

Network Security Model for Analyzing Network-Based Control Systems under Denial of Service Attacks

Men Long, Student Member, IEEE, Chwan-Hwa “John” Wu*, Senior Member, IEEE, John Y. Hung, Senior Member, IEEE, and J. David Irwin, Fellow, IEEE

Department of Electrical and Computer Engineering, Auburn University, Alabama, 36849 USA

* Corresponding author: wu@eng.auburn.edu

Abstract— Denial of service (DoS) attacks have become major threats to network security, which is pertinent to the deployment and performance of network-based control systems (NBCS). In this paper, we propose two queueing models to simulate the stochastic process of packet transmission under DoS attacks. The motivation is to quantitatively investigate how the attacks affect the performance of NBCS. The control system consists of a discrete PI controller (either event- or time-driven), a second-order plant, and two one-way delay vectors induced by networks. Experimental results indicate that the event-driven controller is more robust than the time-driven one under attacks. Model I DoS attacks (excessive packet loss) impair the performance, but do not destabilize the system with the event-driven controller. Model II DoS attacks (increased delay jitter) deteriorate the performance or even destabilize the system.

I. INTRODUCTION

Remote control using the Internet or other IP-based (Internet protocol) wide area networks has become an emerging technology. A possible scenario of a network-based control system is depicted in Fig. 1. It is known that packet transmission in wide area networks is a complex stochastic process; thus, delay jitter/packet loss will be introduced into control loops.

A relevant but more serious issue is the network DoS attacks. These attacks are a significant problem because they have been proven capable of shutting an organization off from the Internet or dramatically slowing down network links [1]. Malicious users send a large number of spurious packets to a destination to consume excessive amounts of endpoint network bandwidth. Furthermore, in the past three years, there have been large-scale worm activities (viral self-propagating computer programs), causing significant disruptions to the Internet [2], [3].

Packet delay jitter and loss become worse under DoS attacks, which in turn may significantly impair the NBCS performance such as percentage overshoot, rise and settling times, and mean squared error.

The motivation of the study is to quantitatively investigate how DoS attacks affect NBCS. It is difficult for legitimate users to launch real DoS attacks against the prototype of NBCS to measure performance, since the attacks are themselves classified as cybercrime against the law [4]. We propose two simple models to macroscopically approximate the packet transmission of NBCS under DoS attacks. The models are based on a multiple-input queue, which essentially captures the mechanism of network equipment operation. Model I estimates the case that DoS attacks target an

endpoint (either the controller or the plant machine) or the customer-edge routers close to the endpoint. In this case, a large number of NBCS packets may be lost. Model II approximates the case that service-provider-edge routers, possibly few hops away from a targeted endpoint in the path, are attacked. Empirically, the latter type of attack tends to slow down the network links. As a result, NBCS packets may endure relatively long and oscillatory delay jitter.

The simulated delay jitter/packet loss are then incorporated into a control loop (a discrete PI controller with a second-order plant). The numerical simulation results indicate DoS attacks causing long delay jitter may significantly deteriorate the performance of NBCS no matter whether an event- or time-driven controller is used. On the other hand, the attacks causing excessive packet loss degrade the performance but do not destabilize the system with an event-driven controller.

A detailed survey on NBCS was given in [5]. There are also a few works that studied NBCS in which underlying networks are in a regular status. A networked PI controller over IP network was implemented in [6] while [7] proposed a neural network middleware for tracking of a networked mobile robot. The effect of delay jitter on quality of control in EIA-852-based networks was investigated in [8]. Asynchronous and synchronous actuation for a networked control system was discussed in [9]. A general-purpose architecture for the Internet-based teleoperation was presented in [10]. A teleoperation control system, based on the characteristics of the measured site-to-site packet round trip time, was designed and tested in [11]. Reference [12] pointed out the importance of network security in industrial informatics.

The remainder of the paper is organized as follows. Section II introduces the specific controller algorithm and plant dynamics. Section III describes the two queueing models for packet transmission under DoS attacks. Section IV gives the simulation methodology. Sections V and VI analyze the NBCS performance under the two models of DoS attacks, respectively. Conclusion is presented in Section VII.

