2009-IOT-4（9）
2009 / 3 / 5

XCP ルータの輻輳制御に関する不正動作手法に関する調査

レーヒェウハン† 嶋村 昌義†† 益井 賢次††† 飯田 勝吉†††

† 東京工業大学 大学院理工学研究科
†† 九州工業大学 ネットワークデザイン研究センター
††† 東京工業大学 学術国際情報センター
E-mail: †hanhlh@netsys.ss.titech.ac.jp, ††shimamura@ndrc.kyutech.ac.jp, †††{kmasui,iida}@gsic.titech.ac.jp

あらまし ネットワークの状態を送信ホストにフィードバックするルータを用いることで，帯域遅延積の大きなネットワークにおいて，ネットワークの公平性と安定性をより効果的に提供する XCP が提案されている．しかし XCP においては，ルータが不正な動作を行うとシステム全体の性能に大きな悪影響が生じてしまうことが考えられる．本稿では，今後の対策法の検討に役立てるため，XCP ルータの輻輳制御の不正動作手法について調査する．

キーワード 輻輳制御，XCP，ルータ不正動作

A study on XCP routers' misbehaviors on congestion control

Hieu Hanh LE†, Masayoshi SHIMAMURA††, Kenji MASUI†††, and Katsuyoshi IIDA†††

† Graduate School of Science and Engineering, Tokyo Institute of Technology
†† Network Design Research Center, Kyushu Institute of Technology
††† Global Scientific Information and Computing Center, Tokyo Institute of Technology
E-mail: †hanhlh@netsys.ss.titech.ac.jp, ††shimamura@ndrc.kyutech.ac.jp, †††{kmasui,iida}@gsic.titech.ac.jp

Abstract Recently, the XCP in which routers are used to control congestion has been proposed in order to provide efficient, fair and stable network in high bandwidth-delay environment. However, it is also considerable that the performance of XCP is effected by routers' misbehavior. In this paper, towards the solution for this issue, we study the possible misbehaviors of routers and evaluate the effect of these to XCP performance relating to bandwidth allocation and network utilization.

Key words Congestion control, XCP, Misbehaving router

1. Introduction

The Transmission Congestion Protocol (TCP) using packet drop as a signal to implicitly control congestion at end-hosts has provided stable, fair and high-utilization network. However, it has been confirmed by theory and experiments that in future network when the bandwidth-delay product increases, which means the link capacity becomes larger, TCP becomes inefficient and prone to instability [1].

In order to deal with this issue, a number of research to develop novel approaches as router supported control congestion have been proposed . In 1994, Floyd [2] extended TCP by adding an Explicit Congestion Notification (ECN) as an option bit which is used by routers to explicitly signal the congestion of network to end-hosts. Later, ECN was also standardized as RFC 3168 [3] in 2001. Next, Katabi et al. [4] has proposed an eXplicit Control Protocol (XCP) which controls congestion by returning feedback information included in packet header to end-hosts.

It has been reported that this approach outperforms TCP in the throughput, packet loss rate, fairness and network utilization in high bandwidth-delay product network. However, the investigation done by Pentikousis et al. [5] shows that the ECN implemented routers have not been widely used. One of the considerable reasons is the security issue of forging the congestion signaling bit at routers [6]. It is considered as a common problem in router supported congestion controls when routers have not operated as defined in theory. Here we define such kind of routers as misbehaving routers.

