Hindawi
Security and Communication Networks
Volume 2021, Article ID 4733190, 17 pages
https://doi.org/10.1155/2021/4733190

Research Article

Stability of SDE-LJN System in the Internet to Mitigate Constant-Rate DDoS Attacks

Kaijiao Huang,[1] **Liansheng Tan**,[1,2] **and Gang Peng**[3]

[1] *Department of Computer Science, Central China Normal University, Wuhan 430079, China*
[2] *College of Science and Engineering, University of Tasmania, Hobart, TAS 7001, Australia*
[3] *School of Computer Science, Shenzhen Institute of Information Technology, Shenzhen 518172, China*

Correspondence should be addressed to Liansheng Tan; l.tan@mail.ccnu.edu.cn

Received 13 May 2021; Revised 20 July 2021; Accepted 2 September 2021; Published 6 October 2021

Academic Editor: Wenjuan Li

The Internet is nowadays suffering dramatically serious attacks, with the distributed denial of service (DDoS) attacks being the representative and dominant ones. It is seen that, to stabilize the buffer queue length around a given target under DDoS attacks in the relevant routes is vitally important and helpful to mitigate the attacks and to improve the quality of service (QoS) for normal users. In the current paper, a stochastic queue dynamic model with Le vy jump noise, which is affected by the continuous Brownian motion and the discontinuous Poisson process, is worked out to develop a novel and accurate mathematical framework for the stability of a route queue that deals with constant-rate DDoS attacks. This article proposes a security defensive mechanism in the network for solving the network collapse that can possibly be caused by DDoS attacks, otherwise. Particularly, based on the formulation of a stochastic queue dynamic with Le vy jump noise, the mechanism that characterizes the behavior of the queue at routers is presented for stabilizing the queue length under constant-rate DDoS attacks. By applying the stochastic control theory into analyzing the performance of queue dynamic under constant-rate DDoS attacks, some explicit conditions are established under which the instantaneous queue length converges to any given target in a route. Simulation results demonstrate the satisfaction of the proposed defense mechanism with sharp contrast to the state of the art active queue management (AQM) schemes.

1. Introduction

Distributed denial of service (DDoS) attackers send large volume of attacking packets through the distributed method, which subsequently prevent the normal users to access the Internet services and seriously affect the availability of the networks. The motivations of DDoS attacks range from commercial competition to extortion and even political motives. There are growing research interests on DDoS attacks, mainly including detecting DDoS attacks and mitigating DDoS attacks [1–3]. The biggest disadvantage of intrusion detection system (IDS), as a DDoS defense platform, is that IDS can only detect the attacks, but it does nothing to alleviate the attacks [4, 5]. Guarino et al. [6] presented a novel application of neural networks to classify DDoS attacks and used hive plot images for DDoS attack classification. The authors [7] apply the machine learning algorithm to differentiate attack and normal traffic in near-real-time and create Firewall rules to make distributed filtering come true. However, due to the static nature of these methods, there are some limitations to recognize the constantly changing DDoS attacks.

Due to the lack of the reasonable modeling methods for DDoS attacks and an effective DDoS combat solution, the trend of size, frequency, and complexity of DDoS attacks still continues to increase. Due to the explosive growth of network traffic under DDoS attacks, the traditional systems are difficult to deal with DDoS attacks. Therefore, it is necessary to establish a targeted and effective mathematical model for research. Moreover, it is key to model the behavior of constant-rate DDoS attacks, explain mathematically the damage behavior of constant-rate DDoS attacks, and provide a theoretical basis for the defense strategy.

1.1. Related Work of Stochastic Dynamic Theory. Stochastic control theory has attracted many researchers' attention and has become a hot research area due to its theoretical and practical significance. At present, stochastic nonlinear systems have been widely used in various fields such as population models, automatic control, and network models. Furthermore, the stability of stochastic nonlinear systems and other related theories have become important research directions. Mao and Yuan [8] conduct in-depth professional research on the stability (e.g., asymptotic stability and exponential stability) of stochastic nonlinear systems. Zong et al. [9] derive the transient and exponential stability criteria for Lyapunov functions on the basis of the functional Itô formula. Nguyen and Yin [10] obtained new conclusions for almost sure and L^p stability of SFDEs with regime switching by using Lyapunov functionals. Various discriminant conditions of stochastic systems are obtained by applying Lyapunov, stochastic inequality, stochastic differential equation, and so on. Stochastic control systems include parameter estimation, characteristics identification, state filtering, optimal disturbance rejection control, and other aspects [11]. Stochastic model and stochastic control theory have been well developed and widely studied in other applications (e.g., finance and signal processing), but they are rarely studied in the field of communication security.

Stochastic dynamic models with Le vy jump noise have been studied extensively [12–15]. In addition, potential applications of Le vy jump noise models in communication engineering have attracted great attention among scholars. The results of relevant theories have become an indispensable part of many cutting-edge technologies, including aerospace technologies, automatic control, and network communications. Hu [16] proposed the stochastic linear quadratic optimal control problem and the optimal stop problem for finite time zone and infinite time zone driven by Le vy process, which provides the theoretical basis. Complex dynamical systems are often affected by non-Gaussian Le vy noise. Chen et al. [17] presented a nonlocal interaction differential equation that describes the average exit time of non-Gaussian discontinuous Le vy jump noise systems.

In order to better model the system, Le vy noise is commonly found in finance [18], signal processing [19], secure communication system [20], and other fields [21] and has been successfully applied in many fields. There is growing evidence that stochastic processes with jumps more realistically describe the behavior of many dynamic models; for example, the load of vehicles can be described by a Poisson process [22]. Besides, the adaptive control of Le vy jump noise systems and the adaptive control of systems' parameter estimation are studied in the real networks. The literature [23] investigates the controllability of stochastic systems which are driven by Le vy process and proposes some assumptions to obtain completely suitable controllability. Zhang et al. [24] presented the class of stochastic systems with Le vy noise on networks and established some criterions to guarantee pth moment exponential stability and stability in probability by applying Lyapunov stability theory and graph theory. Huang and Wang [25] analyzed a quadratic stochastic control system which is driven by Le vy process, verified the existence and uniqueness of explicit control, and obtained the explicit form of optimal control for this control system, therefore solving the quadratic stochastic optimal control problem. This phenomenon that the surge in network traffic is caused by DDoS attacks cannot be described by traditional white noise. Taking into account, Le vy jump noise in a stochastic queue model makes the system analysis more realistic. Unfortunately, there are research gaps in the study of stochastic network dynamics with Le vy jump noise in the field of network security, which deserves more attention. In this context, for constant-rate DDoS attacks problem, this paper introduces control technology to defense against constant-rate DDoS attacks.

1.2. Key Challenge and Contributions. In the Internet, stability of the instantaneous queue length in the relevant routes plays a very important role in the network performance such as high throughput; controlling instantaneous queue size is a key issue that network systems need to address. The variation of network parameters and instantaneous queue length is essentially in random [26] nature, which has not been adequately attended so far in the current expositions in this domain. When large amounts of malicious traffic inject packets into the routers, the inherent randomness of instantaneous queue can be observed to be particularly significant. Therefore, this paper proposes a stochastic differential equation approach with Le vy jump noise (SDE-LJN). Other researchers improve network by building nonlinear controllers [27–29] which adjust controller parameters compatible with system dynamics and then affect system performance. In view of DDoS attack traffic, control theory is used to analyze SDE-LJN system under DDoS attacks and present a kind of so-called parabolic control strategy in the article. The network quality of service (QoS) can be improved by suppressing the attack traffic. Our defense mechanism makes instantaneous queue length in the router converge to a given target and effectively inhibits malicious traffic. We introduce Le vy jump noise into the stochastic queue system, which aims to describe the great influence of constant-rate DDoS attacks and to understand the impact of constant-rate DDoS attacks on network queues. Thus, SDE-LJN model is established and an adaptive defend strategy is derived, which can help to establish an anti-DDoS attack mechanism to block malicious traffic and control outbreaks. Note that, a defense scheme based on SDE-LJN system provides critical insight and guidance into maintaining the desired queue length, resulting in robust performance for networks under constant-rate DDoS attacks. Simulation results indicate the feasibility of our defend strategy against constant-rate DDoS attacks.

It is an important practical problem that is achieving stability of instantaneous queue length under DDoS attacks. According to the characteristics of constant-rate DDoS attacks, this paper establishes a novel accurate model and obtains the corresponding control feedback law, that is, this paper models and analyzes SDE-LJN system under constant-rate DDoS attacks, and then the suitable defend strategy is found to mitigate constant-rate DDoS attacks. The objective of SDE-LJN system is to make the instantaneous queue size converge to a target value. The parameters of SDE-LJN system and the control parameter are adjusted to mitigate the attack traffic. How to mitigate DDoS attacks by using a less conservative technique and how to effectively deal with DDoS attacks are extremely interesting and deserve our investigation. The major contributions of the paper are outlined as follows:

(1) The SDE-LJN model is established under constant-rate DDoS attacks. Some interesting conclusions are obtained to deal with DDoS attacks by applying Le vy jump noise as the disturbance factor to describe the evolutions of instantaneous queue when the networks suffer from DDoS attacks. Then, SDE-LJN system, an accurate model describing DDoS attacks, brings a new perspective for DDoS attacks defense.

(2) A new defend criterion is proposed to regulate instantaneous queue length to a desired target and thus to hold back malicious traffic rate.

(3) An important fact has been revealed that the suitable white noise can suppress the explosion of constant-rate DDoS attacks effectively.

