iIS 資訊科學簡訊 Update

Newsletter of the Institute of Information Science, Academia Sinica, Taiwan

2013

Message from the Director

The Institute of Information Science (IIS) was established in 1982. We currently have 38 full-time research faculty, 30 post-doctoral research fellows, and slightly more than 300 research associates and specialists. Our research is conducted in eight specialized laboratories: Bioinformatics, Computer Systems, Information Processing and Discovery (iPAD), Multimedia Technology, Natural Language and Knowledge Processing, Network Systems and Services, Programming Languages and Formal Methods, and Computation Theory and Algorithms.

IIS is not a degree-granting academic institution, with the important exception of the international graduate program in bioinformatics, under the auspices of Academia Sinica's Taiwan International Graduate Program. This Ph.D. program was established in 2003 and has enrolled more than 39 students over the last eight years.

Many of our research fellows hold joint faculty appointments at top universities in Taiwan. This allows our institution to play a very significant role in training and fostering advanced research talent in the IT industry and in academia in Taiwan.

DIRECTOR:
Dr. Hsu, Wen-Lian

DEPUTY DIRECTORS:
Dr. Ko, Ming-Tat
Dr. Wang, Hsin-Min

GROUP COORDINATORS:
Dr. Sung, Ting-Yi
Bioinformatics Lab
Dr. Wu, Jan-Jan
Computer Systems Lab
Dr. Chen, Meng Chang
Information Processing and Discovery (iPAD)
Dr. Liao, Hong-Yuan Mark
Multimedia Technology Lab
Dr. Hsu, Wen-Lian
Natural Language and Knowledge Processing Lab
Dr. Ho, Jan-Ming
Network Systems and Services Lab
Dr. Wang, Bow-Yaw
Programming Languages and Formal Methods Lab
Dr. Hsu, Tsan-sheng
Computation Theory and Algorithms Lab

In the twenty-nine years since the founding of the Institute of Information Science our faculty members have worked diligently in their areas of expertise. We are proud that their efforts have been recognized both domestically and internationally, including through numerous awards such as IEEE Fellow, the ACM best paper award, the K.T. Li Distinguished Young Scholar Award, the 2009 Outstanding Research Award from the National Science Council, the 2010 Outstanding Young Electrical Engineer Award from the Chinese Institute of Electrical Engineering, the 2010 Pan Wen Yuan Distinguished Research Award, the 2009 Information Science Honorary Medal from the Institute of Information & Computing Machinery, and the 2009 Golden Penguin Award. We hope our efforts can contribute to the development of information science as a whole. I am honored the president of Academia Sinica appointed me to be the director of the Institute of Information Science. I hope to facilitate the institute's development into center of the information science community of Taiwan.

In this series , we will first introduce the technology behind the MIFARE Classic smart card. This card is the basis of Taipei's Easy Card; thus, its security should be closely inspected. Our researchers will approach this from a technical perspective, analyzing the flaws in the Easy Card's design and detailing its operation errors. By doing so, we ultimately hope to spur greater security for this kind of card so that the public may more safely use it as a means of identification and payment.

The article on the Network Systems and Services Laboratory touches briefly on the following topics: improving wireless and delay-tolerant network protocols, leveraging human computation capabilities to help meet key challenges, developing critically needed information and communication technologies for disaster management, and seeking solutions to network computational problems regarding the provision of large-scale services for the management of financial risk.

Also, intelligent robotic systems are finding ever-increasing applications in surgery, military missions, and daily life. Thus, the development of systems that ensure the safety and comfort of human–robot interaction is of paramount importance in robotics research, both now and in the future. Creating robots that work well as helpers of human beings requires not only careful planning and control, but also the balanced integration of a deep understanding of the theory and technology of sensing.

As winter approaches, the campus is sometimes covered with a chilly mist. We hope that you will find some warmth in our fall/winter edition. We welcome your suggestions to make this newsletter better, and we encourage our alumni to contact us and share their good news.

Honors and Awards

Distinguished Research Fellow Dr. **Wen-Lian Hsu** named Director of the Institute of Information Science, effective June 18, 2012.

Dr. **Shin-Cheng Mu** being promoted to Associate Research Fellow, effective September 14th, 2012.

Dr. **Wei-Ho Chung** receiving the 2012 WCNC Best Paper Award from the IEEE Communications Society.

Dr. **Bow-Yaw Wang** being promoted to Research Fellow, effective September 14th, 2012.

Dr. **De-Nian Yang** being promoted to Associate Research Fellow, effective September 14th, 2012.

Distinguished Research Fellow **Hong-Yuan Mark Liao** being elevated to IEEE Fellow

Dr. **Kate, Ching-Ju Lin** receiving the Exploration Research Award 2012 from the Pan Wen-Yuan Foundation.

Ms. **Yan-Ying Chen** co-advised by Dr. Mark Liao of IIS and Prof. Winston Hsu of NTU won the ACM Multimedia 2012 Doctoral Symposium Best Paper Award.

Dr. **Ju-Chiang Wang, Yi-Hsuan Yang, I-Hong Jhuo, Yen-Yu Lin, and Hsin-Min Wang** receiving ACM Multimedia 2012 Grand Challenge First Prize.

Dr. **Lun-Wei Ku** joining us as our new Assistant Research Fellow, August 2012.