The first approach deal with the aforementioned forgery of congestion signaling bit at routers was proposed by Savage et al. in 1999 [7]. The authors extended the ECN to 2 bits,

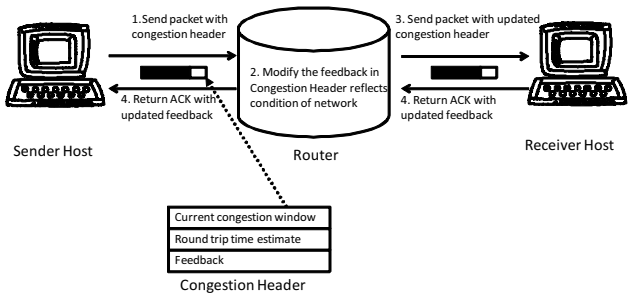


Figure 1 Illustration of XCP

added the random 1-bit Nonce to the sender-hosts and verified the exactness of receiver's behavior predefined in RFC by the operation of this bit with certain rules. Later, Ely et al. [8] proposed a more robust security method by extending Nonce to 16 or 32 bits. However, as indicated in [9], [10], Nonce is still not enough to guarantee the safety of devices (end-hosts and routers) but only protect from smart mischief. In the future, it is necessary to provided a more robust security framework for the next generation network infrastructure.

Our research, there upon, aims to analyze the security protocol, and then to propose a more robust mechanism of router supported congestion control. In order to achieve this, this paper provides a study on misbehaviors of XCP routers on congestion control. In this paper, at first, we suggest a number of misbehaviors which can occur at routers. Next, we perform simulations to study the effects of misbehaving routers to the performance of XCP related to the fairness between flows and the utilization of network. From the simulation results, it is considered that the malicious ISPs who are supposed can control the routers can take advantage of the suggested methods to unfairly provide special services to their customers.

The remainder of this paper is organized into the following sections. At first, we take an overview of XCP in Sect. 2. Next we propose misbehaving methods at XCP router in Sect. 3, and report the simulation and discuss the results in Sect. 4. Concluding remarks and possibilities for future work are given in Sect. 5.

2. XCP

2.1 The basic idea of XCP

XCP is believed to outperform TCP in conventional environment, and further remains efficient, fair, and stable as the link bandwidth and/or the round-trip delay increases. Figure 1 illustrates XCP's mechanism in terms of its protocol and normal behavior. As shown on this figure, XCP packet includes a congestion control header that contains the sender-host's current congestion window, round trip time (RTT) estimate, and a reverse feedback value from the network intended for the packet's recipient. While in transit, XCP-enabled routers can modify the value in the congestion header to reflect the desire for the sender to increase or decrease its congestion window size due to locally observed network conditions. The receiver host uses the reverse feedback value to update its own congestion window, then copies the modified congestion window value into the reverse feedback field of the next packet to be sent. Feedback for each host is built up as they send packets, and the recipient forwards network feedback back to the sender during acknowledgment through the reverse feedback header field. This feedback system enables routers to control exactly how much data flows through them while storing no per-flow state. Routers can prevent congestion by instructing hosts to reduce their windows' values and can keep utilization high in the event of having the unused bandwidth by instructing hosts to increase their windows' values. Fairness is imposed by the same mechanism; any host which reports an anomalous congestion window value will be told to equalize their window size with all other hosts that are sharing the same link.

2.2 Security issue in XCP

Wilson et al. [11] has proposed possible fairness attacks that can be utilized at end-hosts in XCP. In this paper, the authors has suggested that while XCP works exceptionally well when all nodes follow the recommendations of network feedback, it creates an environment that can easily be exploited by a small number of misbehaving end-hosts. Firstly, sender-hosts can ignore or overwrite the router feedback values and then boost their own allocated bandwidth by manipulating the network feedback. Next, there is also a possible that receiver-hosts can mislead the sender-host to generate a denial-of-service attacks on other hosts or routers on the end-to-end path. Therefore, XCP is believed to result in unfair bandwidth allocation and be difficult to detect the DoS attacks in high bandwidth networks.

To encounter with such issue, the newest XCP draft [12] proposes using monitoring techniques in edge routers to police the security of network. For example, when the police sees the negative feedback heading towards a sender-host and no reduction in the throughput, it may punish the flow by severely restricting the throughput. However, this proposal is only used to discover the malicious end-hosts but not the routers which play a very important role in the mechanism of router supported congestion control.