(4) An anti-DDoS mechanism is designed to block malicious traffic to maintain the desired queue length and thereby to ensure normal transmission of legitimate traffic.

1.3. Paper Layout. The remainder of this paper is organized as follows. Section 2 proposes and analyzes the stochastic queue model with Le vy jump noise under DDoS attacks. Section 3 shows the stability analysis of the stochastic queue dynamic with Le vy jump noise under DDoS attacks. In Section 4, simulation results verify our theoretical results and show the satisfaction of the proposed scheme. Finally, Section 5 concludes the paper and discusses future work.

2. Mathematical Modeling of Queue Dynamic with Lévy Jump under Constant-Rate DDoS Attacks

To bring the instantaneous queue length to the desired target and to avoid overflow and serious fluctuations of instantaneous queue are considered to be the vital objectives [30–33]. The instantaneous queue size, to a certain extent, represents the state of networks at the moment and can estimate whether the network in normal or abnormal. Therefore, SDE-LJN system is proposed and the anti-DDoS mechanism is used to block DDoS attack flows into the victim networks.

The sample path of the bottleneck queue size is described by the differential equation as follows [34]:

$$\frac{\mathrm{d}q(t)}{\mathrm{d}t} = -C + \frac{N}{\tau(t)}W(t), \tag{1}$$

where T_p represents propagation delay (seconds), $\tau(t) = q(t)/C + T_p$ means the round-trip time, $W(t)$, wherein $0 \le W(t) \le W_{\max}$) represents the congestion window size in packets, $W_{\max}$ is the maximum window size, $q(t)$, wherein $0 \le q(t) \le q_{\max}$) is the queue size (packets), $q_{\max}$ is the maximum queue size, C is a single bottleneck transmission link of capacity, and N represents the number of connections. Equation (1) can be linearized around its equilibrium point (w_0, q_0) to obtain

$$\frac{\mathrm{d}\delta q(t)}{\mathrm{d}t} = \frac{1}{\tau_0}\left(N\delta W(t) - \delta q(t)\right), \tag{2}$$

where $\delta W(t) = W(t) - W_0, \delta q(t) = q(t) - q_0$ and τ_0 represents the delay time at the equilibrium point of the system, which is the summation of the propagation delay and the queuing delay at the equilibrium point. That is, $\tau_0 = q_0/C + T_p$.

2.1. Attack Model. As depicted in Figure 1 [35], Figure 1(a) is composed of a single bottleneck queue driven by DoS flows, and Figure 1(b) shows that the periodic l-length bursts create short l'-length outages. The incoming packets from the violators reach the queue, which results in reducing the congestion window for users.

If all users including normal users and perpetrators send a mixed stream $q^{\mathrm{TCP}}(t)$ and $q^{V}(t)$, then the associated rate of the congestion windows is

$$q^{\mathrm{TCP}}(t) + q^{V}(t)I_{q^V}(Z) = \frac{W(t)}{\tau(t)}, \tag{3}$$

where $I_{q^V}(Z)$ is an indicator function in an attack packet set q^V; the function value equals 1 if Z is true, 0 otherwise:

$$I_{q^V}(Z) = \begin{cases} 1, & Z \in q^V, \quad \text{there is DDoS attack;} \\ 0, & Z \notin q^V, \quad \text{no DDoS attack.} \end{cases} \tag{4}$$

When these attackers launch a DDoS attack, the network traffic increases significantly and does not attenuate during the attack, which is much higher than the normal network traffic value. Therefore, the total incoming rate of the congestion window can be used as a statistical feature of the network traffic, and attacks can be judged by comparing the current network state with the normal network state. Once the aggregation rate spikes significantly, the alarm will sound. However, some of the warnings may be false. Thus, once the warning is issued, the detection module will carry out attack detection on the suspicious traffic. The detector accurately detects DDoS attacks, and the isolator then correctly distinguishes attack traffic and legitimate traffic. This result is significant for applications in that, once the DDoS attack flows are discriminated from legitimate flows, one is able to block the attack packets from entering the queue [1].

The equivalent form of (3) is

$$\tau(t)q^{\mathrm{TCP}}(t) + \tau(t)q^{V}(t)I_{q^V}(Z) = W(t). \tag{5}$$

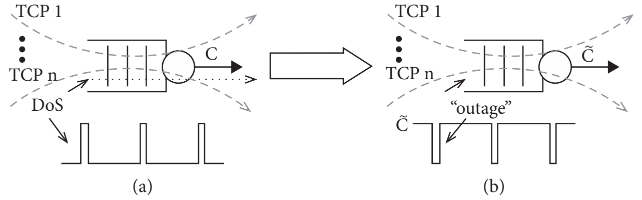

Figure 1: (a) Denial of service attacks scenario and (b) system model.

According to the above description, $\delta q(t)$ and $\delta W(t)$ in the queue model (2) under DDoS attacks will be transformed as follows:

$$\delta q(t) = q^{\mathrm{TCP}}(t) + q^{V}(t) I_{q^V}(Z) - q_0^{\mathrm{TCP}}, \tag{6}$$

$$\delta W(t) = \tau(t) q^{\mathrm{TCP}}(t) + \tau(t) q^{V}(t) I_{q^V}(Z) - W_0^{\mathrm{TCP}}, \tag{7}$$

$$\tau_0 = \frac{q_0^{V} I_{q^V}(Z) + q_0^{\mathrm{TCP}}}{C} + T_p. \tag{8}$$

Assume that the instantaneous queue without a DDoS attack is under a stable initial state, where W_0^{TCP} and q_0^{TCP} are the initial values in a steady state, which are fixed at equilibrium points without DDoS attacks. Taking DDoS attacks into consideration, equations (6)–(8) impose the effect of DDoS attacks on the network system dynamics. Starting from (3), all the equations contain the factor of DDoS attacks in our paper, and our discussions focus on the solution to handle the traffic under the DDoS attack.

2.2. System Model. The deterministic systems mean that network parameters in the models are all deterministic irrespective of stochastic fluctuations, from the points of real network view, which has some limitations in modeling and practical application of network dynamic models. White noise or Brownian motion is an ordinary model to describe disturbances, and network systems in real-world environment are affected inevitably by random noise. Therefore, considering stochastic perturbation into the sample path of the bottleneck queue size is necessary. We study a parametric class of stochastic processes to model instantaneous queue in our paper. As a result, (2) can be written as

$$\mathrm{d}\delta q(t) = \frac{1}{\tau_0} (N\delta W(t) - \delta q(t)) [\mathrm{d}t + \xi \mathrm{d}B(t)], \tag{9}$$

where $\dot{B}(t)$ denotes a white noise and $B(t)$ represents a Brownian motion defined on a complete probability space $(\Omega, \mathcal{F}, \mathbb{P})$ with a filtration $\mathcal{F}_{t\geq 0}$ satisfying the usual conditions (namely, it is right continuous and increasing while $\mathcal{F}_0$ contains all $\mathbb{P}$-null sets). ξ is the intensity of the noise process.

In general, researchers regard white noise as random interference in stochastic systems. However, a drawback of white noise is not sufficient to describe the change of instantaneous disturbance. In addition to the continuous white noise, network systems may also be affected by discontinuous noise such as Le vy jump noise. Interference from DDoS attack streams is discontinuous (see Figure 2). In general, this phenomenon can be described as a combination of stochastic differential equation of white noise and Le vy jump noise mathematically. Networks may suffer from sudden and powerful DDoS attacks with devastating force. DDoS attacks disrupt the QoS of a host from the Internet and dramatically waste network resources of target users, thus resulting in QoS cliff drop. Unfortunately, stochastic equation (9) with white noise is not enough to explain this kind of sudden and explosive phenomenon. This kind of phenomenon is generally described by stochastic differential equations with Le vy jump noise, which describes the dynamic behavior of system with the combination of continuous and jump noise disturbing factors.

The DDoS attack strategy is the description of attack traffic at every time during the attack process. All DDoS attack strategies could be classified into three categories (i.e., varying-rate, constant-rate, and increasing-rate). The constant-rate DDoS attack differs from other DDoS attacks with the obvious feature that periodically sends a short-time high rate such as pulse. The constant-rate DDoS attack stream is created by the model given in Figure 2 [36], where a is the attack period, u indicates the burst period, and $r(u)$ means the burst rate. DDoS attackers inject TCP flows into the time-out (RTO) mechanisms by sending attack rate *r(u)*; thus, the TCP throughput will be reduced. Mathematically, discontinuous Poisson process can depict the major unpredictable disaster events, thus it can describe this characteristic phenomenon caused by DDoS attacks.