Distinguished Lecture Series

October	**Ching Y. Suen**	Director, CENPARMI at Concordia University in Canada Computational Linguistics, Computer Analysis and Recognition of Documents
December	**Erik Demaine**	Professor, Computer Science, Massachusetts Institute of Technology Theory, Algorithms, Geometric Folding
March	**Emmanuel Candes**	The Simons Chair, Mathematics and Statistics, Stanford University Theoretical Computer Science, Mathematical Optimization, Information Theory

Contactless Smartcard Technology Needs More Security

Project Coordinator: Dr. Yang, Bo-Yin

MIFARE Classic is a contactless smartcard technology owned by NXP Semiconductors. More than 1 billion cards and one million readers have been sold. Without a doubt this is the contactless smartcard technology with the highest market share. In fact, MIFARE Classic dominates the smartcard market for public transportation ticketing systems in cities around the world. Taipei's MRT uses Easycards featuring MIFARE Classic as do the ticketing systems for metropolitan mass transportation systems in these countries: Argentina, Brazil, Australia, Canada, China, Denmark, Germany, India, Ireland, Korea, Sweden, Turkey, UK, and the U.S.

MIFARE Classic cards run on miniscule amount of energy that its wire loop collects from a quickly varying electromagnetic field. Aside from a small amount of control circuitry, it is basically a memory stick with flash memory divided into several sectors, each with four blocks. In the standard MIFARE Classic each block is 16 bytes. The MIFARE Classic uses NXP's proprietary CRYPTO1 cryptosystem for access control. Before any sector is read, the card and reader carry out an authentication protocol to assure that they have the same keys.

NXP kept CRYPTO1 under wraps as a trade secret in an effort to keep MIFARE Classic safe, but this is doomed to fail nowadays, due to the free flow of information. Shanghai Fudan Electronics was reportedly able to build clone cards compatible with official MIFARE Classic readers as early as 2004. This can only mean that the secret has already leaked. More rumors circulated in 2006 that academics finally had reverse-engineered CRYPTO1, which at the end of the following year was confirmed at Chaos Communication Congress 2007 by Nohl and Pl¨otz, two engineers hailing from Germany, who publicized their results at USENIX security Symposium 2008. Finally, in 2008 another team from Raboud Universiteit Nijmegen publicized their onset on MIFARE Classic. Actually NXP had sought to prevent this via legal means, but their case was thrown out of court on Freedom of Expression grounds.

MIFARE Classic has been a huge commercial success. It is cheap, convenient and sturdy, enabling it to penetrate many public transportation ticketing systems in less than a decade. However, as a cryptographic project it is sadly deficient, which means that it cannot assure the basic security. We will briefly summarize some of the design errors in its cryptosystems and protocols. MIFARE Classic cards communicate with readers in three different stages: anti-collision, certification, and storage operations (read/write). The anti-collision conforms to the ISO-14443 standard and marks the beginning of a session. A reader can then triggers the certification mechanism which establishes a session key for the encryption of all ensuing communications, including all reads and writes and authentication to other datasectors during this session.

As mentioned above, MIFARE Classic embraces a proprietary cryptosystem called CRYPTO1. This is a stream cipher, enabling you to generate from any key a pseudorandom stream of bits ("keystream"), which is XORed to the message bits to form the ciphertext bits. If a stream cipher is good enough, then one cannot distinguish the pseudorandom bitstream from a really random one and security is guaranteed by Shannon's theorem on OTPs (One-Time Pads). However, for a stream cipher to be good enough, it requires that an attacker have many keystream bits along with enormous computational power. This is because attackers often know or could guess with high probability certain parts of the message, and

hence could obtain the corresponding keystream bits. This is called a "Known Plaintext Attack" and happens, for example, when a card transmits a known control character encrypted as a response of a protocol. Unfortunately, MIFARE Classic is not good enough, and we list below some reasons:

- CRYPTO1 uses a short — 48-bit — secret key, making it easy to be searched with modern computing power. NXP made other mistakes but this is clearly the worst one. If one could eavesdrop on an authentication session or have access to cheap and off-the-shelf commercial radio equipment, one can break CRYPTO1. Our group did so using only 16 nVidia graphics cards (from two generations ago, and they are standard— not specialty cards) in 14 hours. This attack also applies to MIFARE Classic Plus, used in 2nd generation MRT Easycards.
- The MIFARE Classic protocol uses parity check bits, which is fine — except when you first compute the parity bit and then transmit it along with the message byte. Clearly this leaks information. What is worse is that this parity check bit is encrypted with the same bit of keystream that is used for the first bit of the next byte, leading to leakage of extra information. A rough estimate is that this problem leaks about 1/8 of the bits in a key.
- In first-edition MIFARE Classic cards, the random number generator used for the nonce ("number used just once") has only 216 = 65536 outputs. This makes it ridiculously easy to go over all possibilities, and one can even make timely attack so as to repeat a nonce, making brute-force attacks much easier.
- When an authentication phase is not complete, theoretically a card should always give the same response, some equivalent to "I do not understand." However, MIFARE Classic fails to do so, and different responses to failure give an attacker even more ways to garner side channel information.

An RA with the graphic cards used for our cryptanalytic efforts.

The only saving grace among all these problems is that none of them leaks the master signing key of the vendor (i.e., Taipei's Easycard company). However, an eavesdropped session let an attacker (through attacking CRYPTO1) read and modify all data on a MIFARE Classic card, making it the equivalent of an unprotected USB drive on a network as far as security is concerned. The MIFARE Classic Plus did patch the latter 3 holes, but compatibility means that the short key length has to be retained. Therefore as mentioned above, brute-force attacks still works fine against the 2nd generation Easycards.

In summary, making micropayments with Easycards does make life easier, but the security of MIFARE Classic as part of the supporting infrastructure should be carefully scrutinized. Of course MIFARE Classic makes up but one small—and terminal—piece of the puzzle, but lower security means that forgery and leakage of personal information raises the hidden cost of using this technology. In particular, catering to legacy cards means that to sustain the system the users would lose out in terms of privacy. The corporations dealing with MIFARE Classic cards such as Taipei's Easycard must be carefully monitored and held accountable, and not allowed to transfer the cost to the society as a whole. Only when such contactless smart cards are made secure can authenticating and micropayments based on such cards be popularized safely, resulting in the greater good.

