

# Mitigating Performance Degradation of 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**— One obstacle for the widespread deployment of network-based control systems (NBCS) is the stochastic delay induced by the underlying shared and open networks. Denial of service (DoS) attacks cause significant disruptions to the Internet, compounding the delay jitter and loss of packets that are used to transmit sensor measurements and control signals. Existing works have mainly focused on controller design under network normal operation, which might be inadequate to the threats of DoS attacks. In this paper, the authors present two mitigation measures from the viewpoint of network intrusion detection and response. The basic idea is that the routers close to the attack sources actively drop the attack traffic or lower-priority traffic to protect the resource for the legitimate application traffic. The simulation results indicate that the proposed defense measures are effective for ameliorating the NBCS performance degradation. We suggest that a plausible direction for the security of NBCS may combine the proposed network defense measures with specific controller design to compensate for delay jitter/packet loss.

## I. INTRODUCTION

The Internet connects hundreds of millions of computers across the world, and it has brought unprecedented innovative changes into commercial, industrial, and private use applications. On the other hand, this interconnectivity among computers also enables malicious users to misuse resources and mount DoS attacks against arbitrary websites or networks. For instance, in February of 2000 a series of massive DoS attacks incapacitated several high profile Internet sites including Yahoo and eBay; in October 2002 a fierce DoS attack brought down 8 of 13 root DNS servers in an effort to paralyze the Internet. Despite these noticeable attacks, the majority of attacks are not well publicized [1]. The victims of DoS attacks range from smaller commercial sites, to educational institutions, public chat servers, and government agencies. Another aspect of DoS attacks is that attack tools are readily available on the Internet and the detailed instructions allow even an amateur to use them effectively.

Today, the Internet takes on a bigger and bigger role in industrial control applications. Among the emerging technologies is NBCS, where open networks (Internet or other IP-based wide area networks) are used as mediums to transfer control data such as sensor measurements and control signals. The ubiquity of IP-based networks has the potential to make the remote control cost-effective and ease-of-maintenance, which has been supported by the increasing number of controllers with Ethernet and network programming stack modules [2].

Unfortunately, the Internet introduces the random delay and packet loss into control loops because the foundation of the Internet is a shared and open global network. Time periods to send a sensor measurement to a controller and to transmit a control signal to an actuator through the network have a large variance due to factors such as network topology and router congestion. It has been shown by field trials that the performance of NBCS is degraded by delay jitters/packet loss even if the underlying network has no anomaly [3]. DoS attacks will compound the performance degradation. Our earlier results have shown that the DoS attacks cause significant performance degradation or even destabilize the system [4].

Network attacks are unavoidable to the Internet and consequently they may hinder or discourage the development of NBCS. Nevertheless, the positive thing is that we have the opportunity to design the security solutions into these systems from the outset since NBCS is still in their early design and trial stages. The existing literature in the NBCS research has mainly emphasized on the design of control algorithms capable of handling the network time-varying delay. Some schemes have been shown to be effective under the normal network operation [3], but it is yet to be determined if these schemes are able to function under the DoS attacks, which generally cause much worse delay jitter/packet loss.

The contribution of this paper is to introduce network intrusion detection and response schemes into the field of NBCS security. The rationale is that NBCS is an interdisciplinary project involving both control engineering and computer networking. The performance of NBCS depends on the underlying network and thus a necessary step should include securing the network itself.

We propose one mitigation scheme that can be implemented by customer-edge routers to deal with the locally launched DoS attacks. The basic idea is that the local routers will start to drop the non-NBCS traffic when an attack is under way. Another possible scenario of DoS attacks is that attackers will attack the service-provider-edge routers few hops away from a controller or a plant. The effect is that the routers in the path between the plant and the controller become congested. In this case, the Internet service providers have to intervene and stop the attack traffic at source as soon as possible. We introduce the algorithm proposed in [5] into the defense where the basic idea is that the Internet routers store the digest of *en route* packets. As long as the attack traffic is identified, the routers will recursively trace the upstream sources of attack traffic until the origins. These edge

routers then cut off the attack traffic. The simulation results of the two algorithms indicate that they are effective in alleviating the DoS attacks. We suggest that a conceivable roadmap for NBCS security is to combine the tools of network defense with the techniques derived from control system design theory.