3. Misbehaviors of XCP Router

In this section, we suggest a number of misbehaviors of routers which can lead to the diminishing of XCP performance. In XCP, in order to utilize high utilization rate, stable and fair network, the congestion window of sender-hosts

are adjusted by using the feedback calculated by routers corresponding to network's condition. However, because depending on the correct of feedback calculation, XCP performance can be decreased in the case of routers are impossible to provide the correct feedback such as routers are failed or be controlled by malicious users.

3.1 Failure Router

The considerable simplest misbehavior of router is the failure of it. For some reasons, when the router cannot correctly calculate the feedback value but always set this value to a certain value. For example, when this value is set to 0, sender-hosts consequently cannot change their congestion window. Hence, they cannot increase their throughputs although there are still a lot of possible empty bandwidth in network. As consequence, the utilization of the bottleneck link is decreased.

3.2 Controlled Router

Different from the above misbehavior, here we suggest a method of allocating the available bandwidth to specific users by using the feedback value calculated at routers. We assume that the routers are controlled by a malicious user, who always wants bandwidth as much as possible from the network. Although it is considerable that the a malicious user can stop all of other flows' traffic when controlling the router, here we present a method by which an almost exactly given bandwidth from network can be allocated to this flow. For instance, nonetheless how many flows are there in the network, the specific flow always wants 50% bandwidth from network. This causes the network loosing the fairness between flows in terms of congestion control.

Firstly, the optimized congestion window is calculated at router corresponds to the wanted bandwidth of specific flow from network by next formula:

$$\mathrm{cwnd}_{\mathrm{opt}} = \frac{\mathrm{bandwidth} \times \mathrm{RTT} \times \alpha}{\mathrm{PacketSize}}, \qquad (1)$$

where $\mathrm{cwnd}_{\mathrm{opt}}$ is the optimized congestion window, bandwidth is the possible bandwidth of network, RTT is round trip time and α ($0 \leqq \alpha \leqq 1$) is the parameter to adjust the wanted bandwidth for specific flow.

Next, the current congestion window of this flow is converged to the optimized congestion window calculated from (1) at controlled routers. Because of the necessary of assuring the stability of network, it is thought to utilize the converging process by adjusting the feedback value from the feedback calculated when routers are normal as below:

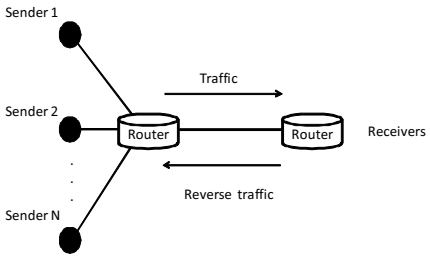


Figure 2 Single bottleneck topology

$$\mathrm{feedback} = \begin{cases} -|\mathrm{feedback}| & \mathrm{cwnd} > (1+\varepsilon) \times \mathrm{cwnd}_{\mathrm{opt}}, \\ |\mathrm{feedback}| & \mathrm{cwnd} < (1-\varepsilon) \times \mathrm{cwnd}_{\mathrm{opt}}, \\ 0 & \text{otherwise.} \end{cases} \qquad (2)$$

where cwnd is the current congestion window, ε ($0 \leqq \varepsilon \leqq 1$) is the acceptable error rate when converging cwnd to $\mathrm{cwnd}_{\mathrm{opt}}$. The smaller ε is, the more precision the algorithm receives.

4. Simulation

The purpose of our simulation is to verify the aforementioned misbehaviors and to study the effect of these misbehaviors to the performance of XCP in the real network. In order to perform this, we implemented the idea and compared the results with the normal case, when there is no misbehaving router in network relating to bandwidth and network's utilization.