An accurate mathematical model is crucially important to study how to mitigate DDoS attacks. In order to explain the phenomenon of DDoS attacks, Le vy jump noise was introduced into queue dynamics. DDoS attacks make the network traffic have high noise characteristics, so the stochastic model with Le vy jump noise (SDE-LJN) is a reasonable and necessary way to describe networks under DDoS attacks and provides a feasible and more realistic model that directly reflects the dynamic characteristics, the dynamic variation of the parameters of SDE-LJN system and performance of instantaneous queue. Referring to the stochastic dynamic models with Le vy noise, the novel SDE-LJN model is formulated to analyze the evolution of network states under attacks. Therefore, SDE-LJN system is established as follows:

$$\mathrm{d}\delta q(t) = \frac{1}{\tau_0} (N\delta W(t) - \delta q(t)) [\mathrm{d}t + \xi \mathrm{d}B(t)] + \delta q(t^{-}) \int_{\mathbb{Y}} r(u) \widetilde{\mathcal{N}}(\mathrm{d}t, \mathrm{d}u), \tag{10}$$

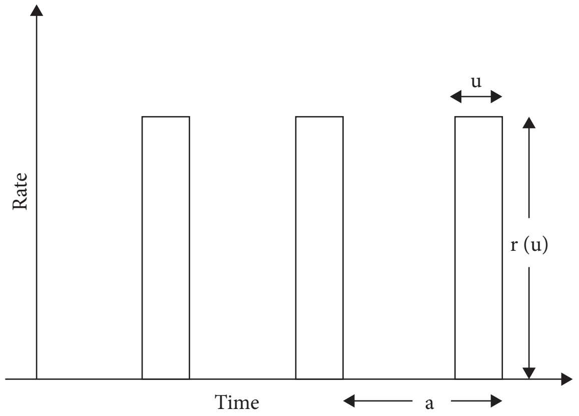

Figure 2: The constant-rate DDoS attack stream pattern.

where τ_0 represents the delay time at the equilibrium point of the system under a DDoS attack. The function $r(u)$ is called the jump term with jump size u. According to equation (10) and Figure 2, the jump term $r(u)$ in equation (10) is equal to the attack rate $r(u)$ in Figure 2; the jump size u in equation (10) is the same as the burst period u in Figure 2. Therefore, as can be seen from Figure 2, equation (10) describes the characteristics of constant-rate DDoS attack. In other words, SDE-LJN system well reflects the influence of constant-rate DDoS attack intensity on the system. The component $\delta q(t^-) = \lim_{s\uparrow t}\delta q(s)$. $\widetilde{\mathcal{N}}(\mathrm{d}t, \mathrm{d}u)$ is a Poisson counting measure with characteristic measure λ on a measurable subset $\mathbb{Y}$ of $[0,\infty)$ with $\lambda(\mathbb{Y})<\infty$, $\widetilde{\mathcal{N}}(\mathrm{d}t, \mathrm{d}u)\colon = \mathcal{N}(\mathrm{d}t, \mathrm{d}u) - \lambda(\mathrm{d}u)\mathrm{d}t$. Also, $\mathcal{N}(\mathrm{d}t, \mathrm{d}u)$ denotes an adapted compensated Poisson random measure with intensity measure λ in [37, 38]. Note that $B(t)$ and $\mathcal{N}(\mathrm{d}t, \mathrm{d}u)$ are independent.

SDE-LJN system directly reflects the dynamic characteristics and transient performance of the queue under DDoS attacks. We advocate that the stochastic queue dynamic with Le vy jump noise can greatly benefit to describe the dynamic of network under DDoS attacks and help us to develop more efficient design guidelines. Hence, in order to deal with the DDoS attack, it is significant and necessary to analyze the dynamic of SDE-LJN system.

As explored later, this article gives the following reasonable hypotheses.

Hypothesis 1. Detecting the DDoS attack in the process of an attack can discriminate attack traffic $q^V(t)$ from legitimate traffic $q^{\mathrm{TCP}}(t)$, and $q^V(t)$ and $q^{\mathrm{TCP}}(t)$ can be separated.

Hypothesis 2. $K_{wq}<0$ and $\delta q(t)$ and $r(u)$ are bounded functions; $\delta\check{q}\colon = \sup_{t\in\mathbb{R}_+}\delta q(t)$ and $r(u) > -1, u \in \mathbb{Y}$, $\int_{\mathbb{Y}}[r(u) - \ln(1 + r(u))]\lambda(\mathrm{d}u) \geq 0$.

Hypothesis 3. $\sqrt{8\tau_0^2\int_{\mathbb{Y}}[r(u) - \ln(1 + r(u))]\lambda(\mathrm{d}u)} \geq \xi^2 + 2\tau_0 -1$ and $\xi^2 > 1$.

Only when malicious flows can be differentiated from legitimate flows as stated in Hypothesis 1, the attack flows can be controlled and blocked without affecting the normal flows in the mitigation phase. Hypotheses 2 and 3 are closely related to the parameters of networks and the disturbance intensity of white noise and Le vy jump noise.

3. The Stability Analysis of the Stochastic Queue Dynamic with Lévy Jump under Constant-Rate DDoS Attacks

The stability analysis of networks queue model has caught many researchers' attention [39–42]. However, DDoS attacks are the most main cause of network instability, divergence, and instantaneous queue oscillation. This section will discuss the stability of SDE-LJN system under constant-rate DDoS attacks.

3.1. The Control Analysis of SDE-LJN System under Constant-Rate DDoS Attacks.

Using Itô − Le vy formula [43] to function $\ln\delta q(t)$ with respect to SDE-LJN system in (10), one has that

$$\begin{aligned}\mathrm{d}\ln\delta q(t) = {}& \left\{\frac{1}{\delta q(t)\tau_0}(N\delta W(t) - \delta q(t)) - \frac{\xi^2}{2(\delta q(t))^2\tau_0^2}(N\delta W(t) - \delta q(t))^2 + \int_{\mathbb{Y}}[\ln(1 + r(u)) - r(u)]\lambda(\mathrm{d}u)\right\}\mathrm{d}t \\ & + \frac{\xi}{\delta q(t)\tau_0}(N\delta W(t) - \delta q(t))\mathrm{d}B(t) + \int_{\mathbb{Y}}\ln(1 + r(u))\widetilde{\mathcal{N}}(\mathrm{d}t, \mathrm{d}u).\end{aligned} \tag{11}$$

Integrating from 0 to t and then dividing by t on both sides of (11), one obtains

$$\begin{aligned}
\frac{\ln \delta q(t)}{t} - \frac{\ln q_0^{\mathrm{TCP}}}{t} &= \frac{1}{t}\int_0^t \left\{ \frac{1}{\delta q(t)\tau_0}(N\delta W(t) - \delta q(t)) - \frac{\xi^2}{2(\delta q(t))^2\tau_0^2}(N\delta W(t)-\delta q(t))^2 \right\} \mathrm{d}s \\
&+ \int_{\mathbb{Y}} [\ln(1+r(u)) - r(u)](\mathrm{d}u) + \frac{1}{t}\int_0^t \frac{\xi}{\delta q(t)\tau_0}(N\delta W(t)-\delta q(t))\mathrm{d}B(s) \\
&+ \frac{1}{t}\int_0^t\int_{\mathbb{Y}} \ln(1+r(u))\widetilde{\mathcal{N}}(\mathrm{d}s,\mathrm{d}u) \le \frac{1}{t}\int_0^t \left\{\frac{1}{\delta q(t)\tau_0}\left[\left(\frac{\xi^2}{\tau_0}+1\right)N\delta W(t) - \delta q(t)\right] - \frac{\xi^2}{2\tau_0^2}\right\}\mathrm{d}s \\
&+ \int_{\mathbb{Y}}[\ln(1+r(u)) - r(u)]\lambda(\mathrm{d}u) \\
&+ \frac{1}{t}\int_0^t \frac{\xi}{\delta q(t)\tau_0}(N\delta W(t)-\delta q(t))\mathrm{d}B(s) + \frac{1}{t}\int_0^t\int_{\mathbb{Y}} \ln(1+r(u))\widetilde{\mathcal{N}}(\mathrm{d}s,\mathrm{d}u).
\end{aligned} \tag{12}$$

In order to solve the challenge of DDoS attacks, we study the random queue system with Le vy jump noise and design the parabolic controller as a defense mechanism against DDoS attacks (see Figure 3). The parabolic controller is introduced into SDE-LJN system to improve the practical applicability and anti-interference performance of the system. The purpose of the defense scheme based on SDE-LJN mathematical modeling is to return the network to a steady state when the DDoS attacks occur.

Based on the above analysis, now we consider a novel control strategy for the SDE-LJN system and utilize the parabola equation as feedback control criteria:

$$\delta W(t) = K_{wq}(\delta q(t))^2, \tag{13}$$

where K_{wq} is a control parameter which dynamically adjusts the congestion window size based on the current level of the network. The controller itself emits a signal, which can be used to drive the SDE-LJN system state equation (10) directly. As is seen in Figure 3, as $\delta q(t)$ is a sampled signal input, one is able to compute the output signal $\delta W(t)$ as a feedback signal. Taking parabolic controller (13) into account in the internal structure of SDE-LJN system, then parabolic controller (13) as feedback controller is integrated into the networks, forming a coupling structure with SDE-LJN system. Furthermore, parabolic controller (13) makes the SDE-LJN system (10) become a closed-loop system. Once a DDoS attack is found, the value of K_{wq} is adjusted to less than 0, then mitigation modules can be set off and block the DDoS attack stream, so as to avoid the network congestion and even breakdown. It is worth noting that only if $K_{wq} < 0$, then one has $\delta W(t) < 0$, which means that the congestion window size is decreasing under DDoS attacks and is consistent with the actual situation. Thus, the combination of SDE-LJN system (10) and parabolic controller (13) forms the mitigation mechanism.