The remainder of the paper is organized as follows. In section II, we briefly review some important concepts and results of [4]. Some existing works on the NBCS controller design are also included. The background of DoS attacks is provided in this section as well. In Section III, we present the network mitigation algorithms along with the numerical simulation results. The conclusion is drawn in Section IV.

## II. BACKGROUND

In [4], we proposed two lumped queueing models to simulate two different types of the DoS attacks. The advantage of the models is the flexibility of adjusting the parameters to simulate different severity of the attacks even if attacks have not yet been deployed. The control system in [4] is a second-order plant with a discrete PI controller. Simulation results indicate that Model I DoS attacks (excessive packet loss) result in the slow response of the system, and Model II DoS attacks (increased delay jitter) contribute to higher transient overshoot, and even system instability.

Various NBCS control algorithms have been proposed, i.e. state augmentation [6], stochastic optimal control [7], and gain scheduling [3]. Reference [8] contains a detailed overview on the controller design and [4] lists a few representative works on the NBCS research within the industrial electronics society in the past a few years.

Roughly speaking, there are several general categories of DoS attacks, which can be divided into three classes: bandwidth attacks, protocol attacks, and software vulnerability attacks [9]. This paper focuses on the mitigation of the bandwidth attacks that are relatively straightforward in principle and common in the wild. This kind of attack exploits the throughput limits of computers and networking routing equipment by sending a large number of packets in a very short time span. Routers, servers and firewalls all have constraints on input-output processing, interrupt processing, CPU, and memory resources. Consequently, the network becomes stressed while handling the high packet rate during DoS attacks. In a nutshell, the attackers perform a careful reconnaissance beforehand to learn the connectivity and topology for a particular system of NBCS and then employ the available hosts to send the spurious packets to the endpoints or the victim routers to disrupt the normal communication.

## III. MITIGATION MEASURES AND NUMERICAL SIMULATION

In this section, the authors evaluate how network intrusion detection and response measures ameliorate the performance degradation caused by DoS attacks. The defense to the DoS attacks is an active research area and currently there is no complete solution to this problem. The basic idea of

mitigation is for routers to identify the attack traffic and then block it. We refer readers to [10], [11] for a detailed description of some recent progresses in defense techniques. Throughout this section, the event-driven controller is assumed.

### A. Countermeasure to DoS Attack Model I (Larger Packet Loss)

Since this type of DoS attack is launched locally, the routers within the victim corporate network might detect and stop the attack traffic. It is a common practice for a network to install an intrusion detection system that observes the passing traffic. For instance, if the traffic packet rate is above a certain threshold, the router can reason that a DoS attack is likely taking place, and then can actively drop the background or non-NBCS traffic. In Fig. 1, we propose a simple algorithm to realize this countermeasure.

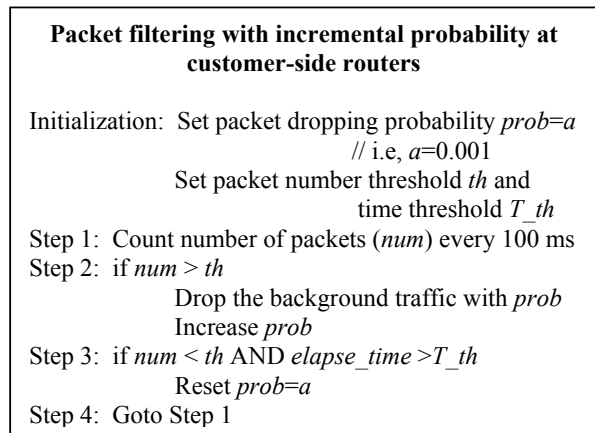


Fig. 1 Algorithm counteracting Model I DoS attacks

The rationale of the algorithm is that customer-side routers in a corporate network can distinguish NBCS traffic from other background traffic. Furthermore the NBCS traffic can be given a higher priority. The router begins to drop the background traffic from an initial small probability if the packet arrival rate is higher than the prescribed  $th$  (rate threshold). Then the router increases  $prob$  (packet dropping probability) until the packet rate is below the threshold. If the time duration  $elapsed\_time$ , under which packet rate is less than  $th$ , is greater than the prescribed  $T_{th}$  (time duration threshold), then  $prob$  will be reset to the small initial value.