II. AN EXAMPLE OF CONTROL SYSTEM

The focus of this paper is to study how network security anomaly affects NBCS. A simple discrete PI algorithm and a second-order plant are used. The ideal control system is well understood so that the performance degradation of NBCS

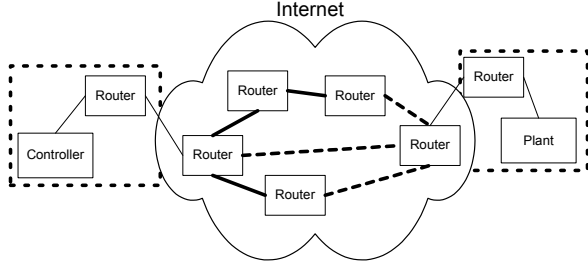


Fig. 1 Realization of a network based control system.

under DoS attacks can be better quantified. The plant transfer function is

$$G_p(s) = \frac{2029.826}{(s + 26.29)(s + 2.296)},$$

and the PI controller has the gains $K_p = 0.1701$, and $K_I = 0.41$ [6]. Note that we use a slightly different value for the integral gain K_I from the original one in [6]. The time scale is in accordance with the control of an electromechanical system, where the sampling rate f_s of the plant is 50 samples/sec.

Under a unit step input, the resultant performance without considering packet transmission latency is: percentage overshoot $po=0.097688$, rise time $t_r=0.16$ sec, settling time $t_s=0.28$ sec, and mean squared error $mse=0.004304$.

III. SIMULATION MODEL

The abstract structure of NBCS control loops is shown in Fig. 2. The sensor measurement and control signal are transmitted between a controller and a plant via network packets. Each sensor packet has a certain time delay before arrival at the controller. Let the latency be $d_{b,i}$, thus the jitter of sensor packets is defined as

$$\tau_{b,i} = d_{b,i} - \min_i(d_{b,i}), d_{b,i} < \infty \quad (1)$$

where the first subscript b represents it is the backward delay from the sensor to the controller and the second subscript i denotes the index of the packet. The packet loss will be treated separately. Similarly, the jitter of control packets is defined as

$$\tau_{f,j} = d_{f,j} - \min_j(d_{f,j}), d_{f,j} < \infty \quad (2)$$

where the first subscript f represents it is the forward delay from the controller to the actuator and the second subscript j denotes the index of the packet.

$\min_i(d_{b,i})$ and $\min_j(d_{f,j})$ can be regarded as the deterministic delay due to the signal propagation and the finite bandwidth. In the simulation, we assume that the deterministic delay has already been compensated. Thus we only consider the stochastic delay jitter τ_b and τ_f in the control loop.

For system operation, the sensor is time-driven. Every $1/f_s$ seconds it sends a packet of the sensor measurement to the controller. The packet will travel through networks

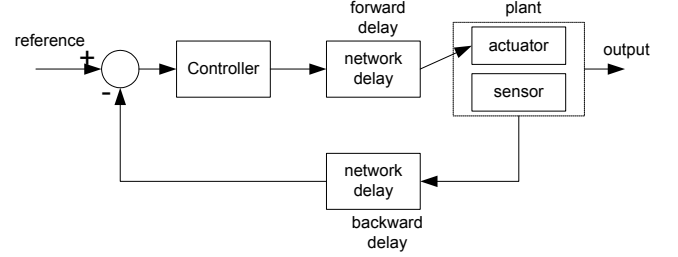


Fig. 2 Abstract structure of a network-based control system

and then arrive at the controller. A packet may be lost during the transit; thus, the controller can be either time-driven (every $1/f_s$ seconds use the latest measurement packet stored in the buffer to calculate control signal and transmit it to the actuator) or event-driven (transmit the control signal upon receiving a measurement packet from the sensor). The actuator will be event-driven.

In computer communication systems, packets moving from one site to another have to access shared resources (communication links and network equipment). For each router in the path between a plant and a controller, the mechanism governing packet transmission can be abstracted by a queue [13]. The discipline for the service is commonly assumed first-come-first-serve. Packets arrive at a router at unpredictable times. If a packet finds that the router CPU is idle, it will be immediately served for a certain amount of time. If the router CPU is busy, the packet will be in the queue to wait. When a queue with a finite size is full, the newly arrived packet is dropped.

