings of IEEE Infocom*, 2002.
- [9] K. Park and H. Lee. "On the Effectiveness of Router-based Packet Filtering for Distributed DoS Attack Prevention in Power-law Internets", *In Proceedings of ACM SIGCOM 2001*, pp. 15-26.
- [10] J. Ioannidis and S. M. Bellovin, "Implementing Pushback: Router-Based Defense against DDoS Attacks", *In Proceedings of ISOC Network and Distributed System Security Symposium (NDSS)*, 2002.
- [11] R. Mahajan, M. Bellovin, S. Floyd, V. Paxson, and S. Shenker, "Controlling high bandwidth aggregates in the network", *ACM Computer Communications Review*, 32(3), July 2002.
- [12] Jiejun Kong, M. Mirza, J. Shu, C. Yoedhana, M. Gerla and Songwu Lu. "Random flow network modeling and simulations for DDoS attack mitigation", *In the Proc. of IEEE International Conference on Communications, Volume: 1, 11-15*, May 2003, pp. 487 - 491.
- [13] A. Isodori, *Lecture Notes on Nonlinear Control (Notes for a Course at the Carl Cranz Gesellschaft)*, Aug 1987.
- [14] A. Isodori, *Nonlinear Control Systems: An Introduction*, Springer-Verlag, New York, 1989.
- [15] T. M. Gil and M. Poletto. "MULTOPS: a data-structure for bandwidth attack detection", *In Proceedings of 10th Usenix Security Symposium*, August 2001.
- [16] Matlab. <http://www.mathworks.com/products/optimization/>.
- [17] lp_solve. ftp://ftp.ics.ele.tue.nl/pub/lp_solve/.
- [18] A. Garg and A.L.N. Reddy. "Mitigation of DoS attacks through QoS Regulation", *In Proceedings of IWQOS workshop*, May 2001
- [19] F. Lau, S. H. Rubin, M. H. Smith, and L. "Trajkovic. Distributed Denial of Service Attacks", *In IEEE International Conference on System, Man and Cybernetics*, Nashville, TN, USA, October 2000, pp. 2275-2280.
- [20] Alefiya Hussain, John Heidemann, and Christos Papadopoulos, "A Framework for Classifying Denial of Service Attacks", *In Proceedings of ACM SIGCOMM 2003*, Karlsruhe, Germany, 2003.
- [21] V. Siris & F. Papagalou, "Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks", *In Proceedings of IEEE Global Telecommunications Conference (Globecom 2004)*, Dallas, USA, 2004.
- [22] Cheng Jin, Haining Wang, and Kang G. Shin, "Hop-Count Filtering: An Effective Defense against Spoofed Traffic", *In Proceedings of the 10th ACM conference on Computer and*

- Communication Security*, Washington D.C., USA, 2003, pp. 30 – 41.
- [23] H. Wang, D. Zhang, and Kang G. Shin, “Detecting SYN Flooding Attacks”, *In Proceedings of IEEE Conference on Computer Communications*, New York, June 2002.
 - [24] Murali Kodialam, T.V. Lakshman. “Detecting Network Intrusions vis Sampling: A Game Theoretic Approach”, *In proceedings of IEEE Conference on Computer Communications*. San Francisco, March 2003.
 - [25] N. Tuck, T. Sherwood, B. Calder, and G. Varghese. “Deterministic Memory-Efficient String Matching Algorithms for Intrusion Detection”, *In Proceedings of IEEE Conference on Computer Communications*, Hong Kong. March 2004.
 - [26] Y. Kim, W. C. Lau, M. C. Chuah, and H. J. Chao. “PacketScore: Statistics-based Overload Control against Distributed Denial-of-Service Attacks”, *In Proceedings of IEEE Conference on Computer Communications*. Hong Kong. March 2004.
 - [27] Vadim I. Utkin, *Sliding Mode in Control Optimization*, Springer-Verlag Berlin, Heidelberg, New York, 1992.
 - [28] T. Peng, C. Leckie and R. Kotagiri., “Proactively Detecting DDoS Attack Using Source IP Address Monitoring”, *In Proc. of IFIP-TC6 conference on Networking 2004*, Athens, Greece, May, 2004
 - [29] T. Peng, C. Leckie and R. Kotagiri, “Prevention from distributed denial of service using history-based IP filtering”, *In Proceedings of IEEE International Conference on Communications 2003*, Anchorage, Alaska, USA, August 2003.
 - [30] John Ioannidis and Steven M. Bellovin, "Implementing Pushback: Router-Based Defense against DDoS Attacks", *In Proceeding of Network and Distributed System Security Symposium*, February 2002.
 - [31] Ratul Mahajan, Steven M. Bellovin, Sally Floyd, John Ioannidis, Vern Paxson, Scott Shenker. “Controlling high bandwidth aggregates in the network”, *ACM SIGCOMM Computer Communication Review*, Volume 32, Issue 3, July 2002
 - [32] Shin, K.G.; Xianzhong Cui, "Computing time delay and its effects on real-time control systems", *IEEE Transactions on Control Systems Technology* 3(2). June 1995, pp. 218 – 224.
 - [33] Morioka, H., Sabanovic, A., Uchibori, A.; Wada, K., Oka, M, "Application of time-delay-control in variable structure motion control systems". *In Proceedings of IEEE International Symposium on Industrial Electronics. Vol. 2.* June 2001, pp.1313 – 1318.
 - [34] Aweya, J, Ouellette, M., Montuno, D.Y.,” Design and Stability Analysis of a Rate Control Algorithm Using the Routh–Hurwitz Stability Criterion”. *IEEE/ACM Transactions on Networking*, 12(4), Aug. 2004.