The effect of the algorithm on NBCS is simulated and the factor in simulation is the elapsed time  $t$  from the onset of an attack to router successfully blocking the attack traffic. Thus, in our model, the packet rate of attack traffic experiences the original exponential growth, but at  $t$  sec ( $0 < t < 15$ ), the attack traffic rate will reduce from the original value to the ideal value of zero.

It has been seen in the DoS attack simulations that different severity of DoS attacks tends to yield different values of  $t$  when the mitigation algorithm is in place. We run 10 replications for a simulation and the average result of performance under different values of  $t$  is reported in Table I, which shows that the rise and settling times and the mean

squared error are significantly reduced by the mitigation measure. For example, without mitigation, the rise time is 0.72 sec; with  $t=1$  sec it reduces to 0.527 sec. Table I also indicates that earlier intrusion detection and packet filtering is better to ameliorate performance degradation. Fig. 2 (a) plots the time domain description of the delay jitter/packet loss without mitigation, and Fig. 2 (b) with the mitigation ( $t=1$  sec). Each time domain plot is drawn from one instance of simulation runs. Comparing Fig. 2 (a) to Fig. 2 (b), we observe that the mitigation mends the packet loss so that the system response becomes faster.

Table I. Mitigation against DoS attack model I with  $ack\_mag=2500$  packets/sec,  $\mu_0=3$  msec, and 60% background traffic load (event-driven

| $t$ (sec):<br>network<br>defense<br>response<br>time | controller) |                    |                         |          |
|--|-------------|--------------------|-------------------------|----------|
|  | PO          | Rise time<br>(sec) | Settle<br>time<br>(sec) | MSE      |
| No<br>mitigation                                     | 0.14857     | 0.72344            | 2.11                    | 0.12403  |
| 5  | 0.14124     | 0.6845             | 1.9784                  | 0.10694  |
| 1  | 0.1219      | 0.52705            | 1.1193                  | 0.012399 |
| 0.5  | 0.15874     | 0.4468             | 0.6763                  | 0.009165 |

$ack\_mag$  represents the severity of DoS attack Model I;  $\mu_0$  influences delay jitter/packet loss under the normal status of networks [4].

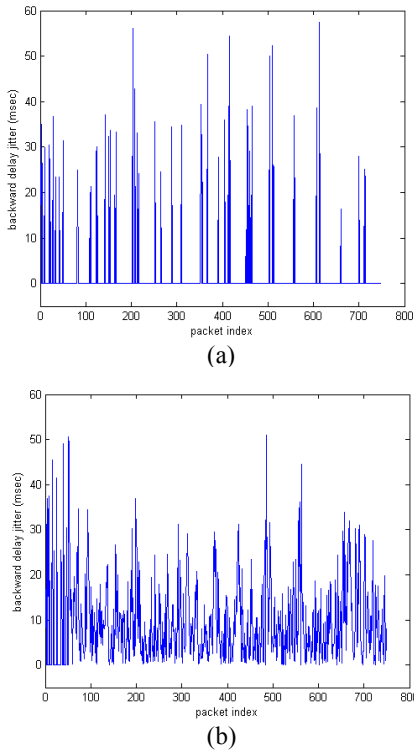


Fig. 2 backward delay jitter (a) DoS attack model I,  $ack\_mag=2500$  packets/sec,  $\mu_0=3$  msec, 60% traffic load, (b) mitigation for DoS attack model I,  $t=1$  sec. Backward delay jitter is the one from the sensor to the controller, and we treat the jitter to be 0 in the case of packet loss.