The routers in the path handle not only the NBCS packet flow, but also other traffic (non-control applications/flows of other NBCS systems). To capture this, we use a queue with two input processes: one is the NBCS packet flow and the other is the background traffic. Later on, we will add the DoS attacks into the queue. Considering the fact that the routers are heterogeneous/dynamic plus it is infeasible to collect the very detail of traffic data from the routers, we choose to use a lumped queue to simulate the process of packet transmission between a plant and a controller. As will be shown in Section V, the simulated delay jitter under the network regular status from the lumped queue is close to the measured data reported by several US network measurement projects [14], [15].

For simplicity of presentation, we use the mean values to represent the corresponding stochastic processes. For the model of backward delay jitter τ_b , λ_1 is the mean arrival rate (packets/sec) of the sensor data; ψ is the mean arrival rate of the background traffic; μ is the mean service time (msec) of the server in the queue; $\tilde{\lambda}$ is the mean arrival rate of the sensor data at the controller. Currently, it is not uncommon that IP routing from a site to another exhibits symmetry [14]. So we assume the background traffic arrival and the server service time in the model of forward delay jitter τ_f will have identical distribution with those in the model of backward delay jitter τ_b . The mean arrival rate of

control signals is $\hat{\lambda} = f_s$ (time-driven) or $\hat{\lambda} = \tilde{\lambda}$ (event-driven).

We are interested in the total time spent in the queue by the packet n of NBCS. This is simply the sum of waiting time and service time of the packet, which is denoted by

$$s_n = w_n + u_n \quad (3)$$

We will simulate s_n and then use it to approximate the delay jitter τ_b and τ_f .

A. DoS Attack Model I (Larger Packet Loss)

This model approximates the case that DoS attacks target endpoints (a plant or a controller) or customer-edge routers close to endpoints. Attackers can send a flood of packets to overwhelm the endpoints. Likewise worms can propagate into the local area network within an organization and make extremely high-rate port scans. The feature of this kind of attack is that a lot of NBCS packet might be dropped. Since only endpoints are attacked, the survived sensor/control packets may experience relatively small jitter, given that the remaining network may have a regular status.

Fig. 3 shows the model, where we explicitly introduce another arrival process (attack traffic) into the queue with mean arrival rate ϕ (packets/sec). We assume that hackers attack the path from the sensor to the controller. The essence of the model is that we are able to change the magnitude ϕ of attack traffic to approximate the severity of the DoS attacks.

B. DoS Attack Model II (Longer Delay Jitter)

Recall that attackers may try to flood the critical routers in the path between a plant and a controller. Those routers may be few hops away from the endpoints. Those routers owned by Internet service providers or telecommunication carriers are commonly high-end and can handle relatively high packet rate. The effect of the attack is to overload these routers and then slow down network links. Since the control or sensor signal packets have a comparatively small arrival rate, the particular NBCS packet flow may have small loss. Nevertheless, it is likely that the packets in the flow may experience a longer delay jitter.

We choose to lump the attack traffic into the mean service time μ in order to approximate these attacks. In other words, no explicit attack flow is added into the queue. A reference value μ_0 is given first as a representative of network normal status. We increase μ to model the escalated severity of the DoS attacks. Since the victim routers may handle the NBCS traffic in both directions, the value of μ in both forward and backward delay will increase under DoS attacks. The model is depicted in Fig. 4.

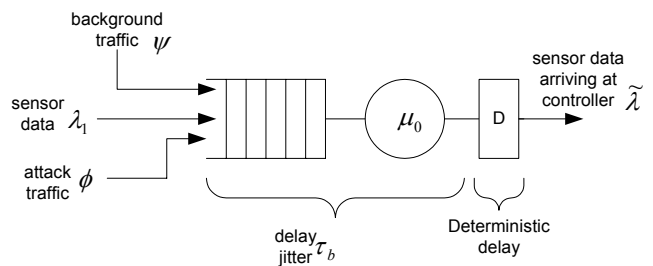


Fig. 3 Model I DoS attacks. Adjust ϕ (attack traffic rate) to approximate the severity of attacks.

IV. SIMULATION METHODOLOGY

The queue in the model is the G/G/1, where “G” denotes the distributions for interarrival and service times of packets are generally distributed, and “1” denotes one server in the queue (serving one packet at a time). In the simulation, we assume the service time under regular or attack status observes an exponential distribution. The background traffic is a Poisson process with a mean rate ψ . Thus, the background traffic load of the channel can be defined as $\psi\mu$.

