PROJECT DESCRIPTION

1 Introduction

To gain back the trustworthiness of Internet infrastructures and network-centric computer systems, it is critical to improve the *measurable* performance of network systems under cyber attacks and threats, and to provide end users with timely information and more control. This IMPACT project focuses on the research and design of a high confidence software framework that supports the dynamic configuration and deployment of adaptive intrusion detection systems (IDSs), and support distributed real-time control for managing intrusion detection and responses. A prototype system will be developed to demonstrate the effectiveness of IMPACT framework on improving measurable performance of cyber infrastructures. Curriculum development discussion here briefly also?....

1.1 Motivations

The proliferation of Internet applications and network-centric mission-critical services is bringing network and system security issues to the fore. The past few years have seen significant increase in cyber attacks on the Internet, resulting in degraded confidence and trusts in the use of the Internet and computer systems. The cyber attacks, including email virus, worms, and DDoS, are getting more sophisticated, spreading quicker, and causing more damage. Attacks originally exploited the weakness of the individual protocols and operating systems but now have started to target the basic infrastructure of the Internet. To gain back the trustworthiness of Internet infrastructures and computer systems, there is an urgent need to enhance the dynamics and effectiveness of the cyber defense systems, to provide people with timely intrusion response and more control, and to improve the measurable performance of network systems when under attack.

Improving the measurable performance against cyber threats requires a multi-faceted research program that includes:

- design of adaptive IDSs, taking into account quality-of-service (QoS) control technologies and novel intrusion tolerance capabilities,
- design of a distributed real-time control infrastructure for managing and correlating intrusion detection and responses,
- enhancement of exisiting networks and systems QoS support technologies for intrusion mitigation under uncertain and new threats,
- development of novel intrusion tolerance approaches to reduce the impact of the severe cyber attacks by making new network capabilities such as multi-path indirect routing and delivering timely network/system information to end users,
- development of evaluation tools to allow at least statistical confidence in the experimental results.

There are, of course, many other research components that will also improve the trustiness of cyber infrastructures, but we envision that the five items above need to be a part of any serious solution to the growing cyber security problems. They are the focus of this proposal.

As we rely more on IDSs, they also give us more false alarms. This is due to the lack of adaptivity and dynamic reconfiguration capability under new cyber attacks and uncertain threats. Some cyber attacks are initially unobvious and disruptive. And, it is often too late when they are diagnosed as malicious attacks. Some *malware* (malicious programs and code propagating on the Internet) [16, 31] can spread at exponential rates. They can quickly propagate through the network, infecting many machines before the severity of the situation is recognized. Most of today's DDoS attacks aim to completely disable the victim system's service to its clients by consuming its available resources. Compared to the disruptive DDoS attacks, degrading DDoS attacks are emerging. The goal is to increasingly or periodically consume portions of a victim system's resources so as to result in denial of service to legitimate clients during high load periods. Some legitimate clients may also leave the victim system due to the poor QoS experiences. Degrading DDoS attacks can remain undetected for a long time period since they do not lead to total service disruption, and therefore, it is difficult to identify the attackers. Current IDSs lack of dynamics as well. Many existing IDSs are developed domains and/or software environment specific. Today's networks are not only heterogeneous, they are also dynamic. Therefore, IDSs need mechanisms to adaptively change and update their configurations as the security state of the protected systems evolve.

Adaptive IDSs need the support of QoS-aware resource management in network routers and end systems. On one hand, QoS is the target of cyber attacks. Cyber attacks, such as DDoS, aim to reduce QoS level provided by networks and systems and experienced by users; in the worst case, to no service at all. On the other hand, QoS-aware resource management mechanisms can be used as means against cyber attacks. Under uncertain attack scenarios, a router or an end system can handle incoming traffic differently according to the confidence levels about observed traffic behaviors provided by the flexible IDSs. For example, the confidence level can be utilized to limit the propagation rate of a potentially malicious and/or suspicious traffic. Thus, our proposal is to make the performance of networks and systems configurable and controllable by the administrators and users, instead of by parameters and behaviors of uncertain attacks.

We further propose to build a distributed real-time control infrastructure for managing and correlating intrusion detection and responses. Today's IDSs generate large volumes of data from distributed intrusion detection sensors. It often takes a long time to analyze the intrusion data, resulting in slow response time. Efficient information fusion techniques can help correlate distributed intrusion and traffic data and pass along urgent alerts. This enables early warning and intrusion handling. Furthermore, based on the brief network techniques, information fusion component will get intrusion data from IDSs, execute novel alert correlation mechanisms, and provide control parameters to the QoS-adaptive resource management component.

Recent advances in overlay and multihoming networks provides multiple alternate routes that can be used to increase aggregate bandwidth, improve network reliability, and tolerate DDoS attacks. To make these new capabilities available to end users, it is required to enhance the Internet naming architecture and modify the end system's resolver library and routing module. To protect alternate routes, we propose to build a secure collective network defense framework utilizing a set of proxy servers. These proxy servers form the frontline of a wide area demilitarized zone to protect users from further DDoS attacks on these alternate routes. To take advantage of multiple alternate routes at the end systems, we propose to enhance the DNS to include the alternate route information in the DNS entries. To enhance the availability of the DNS system, peer-to-peer secure DNS query will be sent via the indirect routes since the main route could be blocked by DDoS attacks. To avoid stale DNS caching, we will investigate new secure information sharing and notification schemes to provide timely delivery of network status and naming information.

These proposed techniques detect, mitigate, and tolerate cyber attacks and threats. But equally important in improving the performance predictability and trustiness of cyber infrastructures is the design of evaluation tools to allow the computation of statistical confidence intervals. It is not sufficient to know the IDS detected,

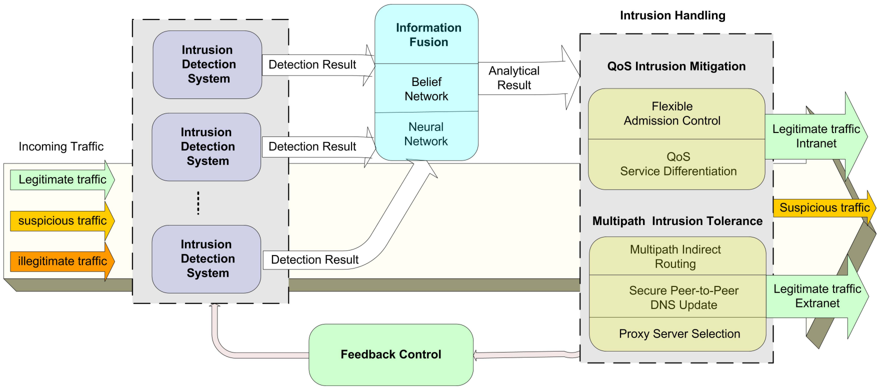


Figure 1: The architecture of the IMPACT high confidence software framework.

say 65% of the attacks in a particular test; we need to know the expected variation in that detection rate over some range of experiments. As we move to adaptive detection and response techniques, we need to develop tools that allow efficient generation of online evaluations as well as offline datasets for further analysis.

1.2 Objectives

The IMPACT project focuses on the research and design of a high confidence software framework that supports the dynamic configuration and deployment of adaptive intrusion detection systems, and support distributed real-time control for managing intrusion detection and response. Fig. 1 illustrates the architecture of the IMPACT software framework. The goal is to improve the measurable performance of network systems under cyber attacks and threats. A prototype system will be developed to demonstrate the effectiveness of the designed technologies. Meanwhile, ... curriculum....

1. Design adaptive IDSs, taking into account QoS control technologies and novel intrusion tolerance capabilities. We will re-design the scan detection algorithm and a behavior-based intrusion detection system to incorporate these changes. To support the tighter interaction such as adaptive monitoring and tracking, we would like to extend the current IDS API to accept requests from QoS-enabled intrusion handling systems. Efficient layer coding of cyber defense data will be investigated. The IDS will be able to dynamically configure itself so that new event streams can be used as input for the security analysis. New signatures can be dynamically included at execution time. Furthermore, a distributed real-time control infrastructure will be designed for managing and correlating intrusion detection and responses. We want to evaluate these new techniques in an integrated enterprise cyber-defense prototype system.

