New Chinese Supercomputer Is the World’s Most Powerful

A new Chinese supercomputer has debuted atop the recently released list of the world’s most powerful computing systems.

The Tianhe-2 again gives China the lead over the US in the two countries’ ongoing supercomputer competition.

The system, which the government-run National University of Defense Technology (NUDT) developed, topped the latest biannual Top500 supercomputer list with a tested performance of 33.86 petaflops (one petaflop is 1015 flops).

That’s much faster than the second and formerly top-ranked Top500 system, the US’s Titan. That system, made by Cray and housed at the Department of Energy’s Oak Ridge National Laboratory, performs 17.59 petaflops.

The Tianhe-2 is expected to have a theoretical peak performance of 54.9 petaflops when completed. The NUDT is currently assembling and testing the system, which it plans to deliver to the National Supercomputer Center in Guangzhou by the end of this year.

The supercomputer uses 32,000 Intel Xeon processors boosted by 48,000 Xeon Phi accelerator processors. There are a total of 3.12 million cores linked by the Chinese TH Express-2 interconnect.

Most of the Tianhe-2’s components are Chinese-made, including the NUDT’s Kylin Linux operating system. The supercomputer has 12.4 petabytes of storage and 1 petabyte of memory.

Among the Top500 systems, the US now has 252, China has 66, Japan has 30, the UK has 29, and France has 23.

Hans Meuer of the University of Mannheim, Erich Strohmaier and Horst Simon of the Lawrence Berkeley National Laboratory, and Jack Dongarra of the University of Tennessee, Knoxville, compile the list.

New Approach Could Enable 5G Wireless Technologies

As an increasing number of devices of many types connect to the Internet wirelessly, the search for faster, higher-capacity mobile technology is growing.

Samsung researchers say they might have found a way to provide such capabilities. They’ve developed a new beam-forming antenna that could send and receive at least 1 gigabit of data per second, more than current 4G technologies offer, over distances up to 2 kilometers.

Samsung’s technology would operate at or near millimeter-wave frequencies (3 to 300 GHz), a part of the spectrum seen as promising for faster wireless communications.

Until now, cellular networks have used lower frequencies. However, experts say, networks have squeezed about as much bandwidth as they can from them. In addition, service providers are already using much of this spectrum, leaving little available for new deployments. On the other hand, Samsung said, much more high-frequency spectrum is available.

Although millimeter-wave technology is already utilized for some types of communications, engineers have expressed concern about using it for wider mobile coverage.

For example, millimeter waves don’t readily penetrate solid materials and are easily absorbed in the atmosphere, causing them to lose energy over long distances. Also, millimeter-wave antennas require more power to send and receive data than cellular systems can handle.

To address these issues, Samsung is using an array of 64 antennas, along with signal-processing technology, to concentrate radio energy in a narrow, directional beam, thereby increasing signal power without requiring more transmission power. To communicate, a base station and mobile...
Researchers Find First Mobile-Device Ransomware

Ransomware has long been a problem for PCs. In some cases, hackers use this type of malware to harass victims or lock up their computers. They then request money to stop the problems.

Security vendor Symantec said this practice has now spread to mobile devices, part of a trend in which hackers are attacking smartphones and tablets with tactics once used only against PCs.

Symantec said the culprit in this case is Android Defender, a Trojan horse that purports to be an antivirus application that will remove malware on victims’ computers.

Users initially find Android Defender on third-party websites disguised as a purportedly useful application. In some cases, for example, it was found listed as an enhanced version of Skype.

Once downloaded, Android Defender appears to scan the victim’s phone. It then reports various viruses that aren’t actually present and urges the user to buy a key for $129—discounted to $89—that will activate malware-removal capabilities.

For those who don’t make the purchase, Android Defender continues displaying reminders and notifications about imaginary infections, and also crashes the Android device.

Meanwhile, Android Defender prevents users from uninstalling it or launching other applications, and also changes OS settings.

All this is designed to encourage victims to pay for the fake antivirus application’s supposed activation key.

In some cases, users might be able to perform a simple uninstall because Android Defender doesn’t always work as designed with certain devices.