We also assume the computational time at a controller is negligible, and hence only stochastic delay jitter (τ_b and τ_f) are put in the control loop simulation. Packet loss and large delay jitter are allowed. The packet out-of-sequence problem in the IP network is regarded as a special case of packet loss in NBCS, since a controller after having received the new packet from a sensor will usually ignore the outdated packets which arrive later.

For each simulation run, the time of simulation lasts 15 seconds. The buffer size of queue is 10 in all cases. The reference input for the control loop is a unit step excitation.

In the remaining sections, the values for performance metrics such as percentage overshoot and so on are understood as an average value of many repetitive simulation runs unless the authors make an explicit statement.

V. PERFORMANCE UNDER DOS ATTACK MODEL I (LARGER PACKET LOSS)

Empirically, in DoS attacks, the injected packet rate roughly grows exponentially in the beginning and then saturate at a high level [2], [3]. To fit our simulation environment, we assume that the rate of attack packets grows exponentially to a maximum point ack_mag (maximum packet rate) at 3 second and then levels off until the end of simulation 15 second. The exponential growth and saturation of attack traffic rate is in accordance

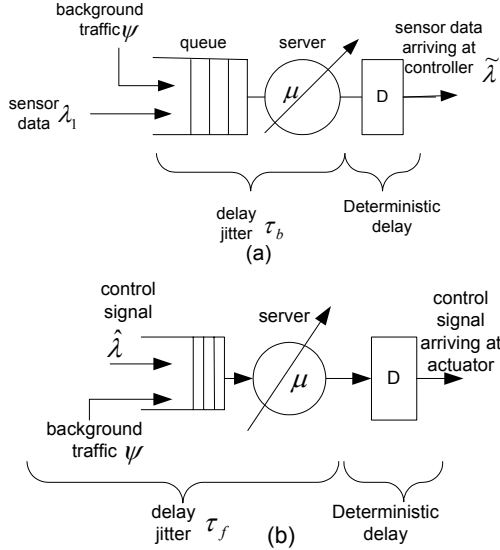


Fig. 4 Model II DoS attacks. Adjust μ (mean service time) to approximate the severity of attacks (a) backward delay (b) forward delay

with one's intuition, though the specific times are a bit arbitrary.

$\mu_0=3$ ms and 60% background traffic load are given as one example of network normal status for both event- and time-driven control approaches. Since the simulation time is 15 sec and the sampling rate is 50 samples/sec, there are 750 measurements packets from a sensor to a controller. Each sensor packet experiences delay jitter of $\tau_{b,i}$ and every control packet endures delay jitter of $\tau_{f,j}$. In one simulation run of the regular case, we average over $\tau_{b,i}$ to get the jitter value $\bar{\tau}_b$ of 6.97 msec. The results of other simulation runs are close to this value. As reported in [15], the one-way jitter of one major US backbone link from Atlanta to Chicago is 8 msec. For any practical NCS system, the jitter including the contribution of edge networks may be above the value. Thus, the parameters we use are a reasonable approximation for representing the network normal status.

Based on DoS attack Model I, we run 10 simulations for each value of ack_mag . Fig. 5 shows the performance of the event-driven control method. It is clear that the system is still stable, though a large number of packets are lost due to the attacks. For example, the loss ratios are: 84%/0 and 85.2%/0.2% for backward and forward channels under ack_mag 2000 packets/sec and 2500 packets/sec. Since attackers do not attack the forward channel, the loss ratio is small there. It can be seen in Fig. 5 that the performance is clearly degraded. The percentage overshoot increases above 0.15, compared to 0.09 without delay. The rise and settling times are even much larger than those without delay.

Fig. 6 displays the performance of the time-driven control approach. When ack_mag is greater than 1000 packet/sec, the system becomes unstable. The loss ratios are 69.2%/0.7% and 85.9%/0.4% for backward/forward channels under rate 1000 packets/sec and 1500 packets/sec. Note that the controller is time-driven so that the number of

packets from the controller to the actuator is high (close to 750). Comparing Fig. 6 to Fig. 5, the time-driven approach is more susceptible to network attacks. These attacks cause excessive packets losses in the path from the sensor to the controller, which makes the controller compensation based on the data stored in the buffer quite inaccurate.