Distinguished Lecture Series

New Frontiers in Formal Software Verification

Gerald J. Holzmann — April 9, 2012

"Much progress has been made in the last ten years to reduce the time required by model checkers to perform correctness checks from hours to seconds."

Technical Computing: Past, Present, Future

Dan Reed — May 7th, 2012

"This talk will examine the scientific, technical, and social issues around high-performance computing, computational science, research empowerment, and new scientific domains."

Human Computer Intelligent Interaction

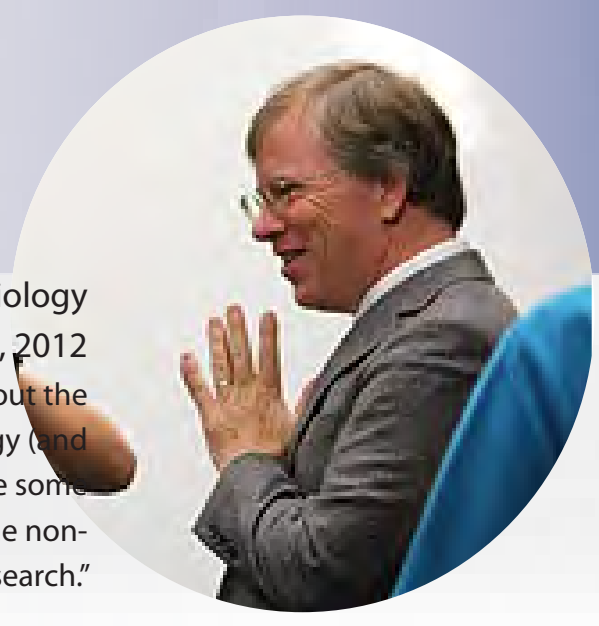
Thomas S. Huang — July 3, 2012

"The tremendous computing speed and the enormous storage capacity come to naught if we do not have intelligent human–computer interfaces. In this talk, I shall describe some of the research my students and I have been doing during the last decade on Human–Computer Interaction."

Towards Google-like Search on Spoken Documents with Zero Resources

Kenneth Church — September 17th, 2012

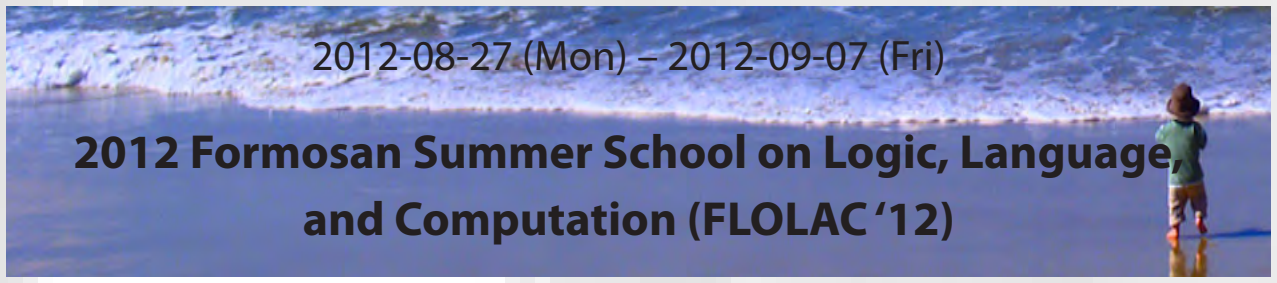
"Many of these systems, especially ASR [automatic speech recognition], are often based on large (expensive) linguistic resources. When we have resources, we should use them. But when we don't, we can still do much of what you can do with bags of words (BOWs), even when many/most/all terms are out-of-vocabulary (OOV)."



Model Checking Cell Biology

David Dill — August 7, 2012

"Perhaps techniques from formal verification could lead to insights about the systems principles that allow biological systems using very low energy (and high noise) components to function dynamic environments. I will explore some past and future research directions in this area, as well as some of the non-computational challenges that arise in this kind of research."



2012-08-27 (Mon) – 2012-09-07 (Fri)

2012 Formosan Summer School on Logic, Language, and Computation (FLOLAC '12)

Researchers in Taiwan who are interested in the foundational aspects of computing science have founded a number of research teams and worked together in some joint projects. As in any discipline, a student will have to go through a series of courses to be prepared for further research in this field. Being affiliated to different institutes, however, the researchers often find it difficult to lecture all these courses alone. It is thus desirable to bring together those who share a common interest and give lectures together.

The aim of this summer school is to give a collection of courses that would prepare the students with enough knowledge to carry on research in foundational computing science. The courses on the even years cover advanced topics in programming languages, those on the odd years on model checking and program verification. The theme of this year is "Advanced Programming Languages and Type Systems".

FLOLAC was held in 2007, 2008, 2009, 2010, and 2011.

The summer school consists of 54 hours of lectures and lab/tutor sessions. In addition, there is a 3-hour exam and a 3-hour research seminar. Students who passed the exam will be awarded 3 credits from National Taiwan University.

further information: http://flolac.iis.sinica.edu.tw/flolac12/doku.php?id=en:start

CODATA 23
Taipei 2012

Open Data and Information for a Changing Planet

2012-10-28 (Sun) – 2012-10-31 (Wed)

Plenary Room in the Humanities building, Academia Sinica

The theme "Open Data and Information for a Changing Planet" encompasses some relevant issues in data-intensive scientific fields. Nurturing an open environment for data and information is crucial for disseminating research results to a wide audience and allowing thorough, collaborative analysis. Also, the theme distinguishes between data and information and by so doing highlights the role data-intensive science plays in transforming raw observations into applicable, intelligible results and discoveries.