2. Enhance existing QoS-adaptive resource management mechanisms for service differentiation and traffic regulation in both network routers and end-point computer system. The main objective is to make the performance of network systems configurable and controllable by themselves, instead of by parameters and behaviors of cyber attacks, and to provide end users with timely information and more control. We will investigate the impact of the QoS techniques for limiting spreading rate of susceptible traffic and regulating traffic under cyber threats. The capability of reducing false alarm rate will also be evaluated.

3. Apply the user-centered paradigm to improve the cyber infrastructure by making new network ca-

pabilities, i.e., multipath indirect routing and delivering timely network/system information to end users. We want to develop intrusion toleration techniques, based on autonomous establishment of secure multiple indirect routes for legitimate connections, to mitigate the impact of inevitable cyber attacks. DNSs will be enhanced to support multiple indirect routes. New secure information sharing and notification schemes will be developed to provide timely delivery of network status and naming information. We want to explore the use of multiple indirect routes for distributed intrusion detection and network reconfiguration.

4. Develop the IMPACT tool-set, which will be a distributed cyber-evaluation tool-set, to facilitate the parallel dumping, sanitizing and scoring of network traffic and thus support generation of new datasets as well as on-line evaluations. The tool-set will log with added time-stamping and indexing to support enhanced playback capabilities necessary for the statistical confidence testing. The tool chain will support mapping tables to "remap" users, IP addresses and even some content, thus supporting enhanced resampling as well as addressing privacy issues. The result will be both a tool-set and new significant public datasets for evaluations. An important consideration for on-the-fly intrusion detection is to reduce the performance overhead caused by monitoring. We want to make a good tradeoff between accuracy and performance. The developed technologies will be integrated in a prototype system as as to demonstrate the effectiveness in practical situations.

2 Background & Related Work

2.1 Intrusion Detection and Response

Recent intrusion detection research has been heading toward a distributed framework on monitors that do local detection and provide information for global detection of intrusions. These include GrIDS [21], EMERALD [61] and AAFID [71]. They rely on some predefined hierarchical organization and most of them perform centralized intrusion analysis. Gopalakrishna and Spafford [34] present a framework for doing distributed intrusion detection with no centralized analysis component. Ning et al [58] presents a decentralized method for autonomous but cooperative component systems to detect distributed attacks specified by signatures. In Ning's work, the intrusion event sequences are analyzed and matched with a set of attack scenarios. This leads to a more efficient alert aggregation and correlation technique. Besides providing an abstraction for studying the attack strategies, it also allows the network administration to anticipate the subsequent attacks and plan for the defense. However subtle changes in the signatures of the intrusion traffic can lead to partial matches and require further monitoring or intensive analysis possibly with human involvement.

In [79] a system architecture and mechanisms for protecting mobile ad hoc networks is proposed. Experiment results demonstrate that an anomaly detection approach works well on different mobile ad hoc network with route logic compromise and traffic pattern distortion. It will be interesting to see how their framework can be applied in SCOLD systems.

The work in [40] proposed a novel alarm clustering method that removes redundant alarms and supports the human analysis in identifying root causes. Experiments show significant reduction in alert load. Effective generalization hierarchies for IP addresses, ports, and time duration are used in the alarm clustering.

2.2 QoS-adaptive Resource Management

QoS differentiation has been an active research topic in both network core and end-point computer systems for several years. The idea was originated in the network core; DiffServ architecture [14] was proposed by IETF to provide differentiated QoS levels with respect to delay and loss among classes of aggregated traffic flows. To receive different levels of QoS, a packet can be assigned to different service types or traffic classes at the network edges by setting its Differentiated Services code points; a DiffServ-compatible router performs different forwarding operations, so-called "per-hop behaviors" (PHBs), to the classified packet.

Recently, many packet scheduling algorithms have been developed for quantitative QoS differentiation with respect to delay and loss rate. Representatives of algorithms for proportional delay differentiation include BPR [26], JoBS [47], PAD [28], WTP[28], adaptive WTP [46], HPD [28], and LAD [78]. Representatives of algorithms for loss rate differentiation include PLR(∞) [27], PLR(M) [27], JoBS [47], and BRD [38]. They demonstrated various characteristics in support of the proportional differentiation model in different class load conditions and different time-scales. There are also efforts focused on providing QoS differentiation in the end-point computer systems. The efforts include content adaptation techniques for differentiation in multimedia servers [19, 83], priority scheduling with admission control and feedback control for responsiveness differentiation in individual Internet servers and server clusters [1, 23, 45, 80, 81, 82].

QoS has not been used for network and system security purpose until recently. In [22], the authors developed rate-limit algorithms to slow down the propagation of Internet worms. The work is based on the observation that a worm-infected host has a much higher connection-failure rate when it scans the Internet with randomly selected addresses while a normal user deals mostly with valid addresses due to the use of DNS. The work in [85] designed a practical DDoS defense system that can protect the availability of Web services during severe DDoS attacks. The basic idea is to isolate and protect legitimate traffic from a huge volume of DDoS traffic when an attack occurs. The work in [77] proposed a transport-aware IP router architecture that adopts service differentiation technologies to counter DDoS attacks.

In the past years, we have designed novel QoS differentiation techniques in both networks [78, 84] and end systems [80, 81, 82, 83]. We plan to enhance the QoS differentiation techniques and design QoS-aware adaptive IDSs taking into account the capabilities of the novel QoS techniques. We want to study the impact of the techniques in reducing false alarm rate and the vulnerability of the Internet to cyber attacks and improving measurable network systems performance.

2.3 Proxy-based Multiple Path Routing

With the advent of inexpensive and high-bandwidth broadband connection technologies such as ADSL and cable modem for home and business users, multihoming has emerged as a vital choice for large and small businesses to ensure Internet connectivities even during network failures, congestion, or DDoS attacks [37]. Recent studies on overlay networks such as Detour [65] and RON [13] showed that alternate indirect paths can offer much better performance in some cases. Akella et al [4] compared overlay routing and multihoming route control using relay nodes on Akamai content delivery networks and observed that the performance achieved by route control together with multihoming to that of three ISPs (3-multihoming) is within 5-15employed in conjunction 3-multihoming, in terms of both end-to-end RTT and throughput. They showed that while multihoming cannot offer the nearly perfect resilience of overlays, it can eliminate almost all failures experienced by a singly-homed end-network. Stoica et al [72]proposed a general overlay-based Internet Indirection Infrastructure (i3) that offers a rendezvous-based communication abstraction. Instead of explicitly sending a packet to a destination, each packet is associated with an identifier; this identifier is then used by the receiver to obtain delivery of the packet. This level of indirection decouples the act of sending from the act of receiving, and allows i3 to efficiently support a wide variety of fundamental communication services. The Chord peer-to-peer lookup protocol [73] was used in i3 to map the identifier to the real IP address.

Secure Overlay Services (SOS) [42] was one of the first solutions to explore the idea of using overlay networks for pro-actively defending against DoS attacks. SOS protects end-hosts from flooding attacks by (i) installing filters at the ISP providing connectivity to the end-host and (ii) using an overlay network to authenticate the users. Mayday [12] generalizes this SOS architecture and analyzes the implications of choosing different filtering techniques and overlay routing mechanisms. Adkin et al investigate how i3 overlay network can be used to defense against DoS attacks [2].

Recently, TCP Westwood [32] improves TCP performance when packets are sent over multiple paths. TCP-PR [15] investigates the timer-based techniques for dealing persistent reordering of packets arrived over multiple paths. The research results have demonstrated that the multiple paths pose new challenging problems while improving TCP performance. Chen [20] proposed a multipath transport protocol called MPTCP that opens multiple TCP connections over different paths and multiplexes data among the paths.

3 Proposed Work

3.1 Cooperative Intrusion Detection and Response (Cooperative-IDR)

Existing intrusion detection systems are plagued by too many false positives. Techniques are needed to cluster the reports, and remove the redundant alerts generated by the same root cause. Allowing distributed coordination and direct communications among the IDR devices will help track down the intrusion sources, push back intrusion traffic, detect compromised or malfunction nodes, and provide alternate routes for intrusion tolerance. It will also be of interest to investigate how the collection of proxy servers and the availability of the multiple path indirect routes can be used to improve the security of the network system.