The stochastic queue dynamic with Le vy jump noise takes the feedback control law (13) into consideration; substituting (13) into (12), one has

$$\begin{aligned}
\frac{\ln \delta q(t)}{t} - \frac{\ln q_0^{\mathrm{TCP}}}{t} &\le \frac{1}{t}\int_0^t \left\{\frac{1}{\tau_0}\left[\left(\frac{\xi^2}{\tau_0}+1\right)NK_{wq}\delta q(t) - 1\right] - \frac{\xi^2}{2\tau_0^2}\right\}\mathrm{d}s \\
&+ \int_{\mathbb{Y}}[\ln(1+r(u)) - r(u)]\lambda(\mathrm{d}u) + \frac{1}{t}\int_0^t \frac{\xi}{\tau_0}\left(NK_{wq}\delta q(t) - 1\right)\mathrm{d}B(s) \\
&+ \frac{1}{t}\int_0^t\int_{\mathbb{Y}} \ln(1+r(u))\widetilde{\mathcal{N}}(\mathrm{d}s,\mathrm{d}u) \\
&= \frac{1}{t}\int_0^t \left\{\frac{1}{\tau_0}\left[\left(\frac{\xi^2}{\tau_0}+1\right)NK_{wq}\delta q(t) - 1\right] - \frac{\xi^2}{2\tau_0^2}\right\}\mathrm{d}s \\
&+ \int_{\mathbb{Y}}[\ln(1+r(u)) - r(u)]\lambda(\mathrm{d}u) + \frac{\Phi(t)}{t} + \frac{\widetilde{\Phi}(t)}{t},
\end{aligned} \tag{14}$$

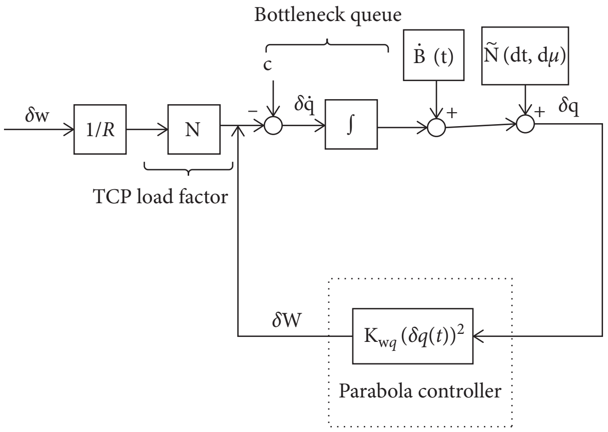

Figure 3: Block diagram of SDE-LJN system under DDoS attack.

where $\Phi(t) = \int_0^t \xi/\tau_0 (NK_{wq}\delta q(t) - 1)\mathrm{d}B(s)$ and $\widetilde{\Phi}(t) = \int_0^t \int_{\mathbb{Y}} \ln(1 + r(u))\widetilde{\mathcal{N}}(\mathrm{d}s, \mathrm{d}u)$ are both local martingales. The quadratic variation processes of $\Phi(t)$ and $\widetilde{\Phi}(t)$ are

$$\langle\Phi,\Phi\rangle_t = \int_0^t \frac{\xi^2}{\tau_0^2}\left(NK_{wq}\delta q(t) - 1\right)^2 \mathrm{d}s,$$
$$\langle\widetilde{\Phi},\widetilde{\Phi}\rangle_t = \int_0^t \int_{\mathbb{Y}} [\ln(1 + r(u))]^2 \lambda(\mathrm{d}u)\mathrm{d}s \tag{15}$$
$$= t\int_{\mathbb{Y}} [\ln(1 + r(u))]^2 \lambda(\mathrm{d}u),$$

respectively.

By (15), one obtains that

$$\limsup_{t\longrightarrow\infty} \langle\Phi,\Phi\rangle_t \le t\frac{\xi^2}{\tau_0^2}\left(NK_{wq}\delta\check{q} - 1\right)^2 < \infty, \text{ a.s.,}$$
$$\lim_{t\longrightarrow\infty} \langle\widetilde{\Phi},\widetilde{\Phi}\rangle_t = \infty, \text{ a.s.,} \tag{16}$$

therefore, in the light of strong law of large numbers for local martingales [44], yielding

$$\lim_{t\longrightarrow\infty} \frac{\Phi(t)}{t} = 0, \text{ a.s.,}$$
$$\lim_{t\longrightarrow\infty} \frac{\widetilde{\Phi}(t)}{t} = 0, \text{ a.s..} \tag{17}$$

Moreover, by Theorem 4.4 in [45], one has that the limit

$$\lim_{t\longrightarrow\infty} \frac{\ln\delta q(t)}{t} = 0. \tag{18}$$

Using Hypothesis 2, namely, $K_{wq} < 0$ and $\int_{\mathbb{Y}} [r(u) - \ln(1 + r(u))]\lambda(\mathrm{d}u) \ge 0$, and taking the limit on both sides of (14), due to (17) and (18), one can conclude that

$$\lim_{t\longrightarrow\infty} \frac{1}{t}\int_0^t \delta q(t)\mathrm{d}s \le \frac{\left(\xi^2/2\tau_0\right) + \tau_0\int_{\mathbb{Y}} [r(u) - \ln(1 + r(u))]\lambda(\mathrm{d}u) + 1}{\left(\left(\xi^2/\tau_0\right) + 1\right)NK_{wq}} \le 0. \tag{19}$$

Moreover, using the basic inequality $ab \le (a + b/2)^2$ $(a, b \in R)$, one can calculate that

$$\begin{aligned}\frac{\ln \delta q(t)}{t}-\frac{\ln q_0^{\mathrm{TCP}}}{t}&=\frac{1}{t}\int_0^t \frac{\left(NK_{wq}\delta q(t)-1\right)\left(\xi^2+2\tau_0-\xi^2 NK_{wq}\delta q(t)\right)}{2\tau_0^2}\mathrm{d}s\\&\quad+\int_{\mathbb{Y}}[\ln(1+r(u))-r(u)]\lambda(\mathrm{d}u)+\frac{1}{t}\int_0^t\frac{\xi}{\tau_0}(N\delta q(t)-1)\mathrm{d}B(s)\\&\quad+\frac{1}{t}\int_0^t\int_{\mathbb{Y}}\ln(1+r(u))\widetilde{\mathcal{N}}(\mathrm{d}s,\mathrm{d}u)\\&\leq\frac{1}{t}\int_0^t\frac{\left[\left(1-\xi^2\right)NK_{wq}\delta q(t)+\xi^2+2\tau_0-1\right]^2}{8\tau_0^2}\mathrm{d}s\\&\quad+\int_{\mathbb{Y}}[\ln(1+r(u))-r(u)]\lambda(\mathrm{d}u)+\frac{1}{t}\int_0^t\frac{\xi}{\tau_0}(N\delta q(t)-1)\mathrm{d}B(s)\\&\quad+\frac{1}{t}\int_0^t\int_{\mathbb{Y}}\ln(1+r(u))\widetilde{\mathcal{N}}(\mathrm{d}s,\mathrm{d}u)\\&=\frac{1}{t}\int_0^t\frac{\left[\left(1-\xi^2\right)NK_{wq}\delta q(t)+\xi^2+2\tau_0-1\right]^2}{8\tau_0^2}\mathrm{d}s\\&\quad+\int_{\mathbb{Y}}[\ln(1+r(u))-r(u)]\lambda(\mathrm{d}u)+\frac{\Phi(t)}{t}+\frac{\widetilde{\Phi}(t)}{t}.\end{aligned}\tag{20}$$

Taking the limit on both sides of (20), due to (17) and (18), one can conclude that

$$8\tau_0^2\int_{\mathbb{Y}}[r(u)-\ln(1+r(u))]\lambda(\mathrm{d}u)\leq\lim_{t\longrightarrow\infty}\frac{1}{t}\int_0^t\left[\left(1-\xi^2\right)NK_{wq}\delta q(t)+\xi^2+2\tau_0-1\right]^2\mathrm{d}s.\tag{21}$$

According to Hypotheses 2 and 3, namely, $K_{wq}<0$, $\xi^2>1$, $\int_{\mathbb{Y}}[r(u)-\ln(1+r(u))]\lambda(\mathrm{d}u)\geq 0$, and $\sqrt{8\tau_0^2\int_{\mathbb{Y}}[r(u)-\ln(1+r(u))]\lambda(\mathrm{d}u)}\geq\xi^2+2\tau_0-1$, leading to

$$\lim_{t\longrightarrow\infty}\frac{1}{t}\int_0^t\delta q(t)\mathrm{d}s\geq\frac{\sqrt{8\tau_0^2\int_{\mathbb{Y}}[r(u)-\ln(1+r(u))]\lambda(\mathrm{d}u)}-\xi^2-2\tau_0+1}{\left(1-\xi^2\right)NK_{wq}}\geq 0.\tag{22}$$

Finally, from (19) and (22), according to the squeeze theorem, one then derives that

$$\lim_{t\longrightarrow\infty}\int_0^t\delta q(t)\mathrm{d}s=0,\tag{23}$$

namely,

$$\lim_{t\longrightarrow\infty}\delta q(t)=0.\tag{24}$$

Substituting (6) into (22), consequently,

$$\lim_{t\longrightarrow\infty}\left(q^{\mathrm{TCP}}(t)+q^{V}(t)\right)=q_0^{\mathrm{TCP}}.\tag{25}$$

Equation (25) indicates that the instantaneous queue length under DDoS attacks can converge to any given initial value q_0^{TCP}, where q_0^{TCP} is a fixed equilibrium point without DDoS attacks; one then has

$$\lim_{t\longrightarrow\infty}q^{\mathrm{TCP}}(t)=q_0^{\mathrm{TCP}}.\tag{26}$$

Combining (23) and (26), then we have

$$\lim_{t\longrightarrow\infty}q^{V}(t)=0.\tag{27}$$

Equation (27) implies that malicious packets tend to 0 and indicates that our defense technology is effective in blocking DDoS attacks based on Hypotheses 1, 2, and 3.