ADVISORY BOARD MEETING

The biannual meeting of the Advisory Committee concluded on May 18. Because the committee members are all internationally acclaimed in their fields, our researchers are always eager to take advantage of their visits to exchange ideas with them. The Advisory Committee also helps determine the direction the institute will take.

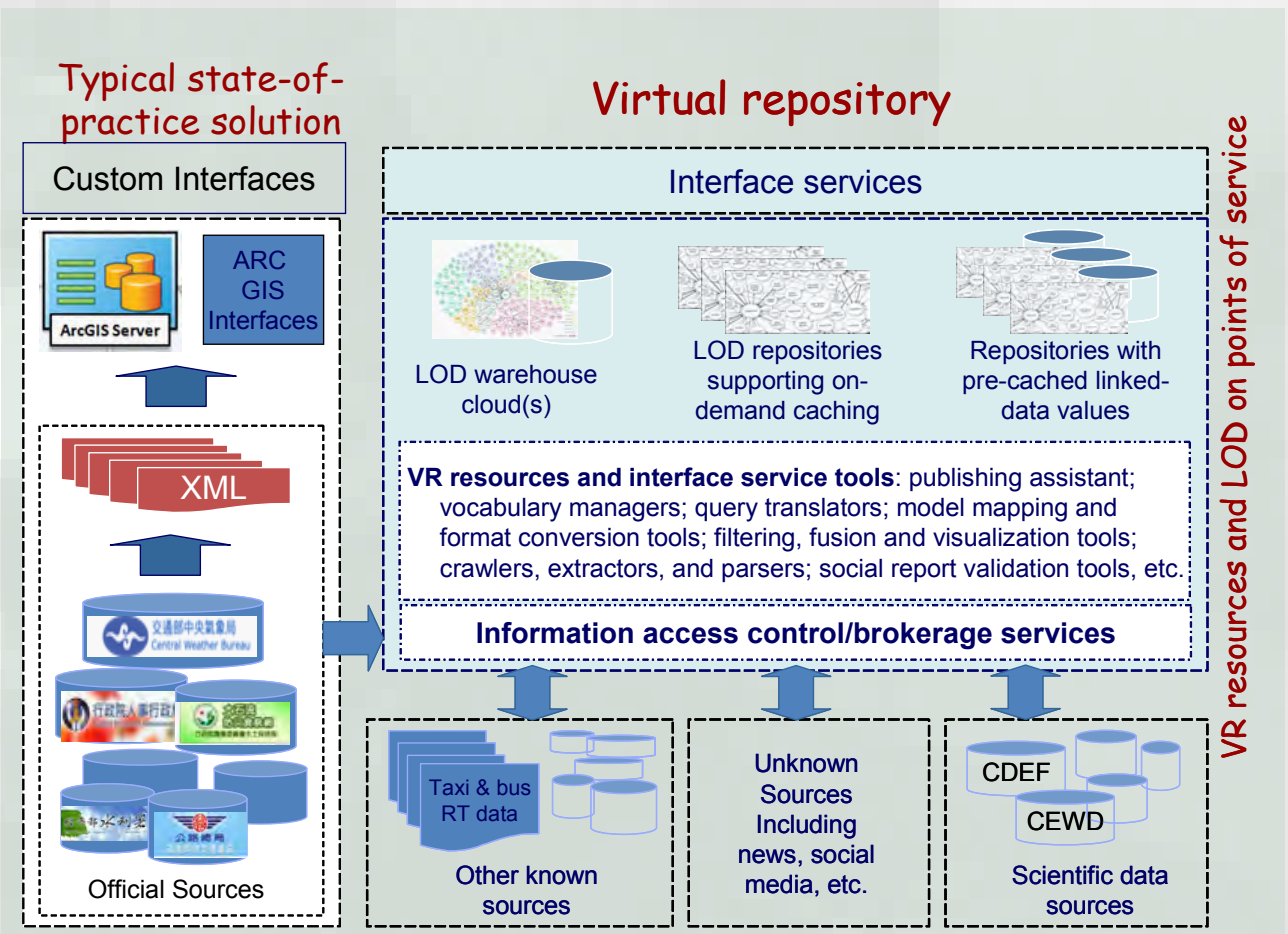
Network Systems and Services Laboratory
Making the World a Better Place with Innovations in Network, System, and Service Technologies

Jan-Ming Ho
Ling-Jyh Chen
Meng-Chang Chen
Sheng-Wei Chen
Wen-Tsuen Chen
Tyng-Ruey Chuang
Jane W. S. Liu

At the Network Systems and Services Laboratory, our research addresses several aspects of network systems and services, including improving wireless and delay-tolerant network protocols, leveraging human computation capabilities to help meet key challenges, developing critically needed information and communication technologies for disaster management, and seeking solutions to network computational problems regarding the provision of large-scale financial-risk-management services.

We study networked sensing systems, including those that focus on energy efficiency and large-scale sensor data management. Among our achievements is the development of an adaptive GPS scheduling algorithm to prolong the lifespan of GPS-enabled mobile sensors, and the design of an algorithm to adjust the duty cycles of GPS receivers and the radio interfaces of mobile sensor devices in accordance with surrounding contexts inferred by low-cost sensors, e.g., accelerometers and thermometers. We have proposed a lightweight and lossless data-compression algorithm for spatio-temporal data and designed a set of data query algorithms to support spatio-temporal data calculation using the compressed data directly. The results of our research have been implemented in two real-world networked sensing systems: Yushan Net, a mission-critical sensor network to aid the tracking, search, and rescue of hikers in Yushan National Park; and TPE-CMS, a mobile phone sensing system to measure crowding on public transportation in the Taipei metropolitan area .