Preliminary Results: In [17], we have developed an Autonomous Anti-DDoS system, called A2D2, where an enhanced SNORT IDS with subnet flooding plug-in is integrated with a multiple level adaptive rate limiting firewall. Fig. 2 shows that alerts which are generated by the enhanced SNORT system with subnet flooding detection, automatically trigger the insertion of the firewall rules. Users of A2D2 can specify the multiple level of rate limiting. The system keeps history records, and adaptively blocks potential intrusion, or puts those suspicious traffic in queues with restricted packet rates. Preliminary experiment results shows that A2D2 can tolerate various DDoS attacks. A subset of Intrusion Detection and Isolation Protocol [57] was developed and is used in cooperative intrusion push back experiments.

Fig. 3 shows the histogram of RealPlayer traffic during an ICMP Stacheldraht attack on our A2D2 testbed: a total of 7,127 packets are received by the RealPlayer instead of the 23,000 packets normally transmitted for the entire 10-minute video clip. Only four packets were recovered out of the 2,105 retransmission requests sent. Fig. 4 shows the histogram of RealPlayer traffic when A2D2 multiple level rate limiting defense is turned on. It improves QoS during DDoS attacks. A total of 23,444 packets were received by the A2D2 RealPlayer client, similar to those received by the baseline test scenario. There was no observable service degrades.

Proposed Work: The above preliminary work has demonstrated the feasibility of an automated cyber defense system based on intrusion tolerance and QoS based intrusion mitigation techniques. To take full advantage of these techniques, it requires us to re-examine the IDS and intrusion fusion techniques for

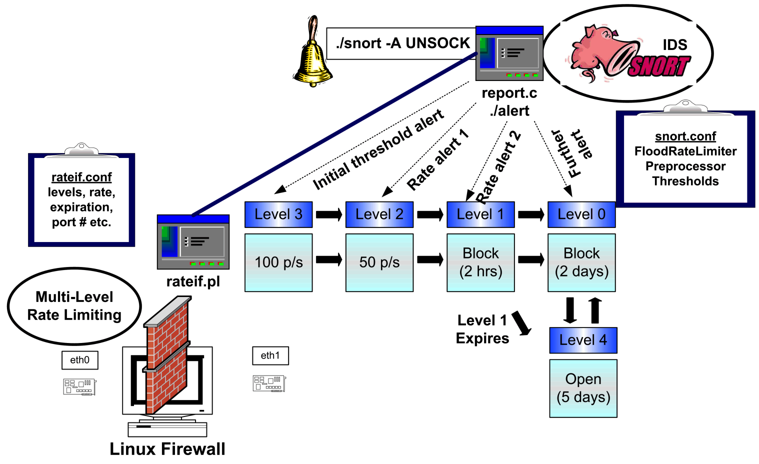


Figure 2: A2D2 Multilevel Rate Limiting.

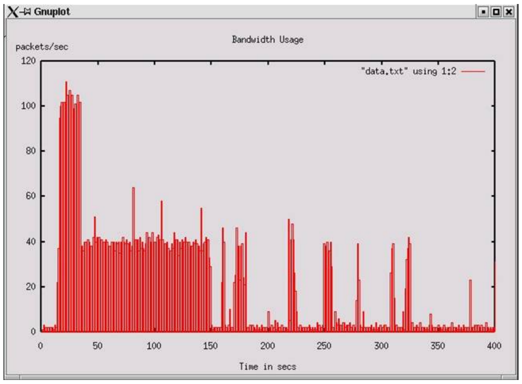


Figure 3: Histogram of a DDoS Attack.

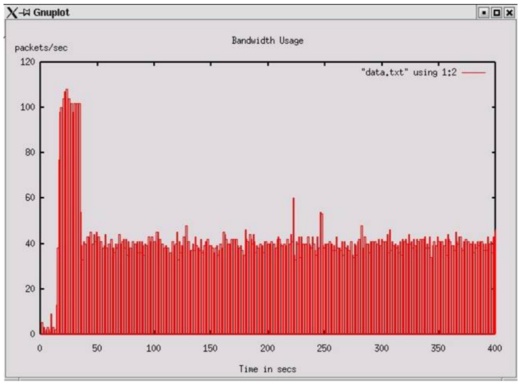


Figure 4: Histogram of an A2D2 Defense.

providing early warnings and to enable the intrusion handling system to take early proper actions. In this project, we plan to conduct the following studies:

1. Re-design the intrusion detection and alert correlation system components by providing early alerts and adaptive tracking feature. We will re-design the scan detection algorithm and behavior based intrusion detection system to incorporate these changes. To support the tighter interaction such as adaptive monitoring and tracking, we would like to extend the current IDS API to accept requests from the intrusion handling system. Efficient layer coding of cyber defense data will be investigated.

2. Develop secure information sharing framework and related API so that all cyber defense system components can communicate using the secure service-oriented architecture (SE-SOA). We will investigate how our existing privilege management infrastructure based on attribute certificate and LDAP systems can be integrated to provide secure access control. We will explore the implementation of secure service-oriented architecture where IDMEF format is used to exchange cyber-defense data. The web service interface will be enhanced with an access control decision engine that queries LDAP systems for proper authorization.

3. Integrate enhanced IDS and adaptive firewall for distributed intrusion detection and handling with SE-SOA. Design efficient techniques for tracing the intrusion routes. Develop specification language for specifying the secure collective defense architecture and the related rules for reconfiguring network, server cluster, and IDS rule updates.

4. Develop an adaptive intrusion handling system that utilizes the QoS-based intrusion mitigation and proxy based multipath intrusion tolerance techniques. Evaluate the effectiveness of these techniques on their effectiveness in blocking DDoS attacks and potential worms from spreading.

3.2 QoS Differentiation and Control for Adaptive IDSs

Today's IDSs often give false alarms due to the lack of flexibility under new cyber attacks and uncertain threats. Some cyber attacks are initially unobvious, while it is often too late when they are known to be malicious attacks. Malware can spread at exponential rates, infecting many machines before the severity of the situation can be recognized by IDS systems. The emerging degrading DDoS attacks aim to increasingly or periodically consume portions of a victim system's resources so as to result in denial of service to legitimate clients during high load periods. Traditional threshold-based firewall techniques are not be able to recognize the attacks. On the other hand, While dealing with false negatives is important to the success of IDSs, false positives often are more harmful as they hamper correct execution of the legal program. Thus, the existing deterministic intrusion detection models are not sufficient. Novel IDSs need to have the flexibility so as to be adaptive under uncertain cyber attacks.

We propose to expand the capability of resource management technologies in network systems so as to enable the flexibility of IDSs. If a network system is able to manage its resources and provide QoS levels differently to various incoming traffic, the front-end IDSs can be flexible in reporting intrusion information. Thus, we propose to add a QoS-enabled intrusion mitigation component in the resource management framework. If the confidence about some traffic is below a certain threshold for raising an alert, an IDS can report the confidence level to the intrusion mitigation component which handles the traffic accordingly. Thus, the QoS-aware resource management has dual effect: it enables IDS systems to be flexible in raising alerts and enables network systems to behave differently to different traffic. There are three key issues. The first one is that if network systems have the capability of QoS-differentiated resource management. The second is how

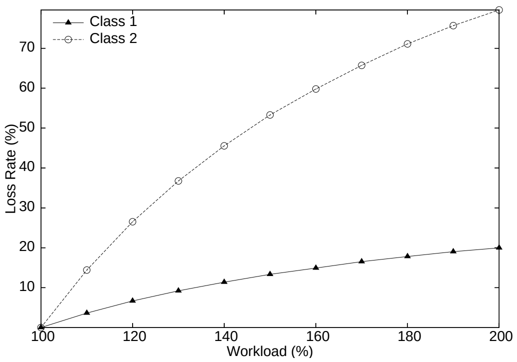


Figure 5: Two-class loss rate differentiation.

