Abstract. ATC (Abnormal traffic controller) is presented as next generation security technology to securely support reliable Internet service in traffic-intended unknown attack. The key concept of the ATC is abnormal traffic monitoring and traffic control technology. When fault factors exist continuously and/or are repeated, abnormal traffic control guarantees service completeness as much as possible. The ATC with control policy on abnormal traffic is superior to the ATC with blocking policy as well as conventional network node, when the ratio of effective traffic to abnormal traffic is higher than 30%. As the proposed ATC can be applied to the edge point of backbone network as well as Internet access point, it guarantees network survivability and provides reliable Internet service.

1 Introduction

Recently the trend of cyber attack is shifted from simple system attack to network attack that makes specific service stopped [1,2]. As an example, Internet worm made Internet service stopped in Jan. 25, 2003. Unknown attack is becoming current trend in global network environment. When unknown attack occurs, network nodes mainly make a decision that input traffic is not malicious but suspicious traffic. If most of abnormal traffic is the traffic made by malicious attack, it is meaningless to serve abnormal traffic. Therefore, we need a mechanism to control abnormal traffic.

In security aspects, representative researches on reliable Internet service are DARPA FTN (Fault tolerant network) [3] and Arbor Inc. Peakflow [4]. When Peakflow measures, aggregates and correlates security data, it depends on traffic analysis of the CISCO netflow. It can be only applied to the environment that CISCO routers exist.

In this paper, ATC (Abnormal traffic controller) is presented as next generation security technology to securely support reliable Internet service. The key concept of the ATC is abnormal traffic monitoring and traffic control technology. When fault factors exist continuously and/or are repeated, abnormal traffic control guarantees service completeness as much as possible.
This paper is organized as follows: next section presents a general description of the concept of the ATC. The tele-traffic model is presented in section 3 and performance measures in section 4. In section 5 some numerical results are presented that indicate the performance improvement achieved by the ATC scheme while in section 6 conclusions are given.

2 The Proposed Scheme

Recently unknown attack frequently happens and it will be usual in the future. In the case of unknown attack, security devices such as IDS, IPS and security appliance have false-positive decision about ISP ingress traffic from customer network.

Security device has a difficulty whether it makes blocking or passing abnormal traffic, because some of abnormal traffic is effective traffic, where the effective traffic means not a corrupted traffic but a real traffic generated by the Internet user. The proposed ATC as shown in Figure 1 has a security policy of soft firewall function on abnormal traffic to protect effective traffic among abnormal traffic.

Assume that the ATC is located nearby access network nodes such as DSLAM in ADSL technology. The ATC is a kind of front-end-processor and is operated as plug-in type in network node or standalone system. Consider that the ATC monitors the start time and the end time of virtual connection per a session. For session management in security node, Internet traffic can be modeled as Erlang loss formula like voice traffic.

Assume that the Packet Monitor can perform flow based packet monitoring. If a packet is doubted as a corrupted packet, it is considered as abnormal traffic. Giving the lower priority to the abnormal traffic controls abnormal traffic. Control policy can be blocking or rate limiting. By doing so, corrupted packets have a lower survivability and total throughput may be increased.

![ATC service model](image)

**Fig. 1.** ATC service model