### B. Countermeasure to DoS Attack Model II (Longer Delay Jitter)

Under Model II, remote attackers send a flood of traffic to the service-provider-edge routers close to an endpoint of a NBCS system. The difference in this case is that intermediate routers in the Internet may not distinguish the particular NBCS traffic from other application traffic. Nevertheless, it is reasonable to expect that the attack traffic rate is much higher than that of NBCS traffic. In a probabilistic sense, the likelihood of dropping NBCS packets will be lower than that of dropping attack packets. Since the attack sources are located somewhere on the Internet, the desirable strategy of the Internet service providers (ISPs) is to identify the attack traffic and then cut off the attack traffic at the source.

An effective countermeasure system was proposed in [5]. The idea is that the Internet routers generate audit trails for traffic passing through and then trace the origin of the attack packets upon the request of an endpoint. In other words, the ISP router closest to the victim initiates the process of interactively testing the upstream links. This procedure is recursively repeated on the upstream router until the routers determine which ones are used to carry the attackers' traffic. Then the attack traffic is cut off at the edge. The algorithm is listed in Fig. 3, which is self-explanatory. One innovation of the method is that routers store the packet digest instead of the packet itself by using a special technique of hash functions. Consequently, the memory requirement for Internet routers is significantly reduced.

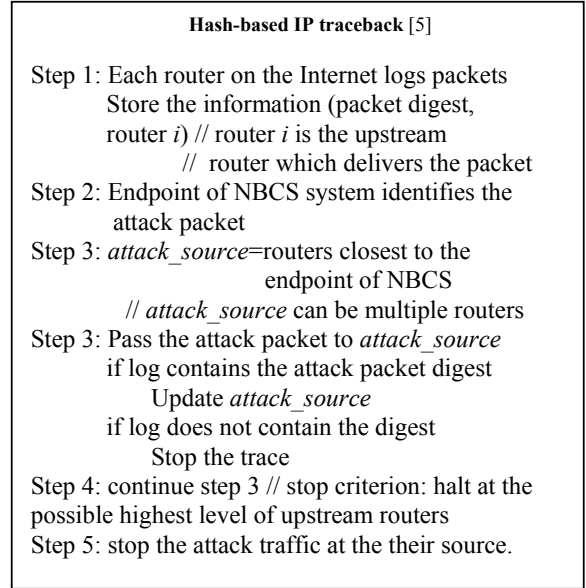


Fig. 3 Algorithm counteracting Model II DoS attacks

The effect of the algorithm on NBCS is simulated and the factor in simulation is again the elapsed time  $t$  from the onset of an attack to router successfully blocking the attack traffic. We model the effect by decreasing  $\mu$  to a lower value  $\hat{\mu}$  ( $\mu$  represents the severity of DoS attack Model II [4]). In the simulation, we choose the case of  $\mu=15$  msec and background non-attack traffic load of 10% because without

mitigation this case is unstable [4]. After  $t$  ( $0 < t < 15$ ) sec, the mean service time will decrease to  $\hat{\mu} = 4$  msec ( $\mu_0 = 3$  msec represents network regular status). We run 10 replications for a simulation and the result under different values of  $t$  is reported in Table II. The system will have moderate performance degradation when the network intrusion detection can quickly respond to the attacks. For example, without the mitigation the percentage overshoot is 468.5; with  $t=2$  sec it significantly reduces to 1.035. Fig. 4 (a) plots the time domain description of the delay jitter/packet loss without mitigation, and Fig. 4 (b) with the mitigation ( $t=2$  sec). Each time domain plot is drawn from one instance of simulation runs. The beginning interval of Fig. 4 (a) is similar to the pattern of Fig. 4 (b), but the later intervals of the two figures exhibit sharp difference.