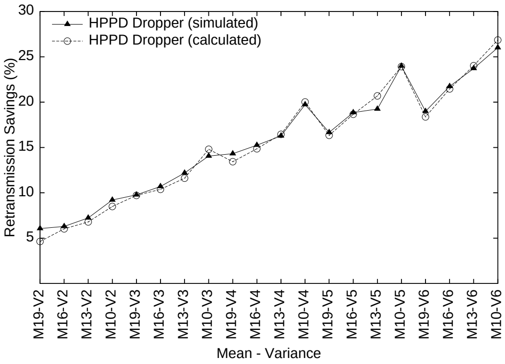


Figure 6: Impact on congestion mitigation.

to execute traffic classification and its correlation to the QoS differentiation capability. The third one is how to evaluate the effectiveness and efficiency of QoS techniques in enabling the adaptivity of IDSs.

Preliminary results in QoS differentiation capability: We propose to enhance existing QoS differentiation and regulation techniques to support the flexible intrusion detection and adaptive intrusion mitigation purposes. We designed resource management technologies to bandwidth differentiation on streaming servers [83], slowdown differentiation on Internet servers [81, 82], and delay differentiation and loss differentiation in networks [78, 84].

In the networks, two key QoS metrics are loss rate (bandwidth) and delay. In [84], we designed a novel hop-count probabilistic packet dropper (HPPD). HPPD aims to meet a two-fold objective by two-dimensional loss rate differentiation: one is inter-class proportional loss rate differentiation; the other is the congestion mitigation that aims to reduce congestion in the first place by dropping intra-class packets differently based on their maturity levels to reduce retransmission cost. None of existing differentiated packet droppers [27, 47, 38] considered an important issue, that is, the retransmission overhead of a dropped packet. A dropped packet will be retransmitted by protocols such as TCP or by end applications. Intuitively, dropping a packet which has travelled 20 hops results in more retransmission overhead and hence heavier congestion in networks than dropping a packet which has only travelled 2 hops. Studies have found that hop count distributions at gateways are usually bell-shaped and the Gaussian distribution is a good first-order approximation [39]. To mitigate the congestion at the first place, HPPD intra-class scheme gives different dropping probabilities according to the number of hops it has travelled so as to reduce the retransmission overhead. The bell-shaped hop count distributions and the TTL information provide the opportunity.

Fig. 5 depicts the experienced loss rate of two classes due to HPPD inter-class dropping scheme under various load conditions. Class 1 is assumed to be the high priority class and class 2 is the low priority class. The pre-specified differentiation weight ratio of two classes was 1:4. The results show that HPPD inter-class scheme can achieve predicted loss rate differentiation in proportion to the pre-specified differentiation weight ratio at different workload conditions. This capability is particularly useful in scenarios with uncertain threats and new attacks. For example, it can be used by an adaptive IDS to deploy rate control to slow down suspicious traffic such as potential Internet worms at the early stage. It makes the speed of suspicious traffic propagation configurable by the parameters of IDSs and hence the adaptivity of IDSs can be achieved.

Fig. 6 shows the impact of the HPPD intra-class scheme on congestion mitigation. A hop count distribution M16-V3 means that the mean and the variance of a hop-count distribution are 16 and 3, respectively. First, it shows that simulation results agree with the expected results under various hop count distributions.

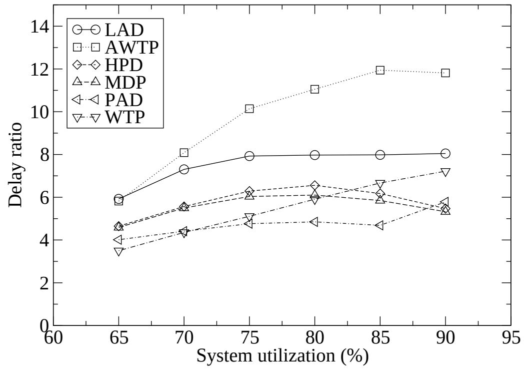


Figure 7: Networks' delay differentiation.

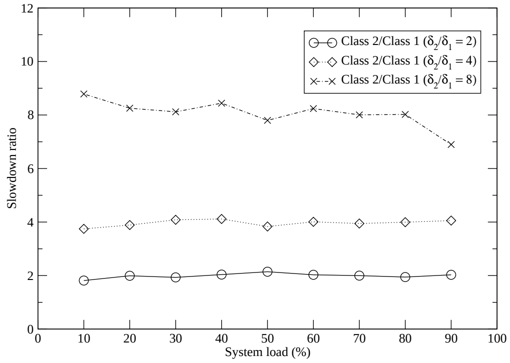


Figure 8: Servers' slowdown differentiation

This demonstrates the effectiveness of HPPD. More important, it is able to reduce the retransmission cost more than 25% compared to PLR droppers [27] and BRD dropper [38]. Note that this saving is achieved in a single hop when it is overloaded. It is indeed a per-hop behavior in the context of DiffServ. But its impact on congestion mitigation will be accumulated polynomially in a route with multiple hops. Results show that HPPD is able to achieve predictable and consistent inter-class differentiation and mitigate congestion by intra-class differentiation at the same time. This novel capability is important to the intrusion mitigation and handling.

Loss rate differentiation aside, we designed novel mechanism for proportional delay differentiation in networks as well [78]. We proposed a new scheduling algorithm, called *Little's average delay* (LAD), based on a *proof* of Little's Law. It monitors the arrival rate and the cumulative delays of the packets from each traffic class, and schedules the packets according to their transient queueing properties so as to achieve the desired class delay ratios in both short and long time-scales. Fig. 7 shows the results of LAD in achieving proportional delay differentiation and compare LAD with other representative algorithms. It shows LAD outperforms its main competitors significantly when the desired delay ratio is large. Simulation results in [78] also show that, in comparison with other scheduling algorithms, LAD can provide no worse level of service quality in long time-scales and more accurate and robust control over the delay ratio in short time-scales. The delay differentiation is important to an intrusion mitigation component because QoS level can be differently handled according to monitored traffic behaviors.

We also conducted research of QoS differentiation in the end-point server systems [83, 82, 80, 81]. For an instance, in [82], we investigated the problem of processing rate allocation for quantitative slowdown differentiation on Internet servers. Slowdown was defined as the ratio of a request' queueing delay to its service time. We first derived a closed form expression of the expected slowdown under workload with a typical heavy-tailed service time distribution (Bounded Pareto distribution). Slowdown differentiation was realized by deploying a task server for handling each request class in a FCFS way. We then developed a strategy of processing rate allocation for the task servers in support of slowdown provisioning. Fig. 8 shows the achieved slowdown ratios of two classes with different differentiation parameter settings. The results shows the effectiveness of the processing rate allocation approach for providing slowdown differentiation on servers. The approach is readily applied to delay differentiation on Internet servers as well. Recently, we implemented a dynamic process allocation approach on an Apache Web server for achieving quantitative service differentiation and the results demonstrate the feasibility and practice of our proposed approaches [80].

With the novel QoS-aware intrusion mitigation and proxy server based intrusion tolerance capabilities, suspicious traffic can be put on special monitoring or classes with lower bandwidth/resource utilization. Further confirmation of the attacks can block those traffic and trigger the dynamic setup of multiple alternate routes for legitimate clients. This implies early reporting of IP sweep and port scaning activities from IDS to the intrusion handling system component, and a much closer interaction among IDS, alert fusion and intrusion handling components.

Research Plans: The preliminary results have demonstrated the feasibility of providing predictable QoS differentiation by adaptive resource management. They advanced our understanding of QoS differentiation techniques to the level where further studies along the line would lead to a breakthrough in the integration of flexible intrusion detection and QoS-adaptive resource management for mitigating the impact of uncertain cyber attacks and threats. We plan to conduct further studies along the line in the following aspects:

1. Develop generalized resource management mechanisms for QoS differentiation and regulation in both network routers and end-point computer system. Current QoS differentiation mechanisms lack of generality, which means their performance depends upon specific assumptions of distributions and characteristic of traffic patterns, i.e., inter-arrivals and job sizes. For example, most differentiated packet forwarding mechanisms assumed Pareto arrival pattern and fixed-size packets on the Internet [28, 38, 46, 47]. This may not reflect the true traffic scenarios on the Internet. A robust cyber-defense mechanism should be of generality.