In the past few years, we have performed extensive studies on the performance of GWAP (Games with a Purpose) systems and designed a human computation game to collect diverse user annotations efficiently. In addition, we have proposed a cheat-proof framework that can be used to assess the quality of experience provided by multimedia content. We have found that crowdsourcing is indeed a powerful strategy for applying collective intelligence to AI-hard pro-



Open ISDM: Open Information Systems for Disaster Management

blems. We will continue to study how best to use crowdsourcing to overcome challenges in a variety of areas.

We are collaborating with researchers in other sections of Academia Sinica, such as the Institute of Earth Sciences and the Center for Climate Changes, along with computer science and engineering faculty members of several leading universities in Taiwan and the United States, to develop an open framework for DMIS free of these limitations . This framework will allow independently developed applications and services to use information from independent sources and can readily accommodate new information sources and applications as needed in response to unforeseen crisis situations.

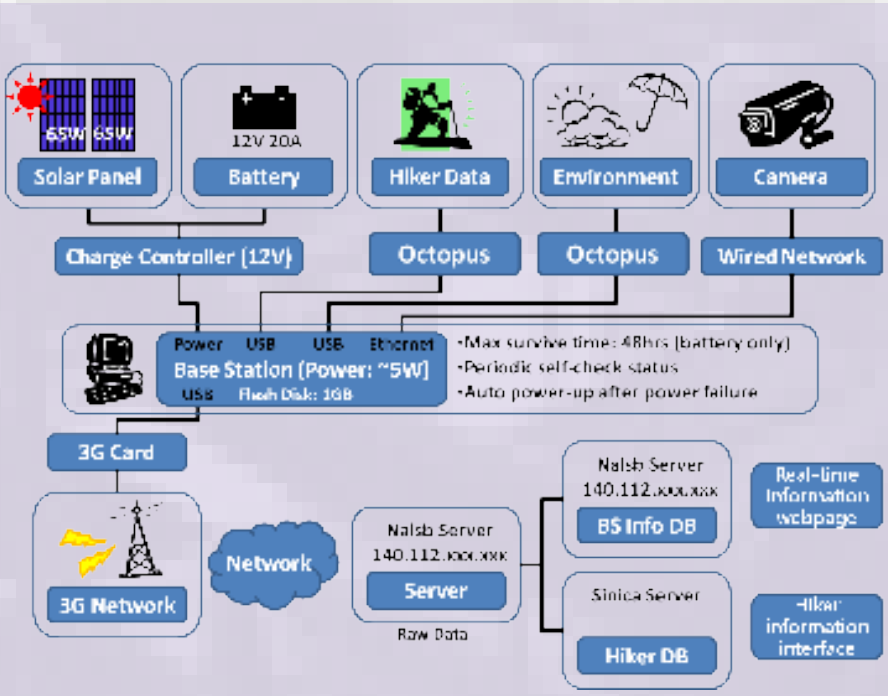
Current projects by members of our laboratory include

- the development of smart cyber-physical devices and applications as elements of a smart environment for disaster preparedness
- strategies for crowdsourcing the collection of sensor information to complement data from in-situ physical sensors
- methods and tools for reducing the amount of work humans must perform collecting, validating, and refining disaster-related information in social reports
- methods and tools supporting communication and computation infrastructures for gathering, caching, fusion, and distribution of ubiquitous and heterogeneous real-time streaming sensor data and information to res-ponse centers, individual responders, and volunteers during disasters
- the exploitation of complementary merits of different network access technologies, approaches, and network types to make the physical connectivity as robust as possible during and after disasters.

We are also studying network computation problems relating to the provision of large-scale risk-management

(cont'd on page 11)