4.1 Simulation environment

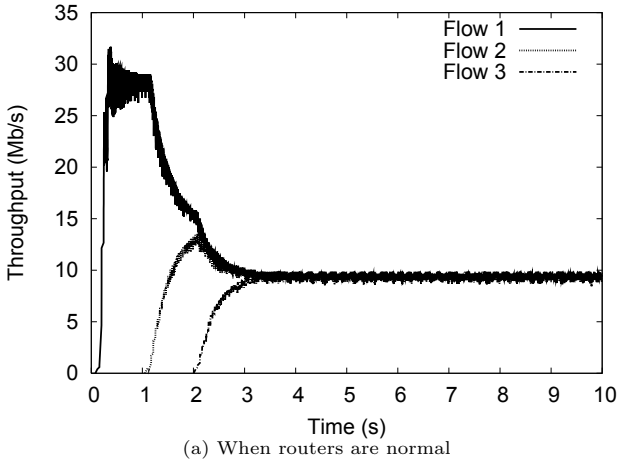
For our tests, we modified the classes related to XCP in ns-2.33 [13] to enable control the feedback value at router. The network topology is shown in Fig. 2 where 3 flows share one bottleneck link and each flow is initiated after each 1 second interval. The simulation was performed with a 30[Mb/s] network bottleneck, 10[ms] delay, and 1,000[Byte] packet size.

4.2 Failure Router

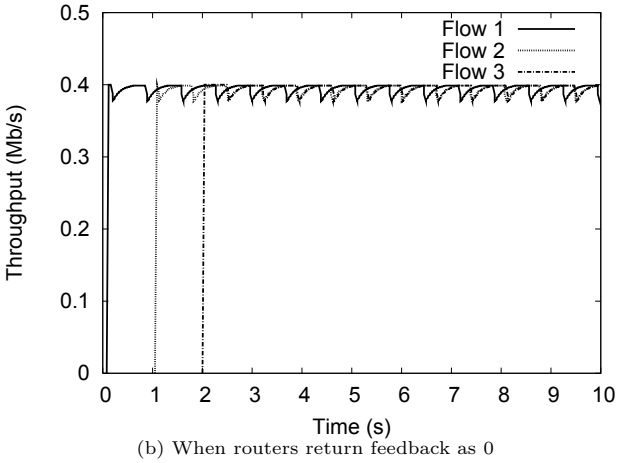
We simulated the aforementioned failure of routers when routers return the feedback value to 0. Obviously, the other value could be chosen but it does not change the nature of the simulation. The simulation results are shown in Fig. 3 and 4.

In Fig. 3(a), in the case of routers are normal, the fairness of flows were guaranteed as all the flows received almost the same throughput of almost 10[Mb/s]. However, because of the broken down of XCP routers, all the flows' congestion windows were not be changed from being initialized, hence they could not received more in spite of there are still spare bandwidth in network (Fig. 3(b)).

It can be seen from Fig. 4 that the utilization of the bottleneck link was badly effected by routers failure. When the routers are normal, the utilization of network was extremely



(a) When routers are normal



(b) When routers return feedback as 0

Figure 3 Throughput of flows

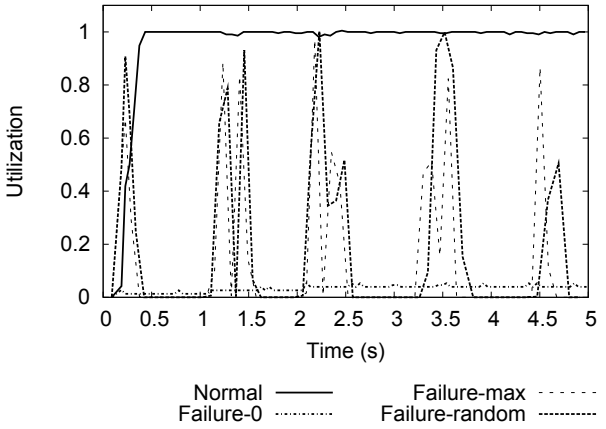


Figure 4 Link utilization when routers are failure and normal

near 1. In contrast, it was significantly decreased to under 10% when the routers return the feedback value to 0. This simulation was also performed when feedback value was returned as a random number generated from the range of 0 to the capacity of link (30[Mb/s]), and a possible maximum number of **long int** type. The results shown that the utilization of link was effected highly by the feedback value. Therefore, when malicious ISPs are possible to control the routers, they can allocate the sharing bandwidth to their customers by adjusting this feedback value. However, as from the above results, it is necessary to find out the optimized value of the adjusted feedback to guarantee the stable and high utilization of network.