2. Investigate the impact of service differentiation techniques based on QoS-aware resource management for limiting spreading rate of susceptible traffic and regulating traffic under cyber attacks. The objective is to make the performance of network systems configurable and controllable by themselves, instead of by parameters and behaviors of cyber attacks. The techniques should minimize the performance impact on normal routers and end-point computer systems.

3.3 Improve Service Availability with Novel User-centered Paradigm

Most of the recent overlay and multihoming work, such Internet indirection infrastructure [72] and CoDNS [76], focus on improving network core or ISP routing and naming infrastructure. Many of them still emphasize making the changes transparent to the end users by hiding them at the network edges or gateways. Few emphasize making the new capabilities such as the multi-path and indirect routing available to and controlled by the end users or end systems. Our SCOLD is the first system that delivers the multi-path and indirect routing capabilities all the way to the end users through the secure peer-to-peer DNS update with indirect routing entries and the enhanced resolver library on end users machine. Following the same user-enabling theme, we propose to make network system status information and new network capabilities available to the end users as much as possible, and as fast and secure as we can. This includes the tasks of designing new subscription/notification APIs to receive network connection status and new interface to provide users more control on the resource in their end machines, their fair share of network bandwidth within the organization, and their internet connectivity. Providing timely notification and giving the user more control are essential to gain back the trust in cyber infrastructure.

Preliminary Results: In [24], we designed and implemented a secure collective DDoS defense system (SCOLD) based on indirect routing. The key idea is to follow intrusion tolerance paradigm and provide alternate routes via a set of proxy servers and alternate gateways when the normal route is unavailable or unstable due to network failures, congestion, or DDoS attacks. The BIND9 DNS server and its DNS update utilities are enhanced to support new DNS entries with indirect routing. Protocol software for supporting the establishment of indirect routes based on the new DNS entries is developed for Linux systems.

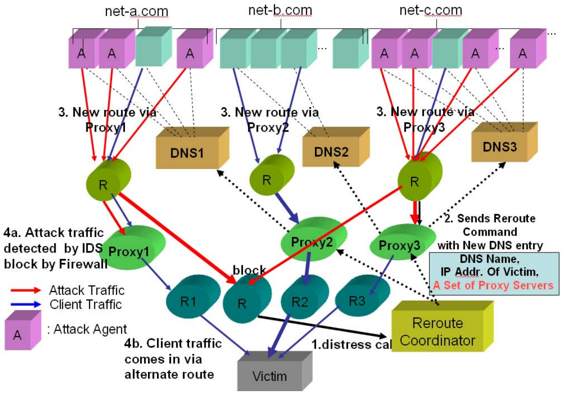


Figure 9: The Scold DDoS defense system.

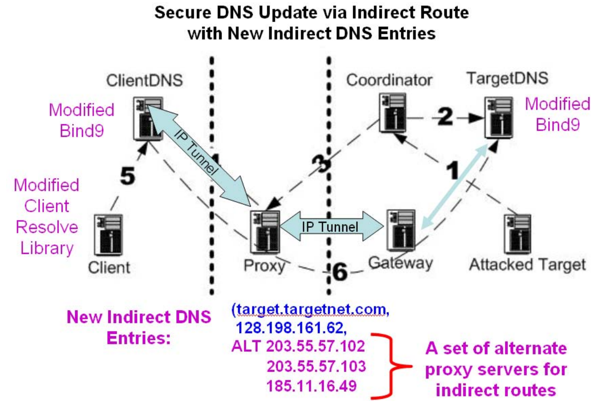


Figure 10: Peer-to-peer secure DNS update.

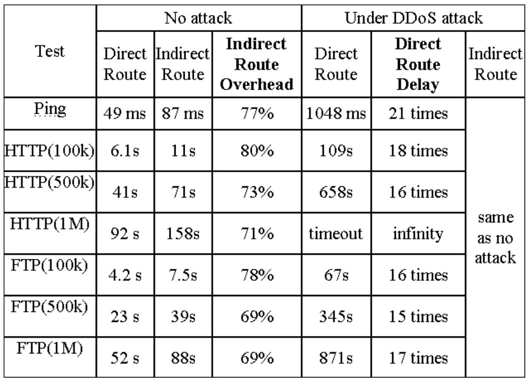
Fig. 9 shows when DDoS attacks were detected by the IDS attached to the main gateway. It sends the distress call to the SCOLD Reroute Coordinator, which computes the proper subset of proxy servers for a client subnet and sends the reroute command with the new DNS entry to update the client DNS server via a selected proxy server. The new DNS entry contains the domain name, IP address of the victim and a set of designated proxy servers for indirect routing. Further attacks on the new routes via those proxy servers will be detected and blocked at the proxy servers farther away from the alternate gateways. The IP addresses of alternate gateways are hidden from the clients. The reroute coordinator informs a proxy server which alternate gateway(s) to use.

Fig. 10 shows that after the client DNS server is updated with the new DNS entry, it can utilize the same indirect route to query the target DNS. This in effect provides a secure peer-to-peer DNS query via indirect route. Since the main gateway is being attacked by DDoS attacks, DNS queries via normal route will not be answered. IP tunnels are established among the client DNS server, the proxy, and the alternate gateway for indirect routing. We modified Bind9 server and DNS update utilities. The client resolver library of Linux system was modified to receive the new DNS entries and to set up the IP tunnel routing entry.

Fig. 11 shows the benefit of SCOLD indirect routing defense against DDoS and its processing overhead, which comes from the IP tunneling overhead and more hops involved in the indirect route. It is observed that the overhead of the indirect route in term of the response time is about 70 percent. Further experiments show the overhead varies from 30 to 200 percent. However, under DDoS attack, the response time with direct route increases dramatically (15 times to infinity), while the response time with indirect route stays the same. Therefore, compared with the serious impact of DDoS attacks on the direct route, indirect routing can improve the network security, availability and performance with acceptable initial setup overhead and processing overhead.

We have modified the networking modules in a 2.4.24 Linux kernel with a thin layer between TCP and IP implementing double buffer to alleviate persistent ordering. It reads the configuration in a *proc* file for spreading the traffic over multiple paths established by the SCOLD system. Fig. 12 shows the aggregate web access bandwidth improves proportionally as the number of proxy servers increases in our testbed. The configuration parameters include the buffer size, the number of multiple paths, and their weights.

Proposed Work: The above preliminary work has demonstrated the feasibility of a secure collective defense system based on peer-to-peer secure DNS update via indirect routes and proxy based multiple path indirect routing. It gives us insight on key issues related the improvement of such secure collective defense system.



Test	No attack			Under DDoS attack		
	Direct Route	Indirect Route	**Indirect Route Overhead**	Direct Route	**Direct Route Delay**	Indirect Route
Ping	49 ms	87 ms	77%	1048 ms	21 times	same as no attack
HTTP(100k)	6.1s	11s	80%	109s	18 times	
HTTP(500k)	41s	71s	73%	658s	16 times	
HTTP(1M)	92 s	158s	71%	timeout	infinity	
FTP(100k)	4.2 s	7.5s	78%	67s	16 times	
FTP(500k)	23 s	39s	69%	345s	15 times	
FTP(1M)	52 s	88s	69%	871s	17 times	

Figure 11: Indirect routing performance result.

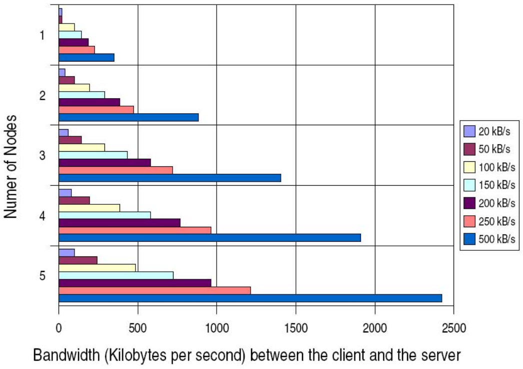


Figure 12: Multi-path routing performance.