3.2. The Proposed Collaborative Architectures of Network Defense Deployment. The attacks defense system, the process of successfully protecting a victim network from attacks, can be widely composed of four modules: prevention, detection, mitigation, and analysis [46]. In this paper, the mitigation phase carries out the task based on Hypothesis 1, therefore the accuracy of discriminating attack traffic from legitimate traffic is required to be very high. Luckily, the current relevant research results and technologies have been able to achieve a very high degree of detection and classification. Many literatures have studied the detection of DDoS attacks and obtained high detection rate. Hoque et al. [47] used a novel correlation measure to detect DDoS attacks; further, field programmable gate arrays (FPGA) devices classify an incoming traffic as attack traffic or normal traffic in real-time. Alsirhani et al. [48] proposed a dynamic DDoS attack detection system composed of three components: a set of classification algorithms, a distributed system, and a fuzzy logic system. Classification algorithms are used to identify DDoS attacks, a distributed system (i.e., Apache Spark) accelerates the enforcement of these classification algorithms, and the fuzzy logic could dynamically select the right classification algorithm from a set of classification algorithms to detect DDoS attacks. Nandi et al. [49] applied the hybrid feature selection method to select the most important features and used various machine learning classifiers to detect and classify the attack packets and normal packets, then achieving the satisfactory detection rate.

We expound the operation of the proposed defense deployment. The proposed collaborative deployment framework of defense DDoS attacks (please see Figure 4) consists of two main modules: network attack detection module and network attack mitigation module. The detection module is responsible for analyzing the traffic characteristics and classifying them as normal or malicious traffic. The mitigation module then is accountable for blocking malicious traffic into networks. Our defense strategy has a complementary defense solution, which provides the combination of detection attack and the execution of mitigation attack. Therefore, how to effectively mitigate the attack is particularly important when the attack is detected, and this paper focuses on the research of mitigating DDoS attacks. Note that SDE-LJN system with the parabola feedback controller is used as the defense mechanism.

3.3. Technical Note. The white noise and Le ́vy jump noise are introduced into a new stochastic queue model and the parabolic feedback controller then is proposed for this queue model. In order to solve or mitigate DDoS attacks, it is necessary to use the control mode and apply control valves to block malicious flows in real-time. Now, consider the relationship between the white noise factor ξ^2 and the attack rate $r(u)$ which conforms to the constraint of inequalities (17) and (20). The relationship between ξ^2 and $r(u)$ under a set of values of $\lambda(\mathbb{Y})$ and τ_0 is plotted in Figure 5, where $\mathbb{Y} = (0, +\infty)$, $\lambda(\mathbb{Y}) = 1$, $\tau_0 = 0.25$. As shown in Figure 5, the white noise factor ξ^2 can be adjusted dynamically to tune the attack rate $r(u)$ so that the optimal value of ξ^2 makes the attack rate $r(u)$ minimum. Figure 5 intuitively reveals an important fact that the suitable white noise can suppress the explosion of constant-rate DDoS attacks effectively. The standard method of calculating the minimum value of the attack rate $r(u)$ requires $o(n^2)$ time.

The specific relationship of the white noise factor ξ^2, the attack rate $r(u)$, and the network parameter τ_0 of SDE-LJN system can be taken as DDoS attacks' defense strategy to achieve the purpose of protecting the networks. That is to say that the attack flows are unable to enter the routers of the victim networks (i.e., $q^V(t) \longrightarrow 0$) by adjusting the parameters of SDE-LJN system. The disadvantage is that the network parameter τ_0, white noise parameter ξ^2, and attack rate $r(u)$ influence each other. Although these parameters are coupled, it is worthwhile to solve DDoS attacks.

The defense strategy objectives of SDE-LJN system are

(i) Effectively controlling and blocking the attack flows into the network

(ii) Minimizing the attack traffic as much as possible, so that DDoS attacks do not make the network collapse

4. Simulation Results

Verifying the effectiveness of alleviating the DDoS attacks is a challenging task. The stability of instantaneous queue under DDoS attacks means the effectiveness of alleviating DDoS attacks. We use ns2 simulator [50] to simulate and evaluate the performance of the instantaneous queue under the DDoS attack. In addition, we also simulate and test the throughput performance metric of ordinary users. The experimentation network environment setup is shown in Figure 6.

In our experiment, we simulate a single bottleneck link with a capacity of 15 Mbps. The maximum buffer size is set to 15, 000 packets. The round-trip time is set to 0.25 s and the target queue size q_0 is set to 1, 450 packets. The ordinary users and malicious attackers both send their packets consecutively within 100 seconds. Attack period a and attack burst u are set to be 1 s and 0.5 s, respectively.

In order to simply distinguish ordinary users from malicious attackers and intuitively evaluate the performance of ordinary users, let ordinary users transmit TCP-based traffic and malicious attackers send UDP garbage packets.

(i) Normal flows: TCP flows of normal users are created by 100 TCP/Reno sources. The TCP-based traffic is transmitted with the rate of 1 kbps.

(ii) Malicious flows: the primary purpose of attackers is to prevent normal packets from arriving at the destination, rather than to ensure the delivery of malicious packets [51]. Malicious traffic is generated by sending attack packets and interfering with the normal communication. The UDP-based traffic as the attack traffic is created by 50 attack sources. The attack rate is 50 Mbps. Tens of thousands packets overwhelm the network in a short time, and the DDoS flows then consume the network resources.

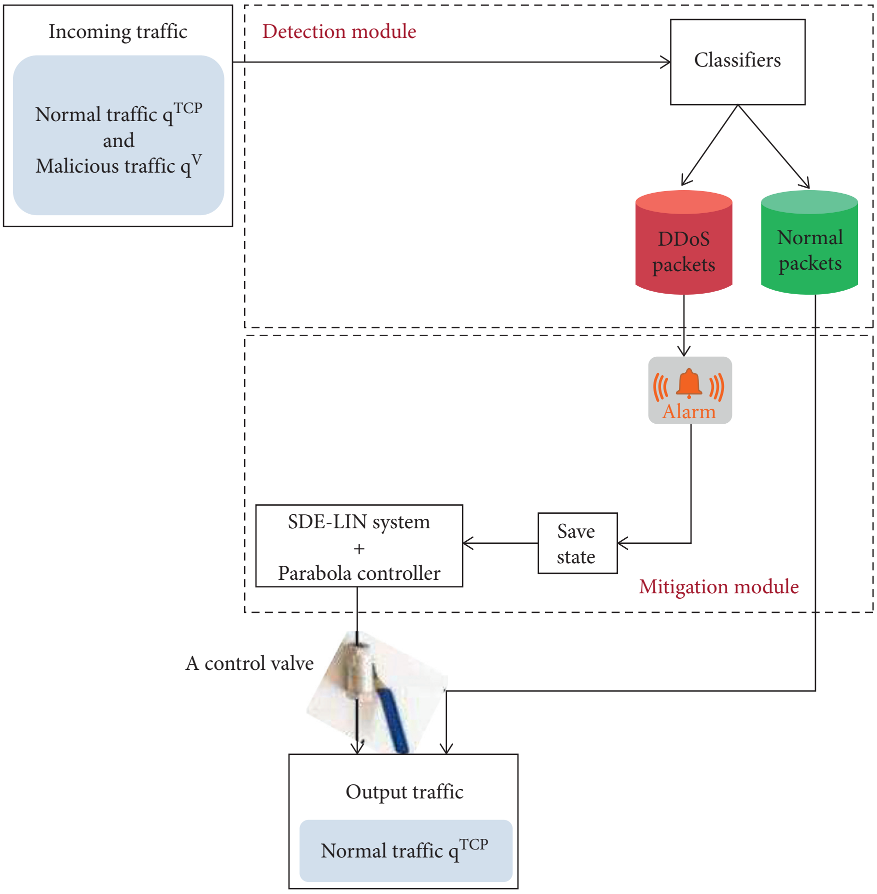

FIGURE 4: A collaborative defense framework.

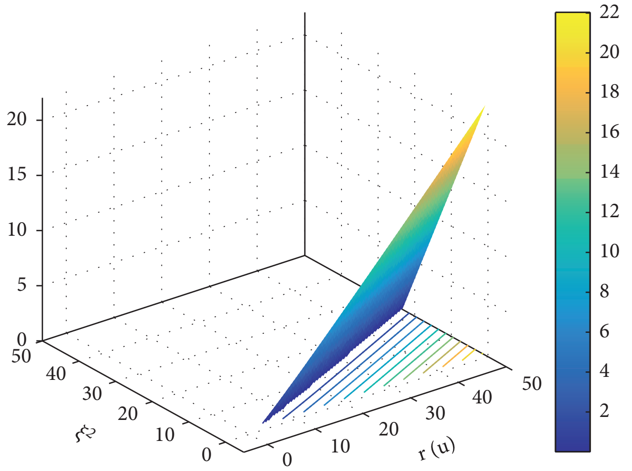

FIGURE 5: Relationship between ξ^2 and $r(u)$ when $\mathbb{Y} = (0, +\infty)$, $\lambda(\mathbb{Y}) = 1$, $\tau_0 = 0.25$.

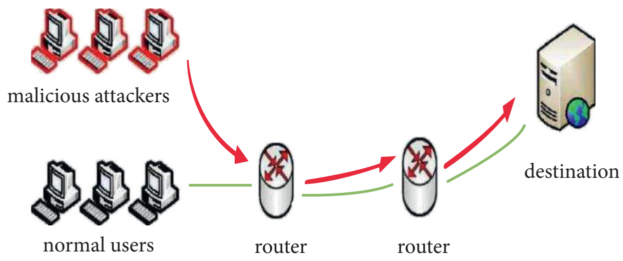

Figure 6: The ns2 simulation environment.