Quadrant of Euphoria a Crowdsourcing Platform for QoE Assessment

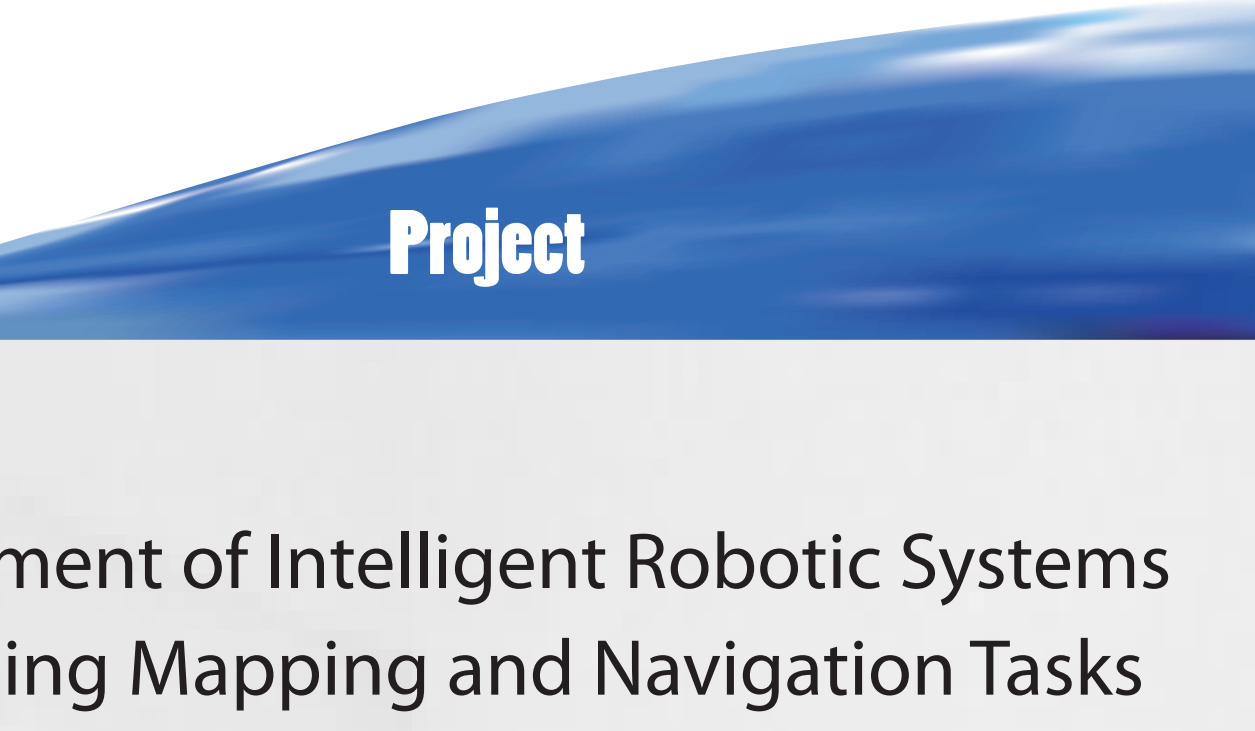


Yushan-Net

Development of Intelligent Robotic Systems Performing Mapping and Navigation Tasks

Project Coordinator

Dr. Liu, Jing-Sin



Incorporating different software/algorithms and sensors makes a variety of indoor navigation missions possible.

Robotics has been attracting attention for more than 50 years. Comparatively recent enormous advances in technology — such as in computing, sensing, and embedded systems — however, have helped dramatically diversify the forms and applications of robotic systems. For example, robotics is finding ever-increasing applications in surgery, military missions, and daily life.

The development of intelligent robotic systems to ensure the safety and comfort of human–robot interaction is of paramount importance in current and near future robotics research. Creating robots that work well as helpers of human beings requires not only careful planning and control, along with a deep understanding of the theory and technology of sensing, but also the balanced integration of all of these.

Our robotics research currently focuses on two basic capabilities for mobile robotics: 3D map building and navigation in indoor environments (such as homes and offices). We have built a platform to experiment with using a rotating 2D laser range finder to acquire 3D environment data. The rotating mechanism is a four-bar crank-rocker with simple harmonic motion. The robot with this mechanism is required to autonomously navigate to the goal by planning a path and avoiding obstacles, all the while exploring the environment.

We further developed indoor-navigation and mapping algorithms the mobile robot has tested in the real world. In our research, edge tracking navigation has been used, edges of obstacles or corners of walls can be identified from the readings of the sensor, certain edges or corners are set as temporary targets and certain areas are marked as repulsive. This method can lead the robot move as straight

as possible while avoiding collisions, also enhance moving efficiency and requiring significantly less memory. Video of experiments in 2D and 3D map building, along with 2D navigation, in the IIS building can be viewed online:

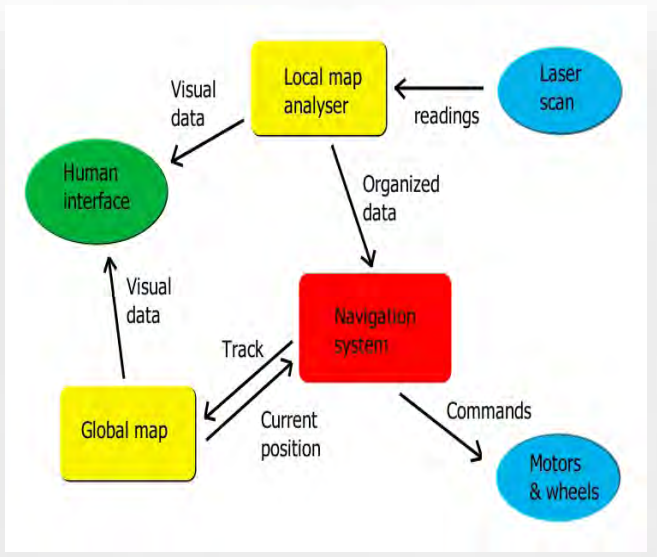
2D map building: http://www.youtube.com/watch?v=RpI7tuGHsUA
3D map building: http://www.youtube.com/watch?v=ceBAgnJhack
navigation: http://youtu.be/jGuq4SsEN9Q

By making use of various programs/

Roomba.


Nao robot.

algorithms and sensors, indoor navigation systems can provide as-sistance in many areas, including ex-ploration, 3D map building, surveillance (through tracking and pursuit), and mobile health care. A current area of interest is boundary patrolling, while applying our work to the fields of pursuit-evasion and home care (using the integration of navigation and mapping) show great promise.



Sytem overview.


Sony humanoid robot.