In this project, we plan to conduct the following studies:

1. Even though our secure peer-to-peer DNS update can deliver the new routing info to the client subnets, the existing connections will not be aware of the changes. To make the new multipath indirect routing and other network capabilities available to the end users, we will develop new secure information sharing and notification system with new API to facilitate the creation of new network services.

2. Develop new efficient proxy server selection algorithms for selecting an optimal or semi-optimal subset of proxy servers between a victim site and a client site. Even though similar cache server selection algorithms exist for content delivery networks, here the metrics for evaluating the algorithms will include both the geographical diversity for security concerns, the aggregated bandwidth, and QoS of connections.

3. Improve the reliability of the SCOLD protocol and server modules. Port our Linux implementations to work on windows systems to make it widely available to end systems. Propose changes to IETF to include the enhancement on DNS for supporting proxy-based indirect routing and secure indirect DNS update.

4. We propose to develop a new thin layer between transport protocol and IP layers that takes advantage of the available multiple paths. We will provide API to inform the status of these connections and to allow users finer control. We will explore the effectiveness of using intelligent buffering with dynamic feedback and evaluate their performance in the testbed. It is important to investigate how to distribute the data over multiple routes based on desirable requirements such as security, performance, and reliability.

3.4 Prototyping and Evaluation of the Integrated Cyber-defense System

We have built a testbed to simulate an internet-connected enterprise cyber-defense system. We simulated DDoS attack traffic by having several computers, each labeled as an attacker or an outside client or server connected to an Ethernet switch. The switch is also connected to the entry point of the enterprise network. This in effect simulates traffic coming into the network via the internet. Incoming traffic is observed by an IDS. Alerts raised by this IDS and potentially several other IDS's in the network are fused. The fusion component, denoted by the arrow with a head at both ends, fuses alert information and makes dynamic recommendations to the QoS-enabled router to classify traffic into different classes and then treat those classes differently as quantitatively specified.

Incoming traffic can only access the enterprise network through the Demilitarized Zone (DMZ). It offers a level of isolation for enterprise servers like Email, Web, DNS, and FTP servers that need to be accessed by the outside world. The servers are connected by a hub so each sees all incoming requests and responds appropriately. The DMZ external firewall provides proxy and network address translation (NAT) or masquerading functionality which makes the servers more reliable under cyber attacks and threats.

a figure is need here; how about using the testbed figure in our CIT proposal?

The DMZ internal firewall is used to restrict incoming traffic to established traffic only and restrict outgoing traffic to particular ports that users are allowed to access. There can be several different subnets in an enterprise network (for example, for different departments, production, development, integration) although only two subnets are shown in the diagram. The subnets consist of internal computers connected to a switch and connected to the DMZ internal interface by QoS-enabled routers. The cyber-defense components consisting of internal IDS and fusion components working in conjunction with the QoS-enabled routers are also available in the internal subnets to provide an additional level of defense and control.

Proposed Work: In this project, we plan to conduct the following evaluation studies:

1. We want to address issues in evaluation of the integrated cyber-defense system with particular emphasis on predictability issues....to be continued

2. The interdisciplinary aspect of the project will use ideas from biometric system evaluation and stratified sampling design to produce evaluation methodologies that include confidence intervals and predictive measures. It will also produce a tool-set to help automate evaluations and produce datasets for offline evaluations of intrusion and anomaly detection. ......to be continued

4 Broader Impact of the Project – Education component

4.1 Impact of the project on cyber-security curriculum development

In addition to the technical contributions, this proposal will have more significant broader impact. The first is a mixture of education and societal. The first impact will be on the university itself, where it will be engaging both graduate and undergraduate students. In its 2004 college rankings edition, “America’s Best Colleges,” US News’s editors ranked CU-Colorado Springs 5th among public master’s universities in the West. While the school’s history is one of undergraduate and MS level education with pockets of research, it is on the road to becoming a regional research university. It has had doctoral programs in Engineering for over a decade, but only small amounts of funded research – limiting the growth of the doctoral program. The proposal will help fund new doctoral students and aid in the transformation of UCCS to a regional research university. UCCS has a non-traditional undergraduate population with a mostly commuting student body, a median undergraduate age approaching 30. A majority of the UCCS students are self-supporting, and opportunities to work on campus will improve their chances of success and potential to have research or advanced development careers. This funding will provide unique opportunities to these students.

4.2 Impact of the project on local industry and workforce training

As part of our program's outreach to the community, we have arranged to develop a local cable-television show focused on cyber security issues within our community. The show, minimally 30 min per month and possibly more depending on costs/sponsorship and viewer feedback, will seek to educate, and actively involve the local IT workforce in cyber security issues. The Colorado Springs area has almost 200,000 white-collar and military employees. The surrounding areas, some of which are served by that same cable company and would receive the broadcasts, nearly doubles that level. The area is home to multiple military groups including US Northern Command (in charge of US Military Homeland Defense), Cheyenne Mounting Complex (US Strategic Command), Fort Carson, Peterson AFB, Shriver AFB, and the Air Force Academy. There are significant installations of major corporations including Intel, Amtel, LockHeed-Martin, Raytheon, ITT, HP/Compaq, Boeing, MCIworldcom, Quantum, Oracle, Federal Express Data Systems, Adelphia Cable, Allied Signal, Qwest Communications, Comp.Sci.Corp., TRW, DRS, and Gateway 2000, as well as three major hospitals and a significant school system. By making it local and related to things they know, we expect this TV show to help to keep this high-tech workforce more up to date and significantly improve our local impact. This effort will be pursued in conjunction with our Networking Information and Space Security Center in Colorado Springs, which already has significant ties with Northern Command and the local military that, given their missions, are very interested in cyber security issues. In conjunction with NISSC, the UCCS CS Department provides a certificate program in Information Assurance, some of the courses might be used to add more detailed technical content to the broadcasts, if there is sufficient demand for the increased frequency and increased depth. ...support from TechWise Inc....

5 Research Schedule and Deliverables

The research team will include two PIs, two graduate research assistants, and two undergraduate research assistants. Dr. Chow has extensive experience in network and protocol design, network restoration, content switching, and network security. Dr. Zhou's expertise is in QoS-adaptive resource management on distributed networks and systems. We are teaming up to investigate cost-effective solutions for establishing trustworthy network system performance.

One GRA will be working on the QoS-aware adaptive resource management and proxy-based multiple indirect routing techniques. The other GRA will improve intrusion detection, alert fusion, and intrusion handling systems that utilize the new QoS-aware intrusion mitigation techniques, and evaluate the performance of the integrated cyber-defense system. Two undergraduate students will work part-time and participate in the research and development effort. In keeping with past experience we also expect 4-6 MS level students to work on the related network and system areas. These unpaid MS students are still expected to produce conference/workshop papers and their travel expenses may come from the grant. The students working on IMPACT are expected to interact closely, and may be contributing to the other aspects of the project, especially the distributed detection components. The proposed research is planned to be carried out on the experimental testbeds at the Networking and Systems Laboratory, with which the PIs are affiliated.

The deliverables include the publications of research results, the software packages developed for enhanced secure DNS update, multiple indirect routing, and cooperative IDR system, a library of the integration of admission control, feedback control, and resource management algorithms, and technical reports after each milestone. The reports will be published in ACM/IEEE sponsored leading technical conferences and journals. Any software package resulted from this project will be released through the project homepage for the public use free of charge.

References

[1] T. F. Abdelzaher, K. G. Shin, and N. Bhatti. Performance guarantees for Web server end-systems: a control-theoretical approach. *IEEE Trans. on Parallel and Distributed Systems*, 13(1):80–96, 2002.

[2] D. Adkins, K. Lakshminarayanan, A. Perrig, and I. Stoica. Toward a more functional and secure network infrastructure. Technical report, Univ. California, Berkeley, UCB Tech. Rep. UCB/CSD-03-1242, http://sahara.cs.berkeley.edu/jun2003-retreat/TR-CSD-03-1242.pdf, Internet Draft, 2003.