4.1. Experiment 1: Comparison of Four Circumstances. The parameters of experiment 1 are implemented under 4 circumstances as follows:

(i) Circumstance I: the configuration parameters $K_{wq} = 0.45 > 0$, $\xi^2 = 1.21$, and $\mathbb{Y} = (0, +\infty)$, $\lambda(\mathbb{Y}) = 1$, $r(u) = 30.15$, $\tau_0 = 0.25$; one then obtains by calculation $\sqrt{8\tau_0^2 \int_{\mathbb{Y}} [r(u) - \ln(1 + r(u))] \lambda(du)} \approx 3.6545 \geq \xi^2 + 2\tau_0 - 1 = 0.7100$ and $\int_{\mathbb{Y}} [r(u) - \ln(1 + r(u))] \lambda(du) = 26.7112$.

(ii) Circumstance II: the configuration parameters $K_{wq} = -0.0001$, $\xi^2 = 0.93 < 1$, and $\mathbb{Y} = (0, +\infty)$, $\lambda(\mathbb{Y}) = 1$, $r(u) = 30.15$, $\tau_0 = 0.25$; one then obtains by calculation $\sqrt{8\tau_0^2 \int_{\mathbb{Y}} [r(u) - \ln(1 + r(u))] \lambda(du)} \approx 3.6545 \geq \xi^2 + 2\tau_0 - 1 = 0.4300$ and $\int_{\mathbb{Y}} [r(u) - \ln(1 + r(u))] \lambda(du) = 26.7112$.

(iii) Circumstance III: the configuration parameters $K_{wq} = -0.0001$, $\xi^2 = 1.21$, and $\mathbb{Y} = (0, +\infty)$, $\lambda(\mathbb{Y}) = 1$, $r(u) = 0.05$, $\tau_0 = 0.25$; one then obtains by calculation $\sqrt{8\tau_0^2 \int_{\mathbb{Y}} [r(u) - \ln(1 + r(u))] \lambda(du)} \approx 0.0246 \leq \xi^2 + 2\tau_0 - 1 = 0.7100$ and $\int_{\mathbb{Y}} [r(u) - \ln(1 + r(u))] \lambda(du) = 0.00121$.

(iv) Circumstance IV: the configuration parameters $K_{wq} = -0.0001$, $\xi^2 = 1.21$, and $\mathbb{Y} = (0, +\infty)$, $\lambda(\mathbb{Y}) = 1$, $r(u) = 30.15$, $\tau_0 = 0.25$; one then obtains by calculation $\sqrt{8\tau_0^2 \int_{\mathbb{Y}} [r(u) - \ln(1 + r(u))] \lambda(du)} \approx 3.6545 \geq \xi^2 + 2\tau_0 - 1 = 0.7100$ and $\int_{\mathbb{Y}} [r(u) - \ln(1 + r(u))] \lambda(du) = 26.7112$.

The configuration parameters of Circumstance I, Circumstance II, and Circumstance III all do not satisfy SDE-LJN scheme. However, the configuration parameters of Circumstance IV are suitable for the conditions of SDE-LJN system.

4.1.1. Instantaneous Queue under DDoS Attacks in Experiment 1. Figures 7–10 depict the instantaneous queue of four circumstances under the DDoS attack, respectively. Figures 7–9 show that the instantaneous queue sizes of Circumstance I, Circumstance II, and Circumstance III have serious oscillations and severe fluctuations under the attacks. However, in Figure 10, the instantaneous queue length fluctuates around the given target with acceptable oscillations under the attacks. Therefore, adjusting the queue length at the target is well done by using our proposed SDE-LJN scheme.

4.1.2. Throughput under DDoS Attacks in Experiment 1. Figure 11 shows the comparison of TCP throughput of four circumstances under the DDoS attack, and Figure 11 indicates that the TCP throughput of Circumstance I, Circumstance II, and Circumstance III has a terrible consequence, respectively, but the TCP throughput of Circumstance IV achieves high throughput under the attacks.

4.2. Experiment 2: Comparison of Three Schemes. The parameters of experiment 2 are implemented under 3 schemes as follows:

(i) Drop-tail: use ns2 defaults.

(ii) RED: the configuration parameters of RED scheme [52] $\text{min}_{\text{th}} = 200, \text{max}_{\text{th}} = 1000\, w_q = 0.006$.

(iii) SDE-LJN: the configuration parameters $K_{wq} = -0.0001$, $\xi^2 = 1.21$, and $\mathbb{Y} = (0, +\infty)$, $\lambda(\mathbb{Y}) = 1$, $r(u) = -0.983$, $\tau_0 = 0.25$; one then obtains by calculation $\sqrt{8\tau_0^2 \int_{\mathbb{Y}} [r(u) - \ln(1 + r(u))] \lambda(du)} \approx 1.2433 \geq \xi^2 + 2\tau_0 - 1 = 0.7100$ and $\int_{\mathbb{Y}} [r(u) - \ln(1 + r(u))] \lambda(du) = 3.0915$.

4.2.1. Instantaneous Queue under DDoS Attacks in Experiment 2. Figures 12–14 display the instantaneous queue for three schemes (i.e., Drop-tail, RED, and SDE-LJN) under the DDoS attack, respectively. From Figures 12 and 13, it is observed that Drop-tail scheme and RED scheme cause the instantaneous queue length serious oscillations and have severe fluctuations of queue length under the attacks. Drop-tail and RED schemes have terrible outcomes because they are not designed to struggle against the attacks. However, Figure 14 indicates that the instantaneous queue length fluctuates around the target with small oscillations under the attacks.

4.2.2. TCP Throughput under DDoS Attacks in Experiment 2. Figure 15 demonstrates the comparison of TCP throughput of three schemes (i.e., Drop-tail, RED, and SDE-LJN) under the DDoS attack. The CPU utilization at the router affects the throughput, so the throughput could be an indirect reflection

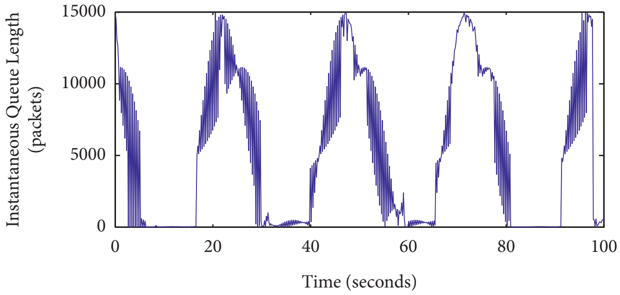

Figure 7: The instantaneous queue length under Circumstance I.

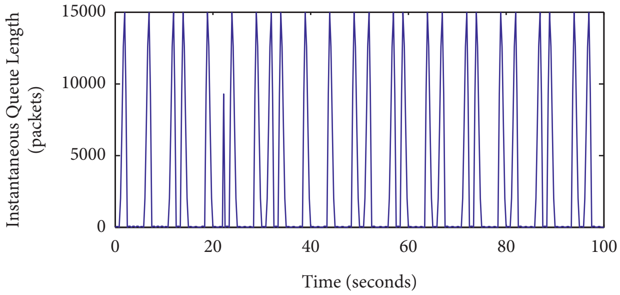

Figure 8: The instantaneous queue length under Circumstance II.

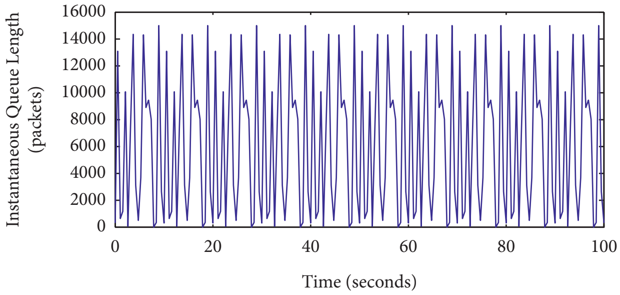

Figure 9: The instantaneous queue length under Circumstance III.

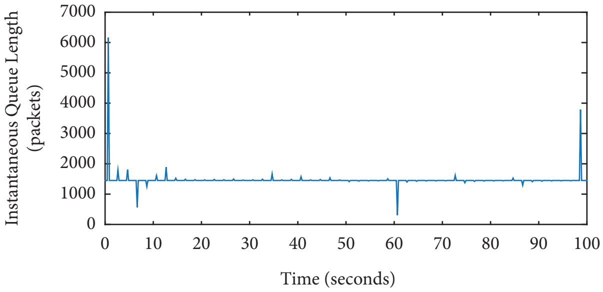

Figure 10: The instantaneous queue length under Circumstance IV.

of router CPU utilization. We can see from Figure 15 that the normal users' throughput of two schemes (i.e., Drop-tail and RED) under the DDoS attack is unsatisfactory, since these schemes cannot mitigate the attack traffic, resulting in high CPU utilization at the router, or even overload. Compared with Drop-tail and RED schemes, the TCP throughput of SDE-LJN scheme is persistently satisfactory under the attacks. The high throughput of normal users under SDE-LJN scheme could indirectly indicate that the CPU utilization at the router is reasonable. Our proposed SDE-LJN scheme is more superior to mitigate DDoS attacks and improve the performance of networks than existing queue policy algorithms (herein refer to Drop-tail and RED).