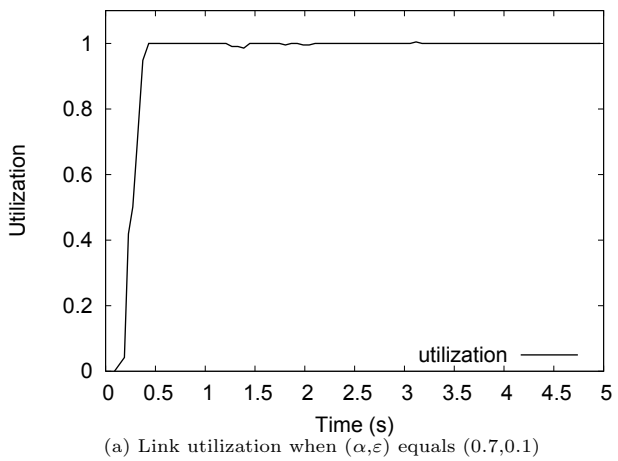
4. 3 Controlled Router

We evaluated the algorithm suggested at Sect. 3. 2 with 3 flows and set the specific flow to Flow 2. Figures 5(a) and 5(b) demonstrate the simulation results of specific flow's bandwidth and link utilization when α in (1) and ε in (2) was temporally fixed as 0.7 and 0.1, which means that the specific flow's bandwidth was assigned as 70% of link's bandwidth with the precision 90%. From this result, it is seen that the proposed method at controlled XCP router can allocate given bandwidth to specific flow while keeps the network stable and at high utilization. Because the specific flow receives more bandwidth than normal by implementing this method, all the other normal flows have to share the remains, which become much smaller than the original. Obviously, lessening the bandwidth of specific flow is also considerable. Figure 5(c) shows the bandwidth of flows when α was fixed as 0.2. From these results, it can be suggested that the proposal method can be used by malicious ISPs to provide a special service for their users.

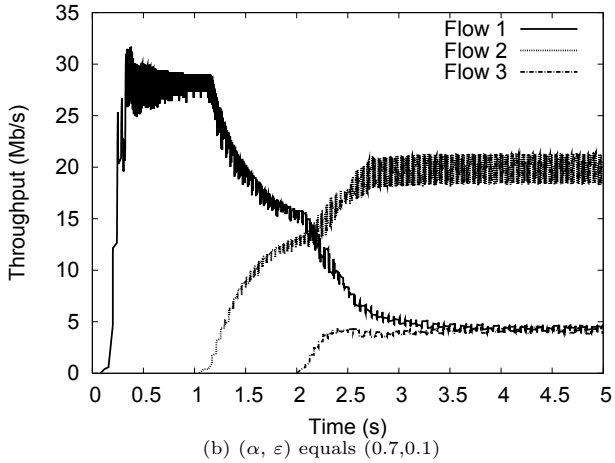
We also performed another set of simulation to verify the effect of parameter ε relating to the precision of converging the specific flow's bandwidth to its requested one. Figures 5(d) and 5(e) demonstrate the results when the precision was heightened by decreasing ε to 0.05 and 0.01. It can be recognized that the stable of network became worse when we tried to increase the precision. The considerable reason is the proposed method is still not good enough to converge the current congestion window of specific flow to the purpose value. In contrast, Fig. 5(f) shows the throughput of flows when ε was set to 0.2, which means the precision of algorithm become smaller. Although the stable of the network was assured, but the allocated bandwidth for the specified flow, i.e. Flow 2, was not reached to the expected value (about 18[Mb/s] instead of 21[Mb/s]). Hence, it is thought that the algorithm was quite good at the precision of about 10%.