[3] S.J. Aguirre and W.H.Hill. Intrusion detection fly-off: Implications for the united states navy. Technical report, MITRE, 1997.

[4] A. Akella, P. Pang, B. Maggs, S. Seshan, and A. Shaikh. A comparison of overlay routing and multihoming route control. In *Proc. of ACM SIGCOMM*, pages 93–106, 2004.

[5] D. Alessandri. Using rule-based activity descriptions to evaluate intrusion detection systems. In H. Debar, L. Me, and S. F. Wu, editors, *Int. Workshop on Recent Advances in Intrusion Detection*, volume 1907 of *Lectures in CS*, pages 183–196. Springer Verlag, 2000.

[6] E. Amoroso and R. Kwapniewski. A selection criteria for intrusion detection systems. In *Proc. 14th AnnualComputer Security Applications Conference*, pages 280 – 288. IEEE, Dec 1998.

[7] G.A. Fink and B.L. Chappell and T.G. Turner and K.F. O'Donoghue. A metrics-based approach to intrusion detection system evaluation for distributed real-time systems. In *Proc. Int. Parallel and Distributed Processing Symposium*, pages 93–100. IEEE, 2002.

[8] D.W. Murray and D.D. Spencer. Statistical process control testing of electronic security equipment. In *IEEE Int. Carnahan Conf on Security Technology*, pages 53–59. IEEE, Oct 1994.

[9] W.H. Allen and G.A. Marin. On the self-similarity of synthetic traffic for the evaluation of intrusion detection systems. In *Proc. Symp. on Applications and the Internet*, pages 242–248. IEEE, Jan 2003.

[10] N. Athanasiades and R. Abler and J. Levine and H. Owen and G. Riley. Intrusion detection testing and benchmarking methodologies. In *First IEEE Int. Workshop on Information Assurance (IWIAS)*, pages 63–72. IEEE, March 2003.

[11] K.M.C. Tan and R.A. Maxion. Determining the operational limits of an anomaly-based intrusion detector. *IEEE Journal on Selected Areas in Communications*, 21(1):96–110, Jan 2003.

[12] D. Andersen. Mayday: Distributed filtering for internet services. In *USENIX Symposium on Internet Technologies and Systems*, pages 20–30, 2003.

[13] D. Andersen, H. Balakrishnan, M. Kaashoek, and R. Morris. Resilient overlay networks. In *Proc. of the 18th Symposium on Operating System Principles*, pages 131–145, 2002.

[14] S. Blake, D. Black, M. Carlson, E. Davies, Wang Z., and W. Weiss. An architecture for differentiated services. *IETF RFC 2475*, 1998.

[15] S. Bohacek, J. Hespanha, J. Lee, C. Lim, and K. Obraczka. Tcp-pr: Tcp for persistent packet reordering. In *Proc. of the IEEE 23rd Int. Conf. on Distributed Computing Systems*, pages 222–231, 2003.

[16] L. Briesemerister, P. Lincoln, and P. Porras. Epidemic profiles and defense of scale-free networks. In *Proc. of ACM WORM*, 2003.

[17] A. Cearns and C. E. Chow. A2d2: Design of an autonomous anti-ddos (a2d2) network. In *Proc. of IASTED Conf. on Applied Informatic*, 2003.

[18] T. Champion and M. Denz. A benchmark evaluation of network intrusion detection systems. In *Proc. of IEEE Conf. on Aerospace Systems*, 2001.

[19] S. Chandra, C. S. Ellis, and A. Vahdat. Application-level differentiated multimedia Web services using quality aware transcoding. *IEEE J. on Selected Areas in Communications*, 18(12):2544–2265, 2000.

[20] J. Chen. New approaches to routing for large scale data networks. Technical report, Ph.D. Dissertation, Rice University, 1999.

[21] S. Chen, S. Cheung, R. Crawford, and M. Dilger. GrIDS-a graph based intrusion detection system for large networks. In *In Proc. of the 19th National Information Systems Security Conference*, 1996.

[22] S. Chen and Y. Tang. Slowing down Internet worms. In *Proc. of IEEE ICDCS*, 2004.

[23] X. Chen and P. Mohapatra. Performance evaluation of service differentiating Internet servers. *IEEE Trans. on Computers*, 51(11):1,368–1,375, 2002.

[24] C. E. Chow, P. J. Fong, and G. Godavari. An exercise in constructing secure mobile Ad Hoc networks. In *Proc. of Int'l Conf. on Advanced Information Networking and Applications*, 2004.

[25] K. Das. The development of stealthy attacks to evaluate intrusion detection systems. Master's thesis, MIT EECS, June 2000.

[26] C. Dovrolis, D. Stiliadis, and P. Ramanathan. Proportional differentiated services: Delay differentiation and packet scheduling. In *Proc. ACM SIGCOMM*, 1999.

[27] C. Dovrolis and P. Ramanathann. Proportional differentiated services, part ii: Loss rate differentiation and packet dropping. In *Proc. of the Int'l Workshop on Quality of Service (IWQoS)*, 2000.

[28] C. Dovrolis, D. Stiliadis, and P. Ramanathan. Proportional differentiated services: Delay differentiation and packet scheduling. *IEEE/ACM Trans. on Networking*, 10(1):12–26, 2002.

[29] National Laboratory for Applied Network Research. Nlar network traffic packet header traces, 2002. http://pma.nlanr.net/Traces/.

[30] J.E. Gaffney and J.W. Ulvila. Evaluation of intrusion detectors: A decision theory approach. In *IEEE Symp. on Security and Privacy*, Oakland, CA, May 2001. IEEE.

[31] M. Garetto, W. Gong, and D. Towsley. Modeling malware spreading dynamics. In *Proc. of IEEE INFOCOM*, 2003.

[32] M. Gerla, S. S. Lee, and G. Pau. Tcp westwood simulation studies in multiple-path cases. In *Proc. International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, 2002.

[33] G. Givens, J.R. Beveridge, B.A. Draper, and D. Bolme. A statistical assessment of subject factors in the pca recognition of human faces. In *"IEEE Workshop on Statistical Analysis in Computer Vision*. IEEE, June 2003.

[34] R. Gopalakrishna and E. Spafford. A framework for distributed intrusion detection using interest-driven cooperating agents. In *Fourth International Symposium on Recent Advances in Intrusion Detection (RAID)1*, 2004.

[35] E.L. Grant and R.S Leavenworth. *Statistical Quality Control*. McGraw-Hill, 1972.

[36] P.J. Grother, R.J. Micheals, and P. J. Phillips. Face recognition vendor test 2002 performance metrics. In *Proceedings 4th International Conference on Audio Visual Based Person Authentication*, June 2003.

[37] F. Guo, J. Chen, W. Li, and T. Chiueh. Experiences in building a multihoming load balancing system. In *Proc. of INFOCOM 2004*, pages 1241 – 1251, 2004.

[38] Y. Huang and R. Gu. A simple fifo-based scheme for differentiated loss guarantees. In *Proc. IWQoS*, 2004.

[39] C. Jin, H. Wang, and K. Shin. Hop-count filtering: an effective defense against spoofed DDoS traffic. In *Proc. of ACM on Computer and Communications Security (CCS)*, 2003.

[40] Klaus Julisch. Clustering intrusion detection alarms to support root cause analysis. *ACM Trans. on Information and System Security*, 6(4):443–471, 2003.

[41] K. Kendall. A database of computer attacks for the evaluation of intrusion detection systems. Master's thesis, MIT EECS, 1999.

[42] A. D. Keromytis, V. Misra, and D. Rubenstein. Sos: Secure overlay services. In *Proc. of ACM SIGCOMM*, pages 20–30, 2002.

[43] J. Korba. Windows nt attacks for the evaluation of intrusion detection systems. Master's thesis, MIT EECS, June 2000.

[44] D. Krewski and J. N. K. Rao. Inference from statified samples: Properties of the linearization, jackknife and balanced repeated replication methods. *The Annals of Statistics*, 9(5):1010–1019, 1981.

[45] S. C. M. Lee, J. C. S. Lui, and D. K. Y. Yau. A proportional-delay diffserv-enabled Web server: admission control and dynamic adaptation. *IEEE Trans. on Parallel and Distributed Systems*, 15(5):385–400, 2004.