Based on the comparison of experiment 1 and experiment 2 above, the simulation results verify the effectiveness of the proposed SDE-LJN system as defense scheme to

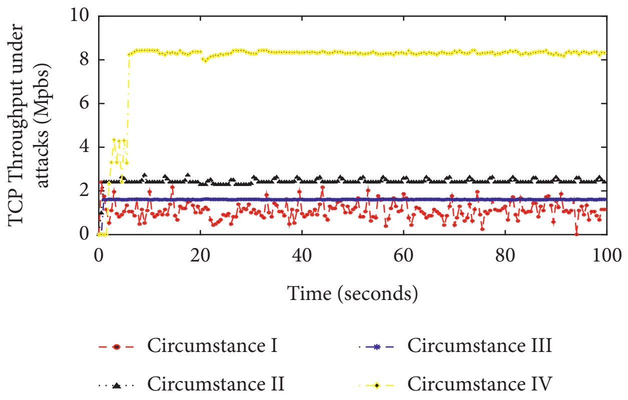

Figure 11: Comparison of TCP throughput of four circumstances under the DDoS attack.

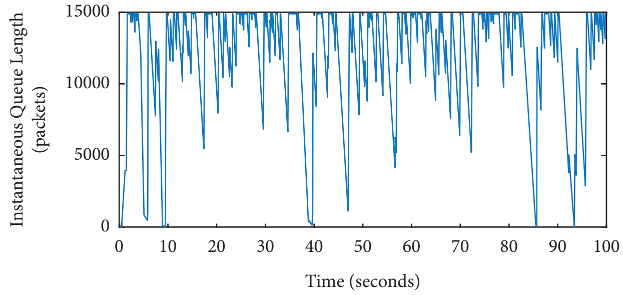

Figure 12: The instantaneous queue length under Drop-tail scheme.

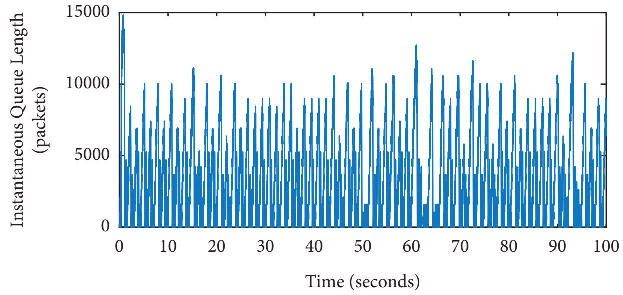

Figure 13: The instantaneous queue length under RED scheme.

mitigate DDoS attacks. In order to more clearly demonstrate this fact, we calculate the mean and standard deviation of the instantaneous queue size. Tables 1 and 2 show that SDE-LJN scheme can achieve the mean queue length closest to the given target and the minimal standard deviation of the instantaneous queue length. Moreover, the results show that the proposed SDE-LJN scheme succeeds in improving the user's experience (i.e., throughput).

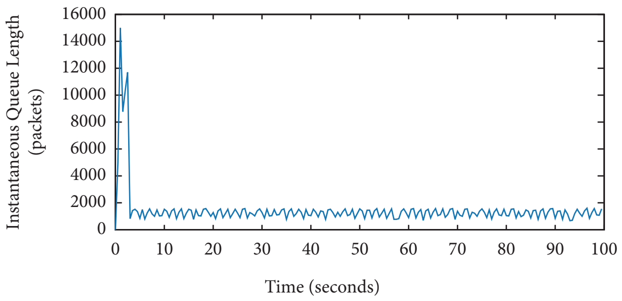

Figure 14: The instantaneous queue length under SDE-LJN scheme.

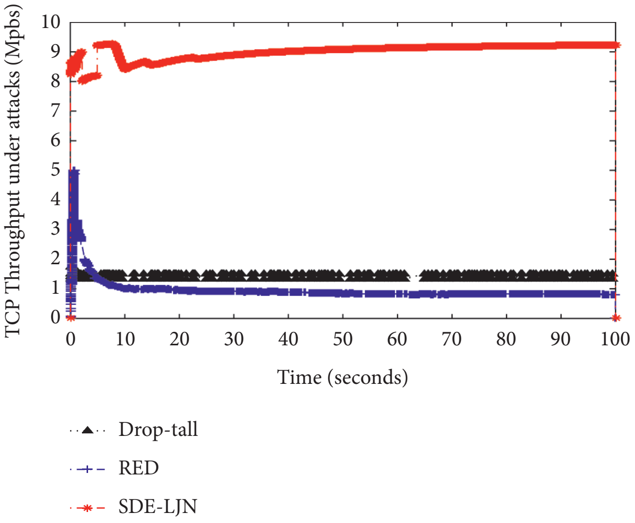

Figure 15: Comparison of TCP throughput of Drop-tail, RED, and SDE-LJN under the DDoS attack.

Table 1: Comparison of mean and standard deviation of instantaneous queue in experiment 1.

	Mean	Standard deviation
Circumstance I	$6.0182e + 03$	$4.2677e + 03$
Circumstance II	$5.8253e + 03$	$5.2641e + 03$
Circumstance III	$6.3045e + 03$	$5.2491e + 03$
Circumstance IV	$1.4649e + 03$	259.6918

Table 2: Comparison of mean and standard deviation of instantaneous queue in experiment 2.

	Mean	Standard deviation
Drop-tail	$4.0150e + 03$	$4.7520e + 03$
RED	$4.2051e + 03$	$3.0884e + 03$
SDE-LJN	$1.4362e + 03$	524.7265

5. Conclusions

This paper addresses the performance problem of users that is caused by constant-rate DDoS attacks. The main objective of this paper has been to create the stochastic queue model under constant-rate DDoS attacks and to design an automated defense mechanism. By analyzing the stochastic queue system with Le vy jump noise, the corresponding defense strategy is designed and the stability conditions of the instantaneous queue are obtained. Furthermore, the feedback controller taking into account SDE-LJN system is adopted to enhance the practical applicability and anti-DDoS attacks. The theoretical analysis and simulation results show that the stability of the instantaneous queue can be maintained under the hypotheses so that constant-rate DDoS attacks can be effectively blocked. The stochastic control theory with Le vy jump noise is applied to constant-rate DDoS attacks defense strategy, and the law of network parameters is presented, which can provide guidelines and application perspectives for designing defense strategies against constant-rate DDoS attacks.

5.1. Future Work. The new queue model and feedback controller proposed in this paper provide novel ideas and feasible technical solutions for dealing with constant-rate DDoS attacks, thus solving the intractable problems in the field of network security. Unfortunately, the research in this paper only focuses on the type of constant-rate DDoS attack. However, there are many types of DDoS attacks, such as varying-rate. Other types of DDoS attacks can be studied in the future. Developing more interesting researches to deal with other types of DDoS attacks is the scope of our future work. In the future, we will apply the proposed SDE-LJN scheme to the complex environment of reality and further research on the influence of control systems on all kinds of attacked networks' performance. Moreover, since the volume of traffic affects the router CPU utilization, the burst traffic can cause high router CPU utilization. If CPU utilization is consistently very high on the router, it is usually considered to be a problem and needs to be investigated. High router CPU utilization (unavailable) causes the network to crash, which is the result of DDoS attacks. Therefore, the first extension to our work will monitor the important metric that is router CPU utilization.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No. 62173157).

References

[1] L. Tan, K. Huang, G. Peng, and G. Chen, "Stability of TCP/AQM networks under DDoS attacks with design," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 3042–3056, 2020.

[2] Y. Shen, C. Wu, D. Kong, and M. Yang, "A two-phase DDoS detection system in software-defined networking," in *Proceedings of the ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, Dublin, Ireland, June 2020.

[3] Y. Zhao, Y. Li, J. Li et al., "Traffic scheduling strategy for mitigating DDoS attack in edge computing-enabled TWDM-PON," in *Proceedings of the 2020 Opto-Electronics and Communications Conference (OECC)*, pp. 1–4, Taipei, Taiwan, 2020.

[4] M. Nenova, D. Atanasov, K. Kassev, and A. Nenov, "Intrusion detection system model implementation against DDOS attacks," in *Proceedings of the 2019 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS)*, pp. 1–4, Tel-Aviv, Israel, November 2019.

[5] N. M. Prajapati, A. Mishra, and P. Bhanodia, "Literature survey—IDS for DDoS attacks," in *Proceedings of the 2014 Conference on IT in Business, Industry and Government (CSIBIG)*, pp. 1–3, Indore, India, March 2014.

[6] M. Guarino, P. Rivas, and C. DeCusatis, "Towards adversarially robust DDoS-attack classification," in *Proceedings of the 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pp. 0285–0291, New York, NY, USA, October 2020.

[7] N. S. Bulbul and M. Fischer, "SDN/NFV-based DDoS mitigation via pushback," in *Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, Dublin, Ireland, June 2020.

[8] X. Mao and C. Yuan, *Stochastic Differential Equations with Markovian Switching*, Imperial College Press, London, UK, 2006.

[9] X. Zong, G. Yin, L. Y. Wang, and T. Zhang, "Stability of stochastic functional differential systems using degenerate Lyapunov functionals and applications," *Automatica*, vol. 91, pp. 197–207, 2018.

[10] D. H. Nguyen and G. Yin, "Stability of stochastic functional differential equations with regime-switching: analysis using dupire's functional itô formula," *Potential Analysis*, vol. 53, pp. 1–19, 2019.

[11] M. Li and X. Liu, "Maximum likelihood least squares based iterative estimation for a class of bilinear systems using the data filtering technique," *International Journal of Control, Automation and Systems*, vol. 18, no. 6, pp. 1581–1592, 2020.

[12] S. Ken-Iti, *Lévy Processes and Infinitely Divisible Distributions*, Cambridge University Press, Cambridge, UK, 1999.