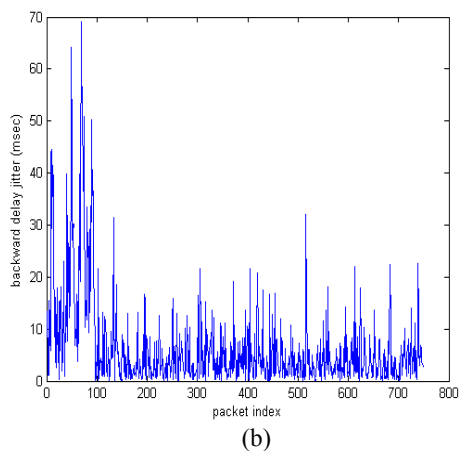
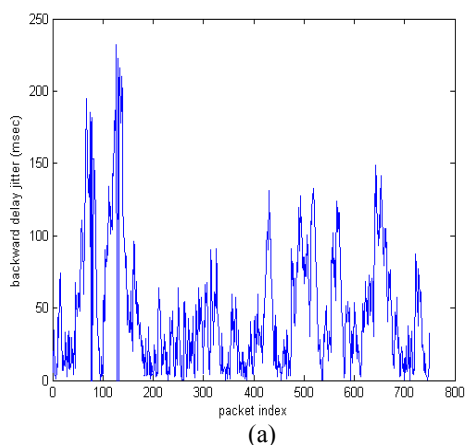


Fig. 4 backward delay jitter (a) DoS attack model II,  $\mu = 15$  msec, 10% traffic load, (b) mitigation for DoS attack model II,  $t=2$  sec.

Table II. Mitigation against DoS attack model II with  $\mu = 15$  msec and 10% background traffic load (event-driven controller)

| $t$ (sec):                    | PO      | Rise time (sec) | Settle time (sec) | MSE      |
|-------------------------------|---------|-----------------|-------------------|----------|
| network defense response time |         |                 |                   |          |
| No mitigation                 | 468.5   | 0.20009         | 7.2761            | 165810   |
| 4                             | 3.2637  | 0.23571         | 3.1345            | 0.36133  |
| 2                             | 1.035   | 0.19611         | 1.8157            | 0.045174 |
| 1                             | 0.95544 | 0.20554         | 1.5458            | 0.046426 |

$\mu$  represents the severity of DoS attack Model II [4].

#### IV. CONCLUSION

In essence, the Internet is an open network with security vulnerabilities. It is foreseeable that the growing deployment of NBCS may draw attention from both amateur and well-equipped attackers. This paper has brought the network defense measures into the area of NBCS security. We suggest that the security of underlying networks is indispensable to the NBCS security and present two network mitigation algorithms to defend against the DoS attacks. The future of NBCS security may combine both the network intrusion response and the specific controller design.

#### V. REFERENCES

- [1] D. Moore, G. M. Voelker, and S. Savage, "Inferring Internet denial-of-service activity," in *Proc of the 10th USENIX Security Symposium*, 2001, Washington, DC.
- [2] 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.
- [3] 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.
- [4] M. Long, C.-H. Wu, J. Y. Hung, and J. D. Irwin, "Network security models for analyzing network-based control systems under denial of service attacks," in *Proc. 30th Conference of the IEEE Industrial Electronics Society*, Nov. 2004, Busan, Korea.
- [5] A. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S. T. Kent, and W. T. Strayer, "Single-packet IP traceback," *IEEE/ACM Trans. Networking*, vol. 10, no. 6, Dec. 2002, pp. 721-734.
- [6] Y. Halevi and A. Ray, "Integrated communication and control systems: part I-analysis," *ASME Journal of Dynamic Systems, Measurement, and Control*, vol. 110, no. 4, 1988, pp. 367-373.
- [7] J. Nilsson, B. Bernhardsson, and B. Wittenmark, "Stochastic analysis and control of real-time systems with random time delays," *Automatica*, vol. 34, no. 1, 1998, pp. 57-64.
- [8] 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.
- [9] 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](http://www.cert.org/archive/pdf/Managing_DoS.pdf).
- [10] H. Aljiffri, "IP traceback: a new denial-of-service deterrent," *IEEE Security & Privacy Magazine*, vol. 1, no. 3, May-June 2003, pp. 24-31.
- [11] R. Chang, "Defending against flooding-based distributed denial-of-service attacks: a tutorial," *IEEE Communication Magazine*, Oct. 2002, pp. 42-51.