[46] M. K. H. Leung, J. C. S. Lui, and D. K. Y. Yau. Adaptive proportional delay differentiated services: Characterization and performance evaluation. *IEEE/ACM Trans. on Networking*, 9(6):908–817, 2001.

[47] J. Liebeherr and N. Christin. JoBS: Joint buffer management and scheduling for differentiated services. In *Proc. of the Int'l Workshop on Quality of Service (IWQoS)*, pages 404–418, June 2001.

[48] R. Lippmann, J. Haines, D. Fried, J. Korba, and K. Das. The 1999 darpa off-line intrusion detection evaluation. *Computer Networks*, 34:579–595, 2000.

[49] M.V. Mahoney and P.K. Chan. An analysis of the 1999 darpa/lincond laboratory evaluation data for network anomaly detection. In *Proc. Recent Advances in Intrusion Detection*, volume 2820 of *Lectures in CS*, pages 220–237. Springer Verlag, November 2003.

[50] R.A. Maxion and K.M.C. Tan. Benchmarking anomaly-based detection systems. In *IEEE Proc Int. Conf on Dependable Systems and Networks*, pages 623–630, 2000.

[51] J. McHugh. Testing intrusion detection systems: A critique of the 1998 and 1999 darpa off-line intrusion detection system evaluation as performed by lincoln laboratory. *ACM Transactions on Information and System Security*, 3(4), November 2000.

[52] R. J. Micheals and T. E. Boult. Efficient evaluation of classification and recognition systems. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2001)*, Hawaii, December 11–13 2001.

[53] R. J. Micheals and T. E. Boult. A stratified methodology for classifier and recognizer evaluation. In *IEEE Workshop on Emperical Evaluation Methods in Computer Vision*, Kauai, Hawaii, Dec 2001.

[54] R. J. Micheals, P. Grother, and P.J. Phillips. The nist human id evaluation framework. In *Proc. of the 4th Int. Conference on Audio and Video-based Biometric Person Authentication*, June 2003.

[55] R.J. Micheals. *Biometric systems evaluation*. PhD thesis, Lehigh University, 2003.

[56] P. Mueller and G. Shipley. Dragon claws its way to the top. *Network Computing*, August 2001. http://www.networkcomputing.com/1217/1217f2.html.

[57] Boeing Phantom Works. Network Associates Labs. Intrusion detection and isolation protocol, IDIP. Technical report, 2002.

[58] P. Ning, S. Jajodia, and S. Wang. Abstraction-based intrusion detection in distributed environments. *ACM Trans. on Information and System Security (TISSEC)*, 4:407–452, 2001.

[59] P.J. Phillips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and M. Bone. Face recognition vendor test 2002. evaluation report. Technical Report IR 6965, National Institute of Standards and Technology, March 2003. www.itl.nist.gov/iad/894.03/face/face.html.

[60] P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss. The FERET evaluation methodology for face-recognition algorithms. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 22(10):1090–1104, October 2000.

[61] P. A. Porras and P. G. Neumann. Emerald: event monitoring enabling responses to anomalous live disturbances. In *In 1997 National Information Systems Security Conference*, 1997.

[62] N. Puketza, M. Chung, R. A. Olsson, and B. Mukherjee. A software platform for testing intrusion detection systems. *IEEE Software*, pages 43–51, September/October 1997.

[63] M. Roesch. Snort - lightweight intrusion detection for networks. In *USENIX 13th Systems Administration Conference - LISA '99*, Seattle, Washington, 1999. usenix. see also www.snort.org.

[64] L.M. Rossey, R.K. Cunningham, D.J. Fried, J.C. Rabek, R.P. Lippmann, J.W. Haines, and M.A. Zissman. Lariat: Lincoln adaptable real-time information assurance testbed. In *IEEE Proc. Aerospace Conference*, volume 6, pages 2671–2682, March 2002.

[65] S. Savage, A. Collins, E. Hoffman, J. Snell, and T. Anderson. The end-to-end effects of internet path selection. In *Proc. of ACM SIGCOMM*, pages 289–299, 1999.

[66] J. Shao and C. F. J. Wu. Asymptotic properties of the balanced repeated replication method for sample quantiles. *Annals of Statistics*, 20(3):1571–1593, September 1992.

[67] G. Shipley. Intrusion detection, take two. *Network Computing*, November 1999. http://www.networkcomputing.com/1023/1023f1.html.

[68] G. Shipley. Iss realsecure pushes past newer ids players. *Network Computing*, May 1999. http://www.networkcomputing.com/1010/1010r1.html.

[69] R. R. Sitter. Balanced repeated replications based on orthogonal multi-arrays. *Biometrika*, 80(1):211–221, March 1993.

[70] D. Song, G. Shaffer, and M. Undy. Nidsbench - a network intrusion detection test suite. In *Recent Advances in Intrusion Detection, Second International Workshop*, West Lafayette, 1999. http://www.raid-symposium.org/raid99/PAPERS/Song.pdf.

[71] E. H. Spafford and D. Zamboni. Intrusion detection using autonomous agents. *Computer Networks*, 34(4):547–570, 2000.

[72] I. Stoica, D. Adkins, S. Zhuang, S. Shenker, and S. Surana. Internet indirection infrastructure. *IEEE/ACM Trans. on Networking*, 12(2):205–218, 2004.

[73] I. Stoica, R. Morris, D. Karger, M.F. Kaashoek, and H. Balakrishnan. Chord: A scalable peer-to-peer lookup service for internet applications. In *Proc. of ACM SIGCOMM*, pages 149–160, 2001.

[74] S. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. Chan. Cost-based modeling for fraud and intrusion detection: Results from the jam project. In *n Proceedings of the 2000 DARPA Information Survivability Conference and Exposition (DISCEX '00)*, 2000.

[75] T. Toth and C. Kruegel. Evaluating the impact of automated intrusion response mechanisms. In *18th Computer Security Applications Conference*, pages 301–310. IEEE, December 2002.

[76] R. "Venugopalan and E". Sirer. "the design and implementation of a next generation name service for the internet". In *"Proc. of the ACM SIGCOMM04"*, 2004.

[77] H. Wang, K.-G. Shin. Transport-aware IP routers: a built-in protection mechanism to counter DDoS attack. *IEEE Trans. on Parallel and Distributed Systems*, 14(9):873–884, 2003.

[78] J. Wei, C.-Z. Xu, and X. Zhou. A robust packet scheduling algorithm for proportional delay differentiation services. In *Proc. of IEEE Globecom*, 2004.

[79] Y. Zhang, W. Lee, and Y. Huang. Intrusion detection techniques for mo-bile wireless networks. *Wireless Network*, 9:545–556, 2003.

[80] X. Zhou, Y. Cai, G. K. Godavari, and C. E. Chow. An adaptive process allocation strategy for proportional responsiveness differentiation on Web servers. In *Proc. IEEE 2nd Int'l Conf. on Web Services (ICWS)*, July 2004.

[81] X. Zhou, J. Wei, and C.-Z. Xu. Resource allocation for session-based rwo-dimensional service differentiation on e-Commerce servers. *IEEE Trans. on Parallel and Distributed Systems*, in press, to appear in 2006.

[82] X. Zhou, J. Wei, and C.-Z. Xu. Processing rate allocation for proportional slowdown differentiation on Internet servers. In *Proc. IEEE 18th Int'l Parallel and Distributed Processing Symp. (IPDPS)*, pages 88–97, April 2004.

[83] X. Zhou and C.-Z. Xu. Harmonic proportional bandwidth allocation and scheduling for service differentiation on streaming servers. *IEEE Trans. on Parallel and Distributed Systems*, 15(9):835–848, 2004.

[84] X. Zhou, D. Ippoliti, and T. Boult. HPPD: a hop-count probabilistic packet dropper. In*Proc. IEEE Int'l Conf. on Communications (ICC)*, 2006.

[85] J. Xu and W. Lee Sustaining availability of Web services under distributed denial of service attacks. *IEEE Trans. on Computers*, 52(2):195–208, 2003.