

# > Securing\_the\_Net

## > by\_Manny\_Romero

>

Information Superhighway. World Wide Web. Internet.

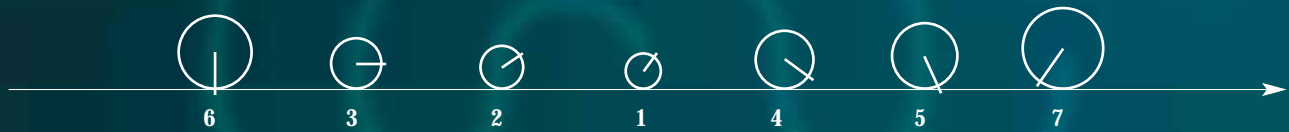
Lots of names for the same creation. Regardless of what you call it, the worldwide network of computers is changing the way people communicate and do business in many ways.

>>The Internet is far reaching and fast; what the Internet is not is totally safe and secure. Nong Ye and her colleagues are working on those concerns. Ye is a professor of industrial engineering at Arizona State University. She also directs the Information & Systems Assurance Laboratory (ISAL). The group is working to make the Internet a better, safer, and more efficient tool for work, school, and communication.

>>“When used for communication and information sharing, the Internet is considered an ‘information infrastructure,’” says Toni Farley, assistant director of the ISAL. “This infrastructure aims to provide a secure, high-quality service to its users.”

That’s not always reality. As the Internet community grows, so does the need for more stringent security and quality of service (QoS) measures. Farley says that the Internet in use today provides minimal security and virtually no QoS.

ASU COMPUTER SCIENTISTS HAVE DEVELOPED A METHOD OF DETECTING ATTACKS ON COMPUTERS AND NETWORKS. THEY USE A STATISTICAL MEASURE CALLED CHI SQUARE, REPRESENTED BY X (THE GREEK LETTER CHI). AT TOP LEFT IS A REPRESENTATIVE GRAPH OF SYSTEM ACTIVITY. UNUSUAL DEVIATIONS FROM NORMAL OPERATION SHOW AS SPIKES IN THE VALUE OF CHI SQUARE.



**Educators, corporate executives, and everyday computer users**

probably agree that the Internet has made it easier and faster to complete projects. However, as technology evolves, so does the demand from a fickle consuming public. We want better, faster, smaller products.

ASU researchers are helping with the "better" and "faster" parts. They've developed a technique that helps reduce the inconsistency of waiting time that Internet users experience when working online.

As is the case with many other inventions, there is always room for improvement, says Nong Ye, director of ASU's Information & Systems Assurance Laboratory (ISAL). Ye and ASU colleagues Xueping Li and Toni Farley created what they call the Yelf Spiral. Named for its three researcher/inventors (Ye, Li and Farley), the Yelf Spiral is a technique for determining the order of jobs to be serviced on-line. It works to reduce the inconsistency of waiting time.



Nong Ye

Ye says that the technique involves scheduling jobs in a spiral fashion based on their processing times.

"This technique has commercial applications in any situation where jobs require scheduling, and where reducing the variance in job waiting time would prove beneficial," Ye explains. "Such applications exist in almost all fields, including computers, cabled or wireless computer networks, Internet, electric power networks, transportation networks, and others."

Think about the process of scheduling requests (jobs) in a Web server, she adds. By reducing the variance of Web request waiting times, user expectations can more easily be established and met.

Many situations already exist where a set of jobs must be scheduled to run on one resource. For example, a Web server often needs to schedule multiple requests for processing. Minimizing the variance in wait time before jobs are serviced may provide stability and predictability to a system. Farley says that the Yelf Spiral can

improve the quality of service provided to Internet users.

"People don't like uncertainty in waiting," she says. "Our technique allows people an option. They can decide how long they want to wait, or if they want to wait at all. It allows them to use their time more efficiently. It also gives them a better sense of assurance with regard to their job completion."

"By minimizing waiting time variance, we can set tighter bounds (predictability) on waiting time for providing Quality of Service (QoS) to the user," Ye adds. "The Yelf Spiral is a job ordering method."

How does it work? Consider a set of jobs with processing times 1, 2, 3, 4, 5, 6, and 7. The smallest job has the shortest processing time. The largest job has the longest processing time. The Yelf Spiral orders the jobs to reduce waiting time. The process is as follows:

- >> FIND SMALLEST JOB AND PLACE IN MIDDLE OF SEQUENCE LIST.
- >> FIND LARGEST JOB AND PLACE AT END OF LIST.
- >> FIND SECOND LARGEST JOB AND PLACE AT BEGINNING OF LIST.
- >> FIND THIRD LARGEST JOB AND PLACE BEFORE LARGEST JOB.
- >> FIND FOURTH LARGEST JOB AND PLACE BEFORE THIRD LARGEST JOB.
- >> FIND NEXT LARGEST JOB AND PLACE BEFORE OR AFTER SMALLEST JOB, DEPENDING ON WHICH PLACEMENT PRODUCES SMALLER VARIANCE OF WAITING TIMES FOR JOBS IN CURRENT LIST.
- >> REPEAT STEP 6 FOR THE REMAINING JOBS.

Using the example, the jobs will be ordered as follows: 6, 3, 2, 1, 4, 5, 7.

The technique can be thought of as a spiral due to the nature of the ordering method. The point of the spiral begins from the outer edge of the list at the end and proceeds to the inside of the list.