4. 4 Discussion

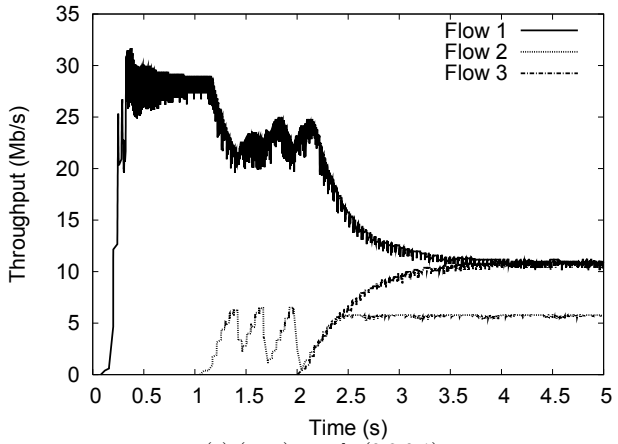
The simulation results confirm that the designers of XCP is aware of the possibility of misbehaving routers. In terms of the security of router, a network device, Hardjono [14] proposed a technique for detecting and locating a misbehaving router in network. The proposal divides network domain



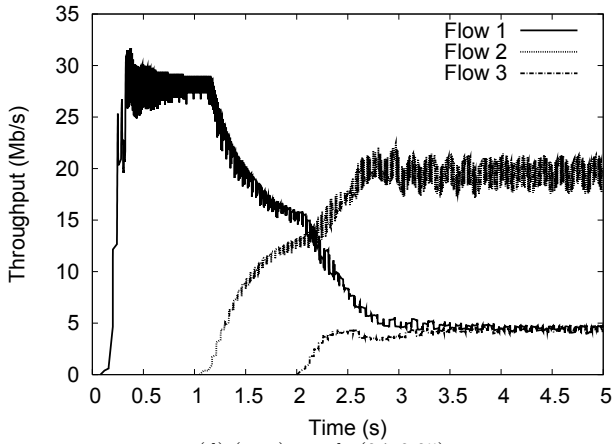
(a) Link utilization when (α,ε) equals (0.7,0.1)



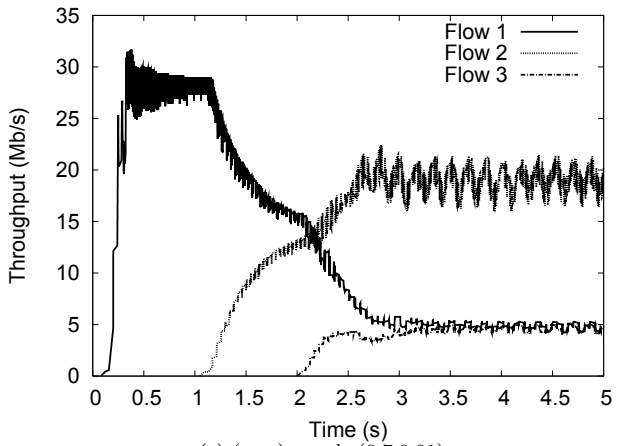
(b) (α, ε) equals (0.7,0.1)



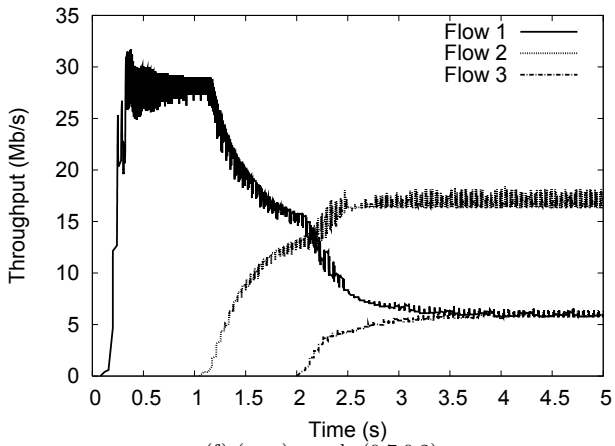
(c) (α, ε) equals (0.2,0.1)



(d) (α, ε) equals (0.7,0.05)



(e) (α, ε) equals (0.7,0.01)



(f) (α, ε) equals (0.7,0.2)

Figure 5 Simulation results - Controlled Router

into multiple sectors that each contains a secure and trusted authority and a number of device, and use a two-level authentication scheme to allow a receiving device to authenticate that a particular packet originated in a particular device. This leads to the possibility of applying the code signing technique to assure the operation of routers as defined in a trusty party such as RFC.