Network Systems and Services Laboratory

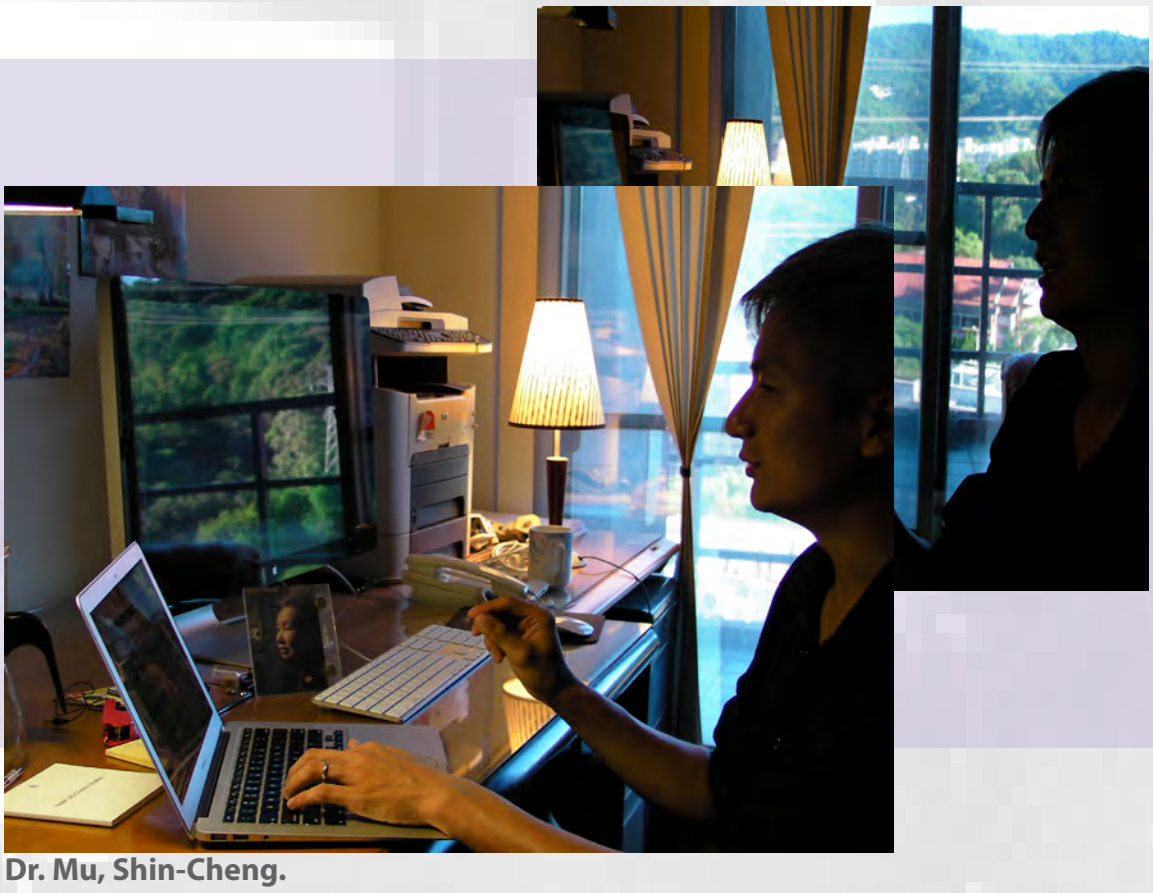
(cont'd from page 9)

services. Although many others have applied economic and financial theories and studied financial risk management, the worldwide credit crisis of 2008 demonstrates the continuing vulnerability of the financial industry. Even the three major rating agencies have been unable to report major default events efficiently. In the case of Enron, its bonds maintained "investment grade" ratings until five days before the company declared bankruptcy in 2001. In 2008, Lehman Brothers had "investment grade" ratings even on the morning the company declared bankruptcy.

Ratings companies claim their reports provide a long-term perspective rather than providing an up-to-minute assessment and note that in rating the credit of a company there are hundreds of firm-specific and macroeconomic variables. There is no doubt that assessing credit risk in real-time is indeed a task with high computational complexity. Nevertheless, accuracy in this is important for maintaining the stability of the financial market. Our research complements economic and financial theories and practices in risk management, adding the development of computing technologies using a cloud-computing framework to help achieve large-scale real-time financial risk management services, including (1) the real-time rating of company credit, (2) the real-time rating of personal credit, and (3) the pricing and risk measures of financial products.

Math is a Discipline to Explain Knowledge in the Simplest Ways

Dr. Mu, Shin-Cheng *Assistant Research Fellow*



Dr. Mu, Shin-Cheng.

Please briefly describe your background and factors triggering your interest in learning?

In the field of computer science, my interest is "programming language." When I introduce my work to outsiders, I often described it as "computer science with heavier emphasis on mathematics." Though, during my pre-college education, I wasn't particularly good at math.

Since I was a kid, I started to use computer and write programs. It was after many years when I learned that during that period, gaming industry was strictly forbidden in Taiwan. Consequently, many factories began to manufacture Apple II clones for survival before switching to the production of PC clones later on. My parents bought one Apple II clone when I was ten years old. At the time, it was easy for people to describe the functions of a TV, a stereo equipment, or an air conditioner. However, few people could clearly tell the works a computer could achieve, especially in view of its limited functions. Like most kids, I only used the computer as a gaming device. Programs at that time were recorded in cassettes, which had to be loaded into a computer through a tape player. After I got tired of playing games, I would read books and magazines that came with the computer, learning to write programs. I started from simple ASCII graphics and small games, such as horse racing. Since I only recognized English letters, instead of any words, I memorized the commands letter by letter. I had to retype the programs every time when I turned on the machine, since I didn't know how to store the programs into recording tapes. Gradually, structures of the programs became clearer in my mind and I noticed myself capable of making the programs shorter and shorter. In retrospect, I see it as a process of understanding the programs in a more abstract level.

Then, I became interested in programming language. I thought the beauty of the discipline lies in understanding a problem in an abstract manner and writing it down in proper notation, thereby producing clear solutions. The discipline tells us the importance of abstract understanding and good notation.