VI. PERFORMANCE UNDER DOS ATTACK MODEL II (LONGER DELAY JITTER)

A. Event-Driven Controller

With the reference $\mu_0=3$ ms, four levels of μ (6, 9, 12, and 15ms) are used to model different magnitude of DoS attack. If μ gets larger, the DoS attacks get more severe. For each value of μ , we change ψ/μ from 10% to 90%, which models the background traffic load from low to high. At every pair of $(\mu, \psi/\mu)$, we run 20 simulations, and the average performance values of 20 runs are reported in Fig. 7.

Fig. 7 clearly conveys that the performance is degraded under DoS attacks. With different classes of μ , the larger μ gets, the worse the percentage overshoot. Under the same class of μ , large background traffic load tends to cause high percentage overshoot. The implication is that the DoS attacks will cause the worse degradation if the path between the controller and the plant has already been under heavy load of background traffic.

The performance of rise time is not affected significantly by the attacks. In all cases, it is within 0.16-0.26 sec. The patterns of settling time and mean squared error are very similar to that of percentage overshoot, which are substantially impaired by DoS attacks. When DoS attacks get more intense (μ increases), the control system may become divergent.

B. Time-Driven Controller

Fig. 8 displays the performance under this strategy. The patterns of Fig. 8 are very close to those of Fig. 7 of event-driven controller. Time-driven method is likely to have a shorter rise time. Since the rise time under the event-driven approach is also reasonable, the improvement of the time-driven approach is minor in this aspect. In terms of percentage overshoot, settling time, and mean squared error, the time-driven approach is inferior to the event-driven method in our simulation environment.

VII. CONCLUSION

In this paper, the performance of a network-based control system under DoS attacks are investigated. We propose multiple-input queuing models to approximate the resultant delay jitter/packet loss, which are then incorporated into the control loop. Model I captures that DoS attacks targeting endpoints may cause excessive packet loss. From simulation results, this type of attack deteriorates the performance, but the system may remain stable with the event-driven controller. Model II captures that DoS attacks targeting the network links cause longer delay jitter. This kind of attack

has a substantial negative impact on the performance. Systems might be destabilized when the DoS attacks get more intense.

REFERENCE

[1] A. Householder, A. Manion, L. Pesante, G. Weaver, and R. Thomas, "Managing the threat of denial-of-service attacks," *Carnegie Mellon CERT Coordination Center*, Oct. 2001. http://www.cert.org/archive/pdf/Managing_DoS.pdf

[2] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the Slammer worm," *IEEE Security & Privacy Magazine*, vol. 1, no. 4, 2003, pp. 33-39.

[3] S. Staniford, V. Paxson, and N. Weaver, "How to own the Internet in your spare time," in *Proc of the 11th USENIX Security Symposium*, 2002. <http://www.icir.org/vern/papers/cdc-usenix-sec02/index.html>

[4] Computer Crime and Intellectual Property Section, *US Department of Justice* <http://www.usdoj.gov/criminal/cybercrime/ccpolicy.html#DDSA>

[5] M.-Y. Chow and Y. Tipsuwan, "Network-based control systems: a tutorial," in *Proc. 27th Conference of the IEEE Industrial Electronics Society*, Nov. 2001, Denver, CO, pp. 1593-1602.

[6] Y. Tipsuwan, M.-Y. Chow, and R. Vanijirattikhan, "An implementation of a networked PI controller over IP network," in *Proc. 29th Conference of the IEEE Industrial Electronics Society*, Nov. 2003, Roanoke, VA, pp. 2805-2810.

[7] Y. Tipsuwan and M.-Y. Chow, "Neural network middleware for model predictive path tracking of networked mobile robot over IP network," in *Proc. 29th Conference of the IEEE Industrial Electronics Society*, Nov. 2003, Roanoke, VA, pp. 1419-1424.

[8] S. Soucek, T. Sauter, and G. Koller, "Effect of delay jitter on quality of control in EIA-852-based networks," in *Proc. 29th Conference of the IEEE Industrial Electronics Society*, Nov. 2003, Roanoke, VA, pp. 1431-1436.

[9] J. Yopez, P. Marti, and J. Fuertes, "Control loop performance analysis over networked control system," in *Proc. 28th Conference of the IEEE Industrial Electronics Society*, Nov. 2002, Sevilla, Spain, pp. 2881-2885.