5. Conclusion and Future Works

In this paper, we suggested two types of misbehaving XCP routers (i.e. failure routers and controlled routers) which are possible to cause the diminishing of XCP performance, especially the fairness of network. We verified this suggestion by performing simulation. The simulation results indicated that the method utilized at controlled routers can be used to unfairly allocated available network's bandwidth by malicious

ISPs to their customers at quite high precision.

In the future, we plan to do the following:

- Perform a more detailed verification of the proposed method at controlled router using more complex topologies.
- Consider the possibility of applying code signing techniques to guarantee the operation of routers on network. As the performance of routers are assured by trusted party, the security issue of forgery of the feedback information from router is thought to be settled.

Acknowledgements

This work was supported in part by the National Institute of Information and Communications Technology, Japan.

References

[1] S. Low, F. Paganini, J. Wang, S. Adlakha, and J. Doyle, "Dynamics of TCP/AQM and a Scalable Control," Proc. IEEE INFOCOM 2002, vol. 1, pp. 239–248, 2002.

[2] S. Floyd, "TCP and Explicit Congestion Notification," ACM SIGCOMM Comput. Commun. Rev., vol. 24, no. 5, pp. 8–23, 1994.

[3] K. Ramakrishnan, S. Floyd, and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP," IETF RFC3168, 2001.

[4] D. Katabi, M. Handley, and C. Rohrs, "Congestion Control for High Bandwidth-Delay Product Network," Proc. ACM SIGCOMM2002, 2002.

[5] K. Pentikousis, and H. Badr, "Quantifying the Deployment of TCP Options - a Comparative Study," IEEE Commun. Letters, vol. 8, no. 10, pp. 647–649, 2004.

[6] S. Floyd, "ECN and Security Concerns," `http://www.icir.org/floyd/ecn/ecn_security.txt`, 1998.

[7] S. Savage, N. Cardwell, D. Wetherall, and T. Anderson, "TCP Congestion Control with a Misbehaving Receiver," ACMSIGCOMM Comput. Commun. Rev., vol. 29, no. 5, pp. 71–78, 1999.

[8] D. Ely, D. Wetherall, S. Savage, and T. Anderson, "Robust Congestion Signaling," Proc. IEEE Intn'l Conference on Network Protocols (ICNP2001), pp. 332–341, 2001.

[9] S. Floyd, M. Allman, A. Jain, and P. Sarolahti, "Quick-start for TCP and IP," IETF RFC 4782, 2007.

[10] P. Sarolahti, S. Floyd, and M. Kojo, "Transport-layer Consideration for Explicit Cross-layer Indications," IETF internet-draft, draft-sarolahti-tsvwg-crosslayer-01.ps, 2007.

[11] C. Wilson, C. Coakley, and B. Zhao, "Fairness Attacks in the Explicit Control Protocol," Proc. IEEE Intn'l Workshop on Quality of Service (IWQoS2007), pp. 21-28, 2007.

[12] A. Falk, Y. Pryadkin, and D. Katabi, "Specification for the Explicit Control Protocol (XCP)," IETF internet-draft, draft-falk-xcp-spec03.txt, 2007.

[13] "The Network Simulator ns-2," `http://www.isi.edu/nsnam/ns`.

[14] T.P.U. Hardjono, "Detecting and Locating a Misbehaving Device in a Network Domain," `http://patentstorm.us/patents/6425004.html`, 2000.