Some users, though, might have to return the device to the manufacturer to have the malware removed.

The problems Android Defender causes could grow because although the Trojan horse is buggy now, Symantec noted, its operators appear to be trying to improve it.

Google Will Provide Internet Service to Remote Areas via High-Altitude Balloons

Google has officially kicked off a project that would create a system of high-altitude balloons to provide wireless Internet access. The company says Project Loon would target typically underserved remote, rural, or poor areas, and would also improve communications in the wake of natural disasters that damage terrestrial networks.

The project—which is still in very early development—would place thousands of specially equipped balloons at an altitude of about 20 km (12.5 mi), twice as high as passenger jets fly but lower than satellites orbit. The system would provide wireless access at speeds like that of 3G cellular networks.

Consumers would use a special antenna to connect to the mesh balloon network. The signal would travel from balloon to balloon, then to a ground-based facility connected to an ISP, and finally to the Internet itself.

Internet access would be available to anyone with a receiver who is within range of a balloon. Each balloon would provide service for a 1,250 sq km (482.6 sq mi) area.

Solar panels mounted just below the balloons generate enough electricity in four hours to power the transmitter for a day so that it can beam Internet signals to the ground stations, which are spaced about 100 km (62.5 mi) apart.

When inflated, the helium-filled, polyethylene plastic balloons would be 15 m (49.2 ft) wide and 12 m (39.4 ft) tall. Below each would hang a small box...
containing electronic equipment including circuit boards for control functions, radio antennas, and batteries to store solar energy for use during nighttime operation.

Google could maneuver the balloons as necessary by using data from the US National Oceanic and Atmospheric Administration to adjust their altitude so that they reach winds moving at the speed and in the direction desired.

A parachute would allow controlled descent when balloons are taken out of service or experience a problem.

Google recently launched about 30 balloons above New Zealand’s South Island as part of a Project Loon experiment in which about 50 local users will test network connections. Transmissions will be over unlicensed 2.4- and 5.8-GHz frequencies.

Next, Google plans to release 300 balloons around the world at the 40th parallel south to provide Internet access to Argentina, Australia, Chile, and New Zealand.

Google’s proposed network could make the company a major ISP. In addition, the system would let developing countries provide Internet access without having to build a costly underground fiber infrastructure. They would also help people in remote parts of developed countries who must use expensive satellite-based service to connect to the Internet.

It’s unclear whether latency-sensitive technologies such as Internet telephony would work well with Google’s proposed system, which must relay signals through multiple balloons before even reaching the Internet.

There are also concerns that politics or opposition by various governments could hurt Project Loon.

Robotic Jellyfish Could Become a Military Spy

Academic researchers have developed a robotic jellyfish that could see duty as a spy someday.

The Virginia Tech scientists have built Cyro as part of a $5 million project funded by the US Naval Undersea Warfare Center and the Office of Naval Research. Several other US schools—including Providence College; the University of California, Los Angeles; the University of Texas at Dallas; and Stanford University—are also taking part in the effort, designed to develop autonomous underwater robots for use in tasks such as surveillance and environmental monitoring.

The Virginia Tech researchers say they designed Cyro—which is 1.7 m (5 ft, 7 in) wide and weighs 77.1 kg (170 lbs)—to look and maneuver like an actual jellyfish. It uses electric motors to move eight aluminum arms and a body covered in white silicone.

The researchers program the system via a control box in the middle of the structure. Cyro currently has no camera, but the scientists say one could be easily added, as could many types of monitoring instruments.

The device uses a rechargeable nickel metal hydride battery and can swim for only about four hours at a time. This limits its ability to act autonomously for weeks or months, which is a goal of the US Navy’s robot-development program.

The Virginia Tech team is thus researching alternative energy sources for the robot, such as solar or wave power, or even microbial fuel cells that generate energy by consuming ocean organisms.

Cyro is years from being sent on live missions. Once deployed, it could be used in conducting military operations, studying fish, monitoring ocean currents, or perhaps even cleaning up oil spills or responding to natural disasters.