[13] D. Applebaum, *Lévy Processes and Stochastic Calculus*, Cambridge University Press, Cambridge, UK, 2009.

[14] T. Wei, S. Wang, and L. Wang, "Permanence and extinction of stochastic competitive Lotka-Volterra system with Lévy noise," *Journal of Applied Mathematics and Computing*, vol. 57, no. 1-2, pp. 667–683, 2018.

[15] X. Yang, Y. Xu, and R. Wang, "The normal deviation for slow-fast systems driven by lévy noise," 2020, https://arxiv.org/abs/2008.08359.

[16] S. Hu, "Infinite horizontal optimal quadratic control for an affine equation driven by lévy processes," *Chinese Journal of Contemporary Mathematics*, vol. 34, no. 2, p. 129, 2013.

[17] H. Chen, J. Duan, X. Li, and C. Zhang, "A computational analysis for mean exit time under non-Gaussian Lévy noises," *Applied Mathematics and Computation*, vol. 218, no. 5, pp. 1845–1856, 2011.

[18] W. Buckley, H. Long, and S. Perera, "A jump model for fads in asset prices under asymmetric information," *European Journal of Operational Research*, vol. 236, no. 1, pp. 200–208, 2014.

[19] L. D. Nguyen, H. D. Tuan, T. Q. Duong, O. A. Dobre, and H. V. Poor, "Downlink beamforming for energy-efficient heterogeneous networks with massive MIMO and small cells," *IEEE Transactions on Wireless Communications*, vol. 17, no. 5, pp. 3386–3400, 2018.

[20] P. X. Nguyen, H. V. Nguyen, V.-D. Nguyen, and O.-S. Shin, "UAV-enabled jamming noise for achieving secure communications in cognitive radio networks," in *Proceedings of the 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1–6, IEEE, Las Vegas, NV, USA, January 2019.

[21] L. Zhou, Q. Zhu, Z. Wang, W. Zhou, and H. Su, "Adaptive exponential synchronization of m time-delayed recurrent neural networks with l noise and regime switching," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 28, no. 12, pp. 2885–2898, 2017.

[22] J. B. Roberts and M. Vasta, "Parametric identification of systems with non-Gaussian excitation using measured response spectra," *Probabilistic Engineering Mechanics*, vol. 15, no. 1, pp. 59–71, 2000.

[23] X. Yin and Z. Liu, "Controllability of semilinear stochastic systems driven by Lévy process in Hilbert space," in *Proceedings of the 2010 International Conference on Intelligent Computation Technology and Automation*, pp. 1043–1045, IEEE, Changsha, China, May 2010.

[24] C. Zhang, W. Li, and K. Wang, "Graph theory-based approach for stability analysis of stochastic coupled systems with Lévy noise on networks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 26, no. 8, pp. 1698–1709, 2014.

[25] H. Huang and X. Wang, "LQ stochastic optimal control of forwardbackward stochastic control system driven by Lévy process," in *Proceedings of the 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, pp. 1939–1943, IEEE, Xi'an, China, October 2016.

[26] S. Patel, "Sensitivity analysis of queue-based AQM over network parameters," *IET Networks*, vol. 8, no. 4, pp. 280–288, 2019.

[27] A. Pitsillides, P. Ioannou, M. Lestas, and L. Rossides, "Adaptive nonlinear congestion controller for a differentiated-services framework," *IEEE/ACM Transactions on Networking*, vol. 13, no. 1, pp. 94–107, 2005.

[28] X. L. Chang, J. K. Muppala, and J. T. Yu, "A robust nonlinear PI controller for improving AQM performance," in *Proceedings of the IEEE International Conference on Communications*, June 2004.

[29] Y. Fan, Z. P. Jiang, S. Panwar, and H. Zhang, "Nonlinear Output Feedback Control of TCP/AQM Networks," in *Proceedings of the 2005 IEEE International Symposium on Circuits and SystemsIEEE*, Kobe, Japan, May 2005.

[30] M. Sheikhan, R. Shahnazi, and E. Hemmati, "Adaptive active queue management controller for TCP communication networks using PSO-RBF models," *Neural Computing & Applications*, vol. 22, no. 5, pp. 933–945, 2013.

[31] R. J. Briscoe and C. Di Cairano-Gilfedder, "Signalling congestion," U.S. Patent No. 9634916, 2017.

[32] S. Patel and S. Bhatnagar, "Adaptive mean queue size and its rate of change: queue management with random dropping," *Telecommunication Systems*, vol. 65, no. 2, pp. 281–295, 2017.

[33] M. Yue, Z. Wu, and J. Wang, "Detecting LDoS attack bursts based on queue distribution," *IET Information Security*, vol. 13, no. 3, pp. 285–292, 2019.

[34] C. Hollot, V. Misra, D. Towsley, and W. B. Gong, "A control theoretic analysis of red," in *Proceedings IEEE INFOCOM 2001. Conference on Computer Communications. 20th Annual Joint Conference of the IEEE Computer and Communications Society*, Anchorage, AK, USA, April 2001.

[35] J. Luo, X. Yang, J. Wang, J. Xu, J. Sun, and K. Long, "On a mathematical model for low-rate shrew DDoS," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 7, pp. 1069–1083, 2014.

[36] S. Patel, B. Gupta, and V. Sharma, "Throughput analysis of AQM schemes under low-rate Denial of service attacks," in *Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA*, Greater Noida, India, April 2016.

[37] Z. Zhang, J. Tong, and J. Bao, "The stationary distribution of competitive Lotka-Volterra population systems with jumps," *Abstract and Applied Analysis*, vol. 2014, Article ID 820831, 7 pages, 2014.

[38] S. Umarov, M. Hahn, and K. Kobayashi, *Beyond the Triangle-Brownian Motion, "Itô Stochastic Calculus, and Fokker-Planck Equation: Fractional Generalizations*, World Scientific Publishing, Beijing, China, 2018.

[39] S. Prasad and G. Raina, "Stability and bifurcation analysis of the AVQ and E-RED queue management policies," in *Proceedings of the 2016 IEEE Conference on Control Applications (CCA)*, pp. 114–121, IEEE, Buenos Aires, Argentina, September 2016.

[40] S. K. Mohapatra, S. K. Bisoy, and P. K. Dash, "Stability analysis of active queue management techniques," in *Proceedings of the 2015 International Conference on Man and Machine Interfacing (MAMI)*, pp. 1–6, IEEE, Bhubaneswar, India, December 2015.

[41] Y. Wu and Z. Li, "Queueing analysis for delay/disruption tolerant networks with random link interruptions," in *Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 94–99, IEEE, Chengdu, China, December 2016.

[42] S. Manjunath and G. Raina, "Stability and performance of compound tcp with a proportional integral queue policy," *IEEE Transactions on Control Systems Technology*, vol. 27, no. 5, pp. 2139–2155, 2018.

[43] S. Wang, L. Wang, and T. Wei, "Well-posedness and asymptotic behaviors for a predator-prey system with l noise," *Methodology and Computing in Applied Probability*, vol. 19, no. 3, pp. 715–725, 2017.

[44] Q. Liu and Q. Chen, "Analysis of a general stochastic nonautonomous logistic model with delays and Lévy jumps," *Journal of Mathematical Analysis and Applications*, vol. 433, no. 1, pp. 95–120, 2016.

[45] J. Bao, X. Mao, G. Yin, and C. Yuan, "Competitive Lotka-Volterra population dynamics with jumps," *Nonlinear Analysis: Theory, Methods & Applications*, vol. 74, no. 17, pp. 6601–6616, 2011.

[46] M. Essaid, D. Kim, S. H. Maeng, S. Park, and H. T. Ju, "A collaborative DDoS mitigation solution based on ethereum smart contract and RNN-LSTM," in *Proceedings of the 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, pp. 1–6, IEEE, Matsue, Japan, September 2019.

[47] N. Hoque, H. Kashyap, and D. K. Bhattacharyya, "Real-time DDoS attack detection using FPGA," *Computer Communications*, vol. 110, pp. 48–58, 2017.

[48] A. Alsirhani, S. Sampalli, and P. Bodorik, "DDoS detection system: using a set of classification algorithms controlled by fuzzy logic system in apache spark," *IEEE Transactions on Network and Service Management*, vol. 16, no. 3, pp. 936–949, 2019.

[49] S. Nandi, S. Phadikar, and K. Majumder, "Detection of DDoS attack and classification using a hybrid approach," in *Proceedings of 2020 3rd ISEA Conference on Security and Privacy (ISEA-ISAP)*, pp. 41–47, IEEE, Guwahati, India, March 2020.

[50] L. A. Usc/I. S. I., "The ns2 simulator and its documentation," [Online]. Available: http://www.isi.edu/nsnam/ns/.

[51] A. Aissani, “Queueing analysis for networks under DoS attack,” in *Proceedings of the International Conference on Computational Science and its Applications*, pp. 500–513, Springer, Perugia, Italy, July 2008.

[52] L. Tan, W. Zhang, G. Peng, and G. Chen, “Stability of TCP/RED systems in AQM routers,” *IEEE Transactions on Automatic Control*, vol. 51, no. 8, pp. 1393–1398, 2006.

[53] J. Jian Yuan and K. Mills, “Monitoring the macroscopic effect of DDoS flooding attacks,” *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 4, pp. 324–335, 2005.

[54] X. Gao and Y.-F. Zhu, “DDoS defense mechanism analysis based on signaling game model,” in *Proceedings of the 2013 5th International Conference on Intelligent Human-achine Systems and Cybernetics,* vol. 1, pp. 414–417, IEEE, Hangzhou, China, August 2013.