[10] K. Brady and T.-J. Tarn, "Internet-based teleoperation," in *Proc. 27th Conference of the IEEE Industrial Electronics Society*, Nov. 2001, Denver, CO, pp. 644-649.

[11] J. Woo and J. Lee, "Transmission modeling and simulation for Internet-based control," in *Proc. 27th Conference of the IEEE Industrial Electronics Society*, Nov. 2001, Denver, CO, pp. 165-169.

[12] A. Weaver, "Survey of industrial information technology," in *Proc. 27th Conference of the IEEE Industrial Electronics Society*, Nov. 2001, Denver, CO, pp. 2056-2061.

[13] L. Kleinrock, *Queueing Systems: Volume I—Theory*. New York: Wiley, 1976, pp. 8-9.

[14] Active Measurement Project, *National Laboratory for Applied Network Research, supported by the National Science Foundation (NSF)* http://watt.nlanr.net/active/maps/ampmap_active.php

[15] One-way Latency Measurement, *Internet 2, supported by the National Science Foundation (NSF)*, http://abilene.internet2.edu/ami/owamp_status_map.cgi/now

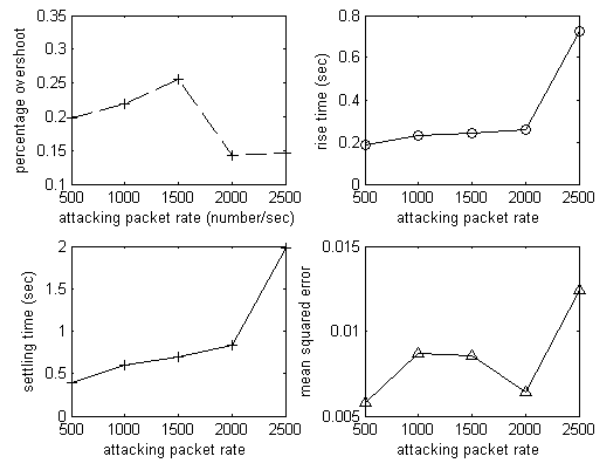


Fig. 5 Event-driven controller under model I DoS attacks. $\mu_0=3$ msec, background traffic load 60%, 50 samples/sec.

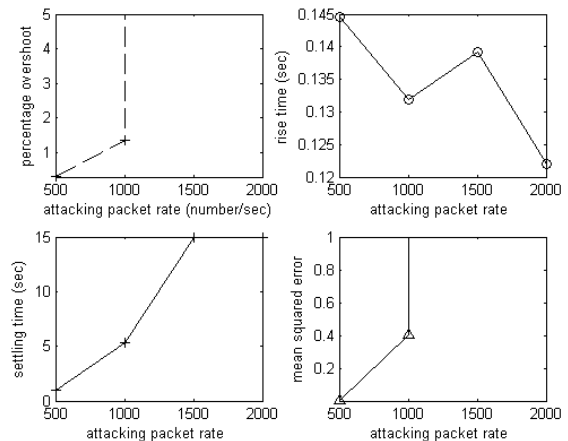


Fig. 6 Time-driven controller under model I DoS attacks. $\mu_0=3$ msec, background traffic load 60%, 50 samples/sec.