"We've performed extensive testing of the Yelf Spiral method in comparison with many existing, popular scheduling methods," Ye says. "The Yelf Spiral has always produced the minimum variance of job waiting times. It's really something that all Internet users could benefit from using." Manny Romero



Toni Farley

<<Our work involves mathematics, computer science, engineering, and language skills, >>  
says ASU scientist Nong Ye. <<All of these factors play a role  
in security and information assurance for the Internet.>>

**The ASU researchers say** that many of the Internet's security-related problems are due to the way in which users detect "viruses" or "intrusions" on a network. "Most current techniques require that a virus or intrusion be known before it can be detected," Ye says. "These techniques are clearly ineffective in detecting new threats."

Existing detection techniques include both signature and anomaly detection. Signature recognition is used in most commercial tools, such as anti-virus software. It is not designed to detect new intrusions. Anomaly detection can detect both known and new intrusions. Ye and her team have had success with a new anomaly detection technique they are developing. She says that many of the Internet's security-related problems require early and quick detection.

"This technique detects intrusions by using a Chi square distance monitoring procedure to monitor event frequency distribution," Ye says. "The benefits of this procedure, in comparison with existing anomaly detection techniques, are its accuracy and its ability to work for very large computer networks."

What is Chi square? Ye's distance monitoring procedure is a method of detecting attack activities on computers and networks. She says that an attacker (hacker) often carries out different activities from normal user activities in order to accomplish an attacking goal. Chi square is essential for tracking down hacker activities.

"The Chi square procedure captures the trend and pattern of normal user activities on computers and networks," Ye explains. "It does this by extracting statistical properties of normal user activities from historic data of normal computer and network usage. It then defines a statistical profile of normal user activities," she says.

"The statistical profile of normal user activities is then used to detect attack activities." The researchers use mathematics to determine the difference between observed activities on computers and networks and the statistical profile of normal user activities.

Ye says that a large value of Chi square distance indicates a huge difference between observed activities and the statistical profile of normal user activities. The number triggers a signal of a possible attack. "This signal alerts system administrators to take actions for stopping the attack, examining damage, and getting computers and networks back to a normal state," she says.

The ASU researchers work closely with scientists at the Air Force Research Laboratory's Defensive Information Warfare Branch. Ye says the working relationship gives her team an opportunity to gain a better understanding of communication and the importance of security.

Work at the ISAL is also supported by the Symantec Corporation, a world leader in Internet security. Ye is an active promoter of collaboration between academia and industry. She says the partnership allows her team to work on laboratory solutions to real-world problems from industry.

"Our work involves mathematics, computer science, engineering, and language skills," Ye says. "All of these factors play a role in security and information assurance for the Internet."

The quality of service (QoS) research conducted by Ye's team also benefits the everyday Internet user. "It is important to figure out how long it takes to get a message to someone. It is also important to make sure that the message is received in a timely manner that allows the other party to respond in a timely manner," she explains. "The Internet's QoS problems are in large part related to the way in which communications (in the form of data packets) are routed through a network as well as the way in which computer and network resources are managed."

QoS can be achieved at many levels in a network. As a result, scientists use several research models. The local model is focused on small networks. A regional model looks at larger networks. Studying the Internet requires a global model. Ye says that none of these modes provide adequate QoS.

The ASU team has had two breakthroughs in this area, techniques they call the Yelf Spiral and Batch Scheduled Admission Control (BSAC).

Ye describes the Yelf Spiral as a task scheduling technique. It provides consistent timeliness of service, performance stability, and predictability for guarantee of quality of service. Obtaining a level of consistency is the first step in predicting the time it takes to complete a task.

"This technique can be applied to any situation where jobs require scheduling and reducing the variance in the job waiting times would prove beneficial," Ye explains.

The BSAC technique batches tasks in a network at scheduled times. Ye says that this can stabilize timeliness performance and provide predictability to the network. ASU had filed patent disclosures for these two ground-breaking techniques. Ye says the ideas are powerful yet simple, and can be applied to services currently being used every day.

"What we are looking at is similar to what a telephone company or cable company may already have in place," Farley explains. "When a customer is placed on hold, many times a recording will say, 'The next available customer service representative will be with you in five minutes.' This time assurance provides users with a choice. They can hang up and try again later or they can wait to communicate."

Such time assurance would provide Internet users the same choice. They can try later if they don't want to wait.

Farley provides a scenario. "Say that you are working on line and you request a Web page. A notice pops up telling you that the page will take five to seven minutes to download," she says. "You now have a choice. You can wait or you can move on to another Web page that may give a faster response."

"Most current work is focused on minimizing the time it takes to complete a task," Ye says. The ASU researchers think that the race to be the fastest has left other quality considerations in the shadows.

RESEARCH AT THE INFORMATION & SYSTEMS ASSURANCE LABORATORY IS SUPPORTED BY THE DEPARTMENT OF DEFENSE, AIR FORCE OFFICE OF SCIENTIFIC RESEARCH, AIR FORCE RESEARCH LABORATORY, AND THE DEFENSE ADVANCED RESEARCH PROJECTS AGENCY. FOR MORE INFORMATION ABOUT INDIVIDUAL PROJECTS, VISIT THE ISAL WEB SITE AT [HTTP://ISA.EAS.ASU.EDU](http://isa.eas.asu.edu)