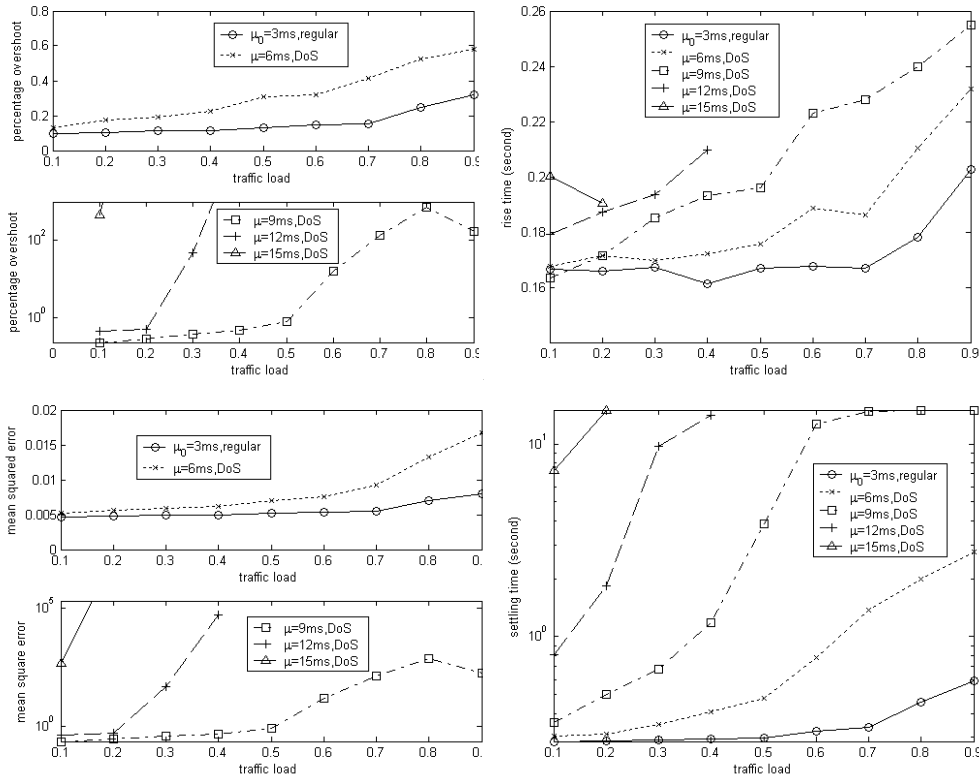


Fig. 7 Event-driven controller under model II DoS attacks. μ represents the severity of DoS attacks. X-axis: background traffic load

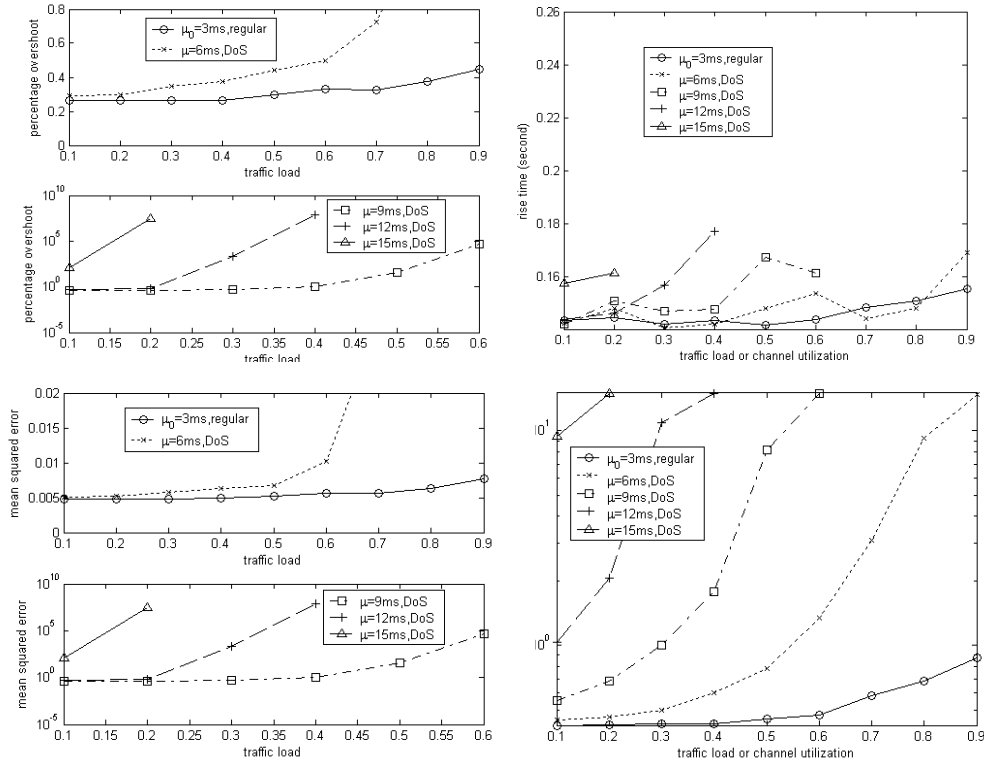


Fig. 8 Time-driven controller under model II DoS attacks. μ represents the severity of DoS attacks. X-axis: background traffic load