When I was in junior and senior high, I spent much time in Kuanghua marketplace and became a member of an underground store then, because the owner pledged to give me a copy of a LISP compiler. It turned out I was the first member of the store, which later on enjoyed prosperous business. Kuanghua Marketplace was an important channel for obtaining various kinds of software, as it housed many illegal counterfeit software firms, whose customers included students, aficionados, and foreigners. I bought the book "Inside Macintosh," in three thick volumes, and read them by using dictionary to check vocabulary, learning

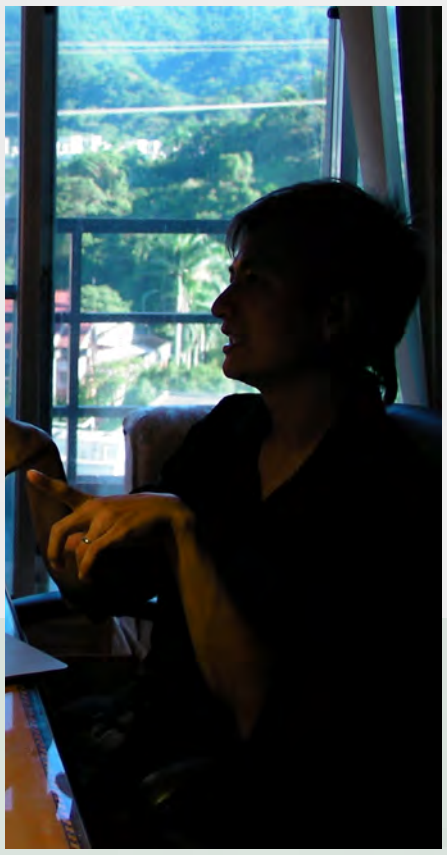
how to write programs on Macintosh computer. Several years later, there emerged a computer craze in Taiwan and parents rushed to send their children to learn computer. At that time, my family worried that I was fascinated by computer, which could affect my performance in college entrance examination. My mother asked the boss of the computer store to advise me not spending too much time in computer. One day, he seriously told me that "I suffered a lot from low educational degree. You have to take good care of your school work."

Your research interest is Programming Language, which is not exactly a popular field in Taiwan. What makes you decide to choose this as your research field? Is there any scientist that you look up to?

After becoming a computer engineering major, those "computer books" I once had to hide and read secretly now became my homework. That was one major change. Computer Engineering was a popular discipline, but I chose a field that not many people were interested in. It might also be the reason why I later became Prof. Richard Bird's student, since he couldn't find many people who are interested in program derivation. Despite what others say, I stubbornly stayed in this field and become one of those with high educational degree. It is strange how life works; though I have chosen an unpopular field, my interest was categorized under a popular industry. Sometimes I felt it unfair for my friends, who like me stubbornly stayed in their field but do not enjoy as much resource as I do. That makes their courage all the more admirable.

It was by accident that I came by a book on functional programming. Then someone recommended to me Introduction to "Functional Programming" by Richard Bird and Philip Wadler. I found "this is exactly what I was looking for," but none of my classmates could understand what I was talking about. One day, I discovered an advertisement looking for a research assistant by Dr. Tyng-Ruey Chuang, and one of the requirements was ability for functional programming. I was so excited that I ran by leaps and bounds to my dorm and I couldn't wait contacting Dr. Chuang for the position. That year, I started at IIS, Academia Sinica as an intern. Everything was so fresh and new. What I remember most is one occasion when Dr. Chuang reproved me. I was trying to explain to him an idea in front of the whiteboard and then he said that "You might know it, but you have to explain it in an understandable way for others." That taught me that only when you can explain an idea clearly, you truly understand the meaning behind it. It is similar to write a clear program.

After deciding what I was interested in, the road lying ahead of me also became much narrower. When most of my classmate became computer engineers, I needed to study aboard to pursue my interest. A year before



The silhouette of Dr. Mu while thinking profoundly…

applying for school, I read "Algebra of Programming" by Bird and Oege de Moor. I couldn't imagine that one could approach programming in such a way. I thought it would be amazing if I could learn it. But could I make it? My math wasn't that good. Anyway, I sent my application and was lucky enough to become one of his students. During those years at Oxford, I was spoiled in academic study completely. Although we all had different topics, we were all speaking the same language. Math, at least the part that we all needed, is not that inaccessible. Math is a discipline that tries to explain knowledge in the simplest ways. I had only realized that till college. It seems that all my math education below high school is a waste. It's a pity that by the time I graduated, only a few people were interested in "program derivation."

"It's your turn to carry the torch," they said.

Richard Bird is the ideal scholar in

(cont'd on page 15)

Free & Open Source Software Makes Your Life Easier!

Free software, or open source software, is more familiar to people living in the world of explosive Internet information than days before. The advantages of free software lie in free usage and redistribution, besides above, the greatest advantage, as well as open source code. Programmers can easily join an open source project to fix bugs or develop new functions. Open Source Software Foundry (OSSF): http://www.openfoundry.org/ is an open source project, as its source code can be downloaded from the website. Open Foundry is a great website which offers many project management tools to developers helping them manage their software projects easily. It also provides teaching materials, resource catalogs, and bi-weekly newsletters, in addition to organizing promotional events for open source software. OSSF is looking forward to your participation!

Xmind

Mind map is be a very useful tool, not only for helping us think, but also for taking notes, inspiring ideas, organizing your writing, and recording conferences, etc. XMind is an open source mind-mapping software tool, similar to FreeMind. Like FreeMind, it helps users easily create mind map diagrams, while offering a much wider range of colors. In addition to a free version, XMind has a commercial version with additional functions that users can access with a monthly subscription.

GanttProject

GanttProject is an open source project management tool, designed to help manage resources, schedules, tasks, sub-tasks, record task logs, time logs, etc. While making schedules, it allows users to draw Gantt or PERT maps. Files can be produced in the formats of PNG, PDF, or HTML. In addition, it can also incorporate Microsoft Project files.

OpenVAS

OpenVAS stands for Open Vulnerability Assessment System and is a network security scanner with associated tools like a graphical user fontend. The core is a server component with a set of plugging to test various vulnerabilities in remote systems and applications. The release introduces new features and a new architecture which forms the basis for turning the vulnerability scanner into a vulnerability management solution. The GPL-licensed Open Vulnerability Assessment System (OpenVAS) has become the Open Source Network Vulnerability Scanner. It undergoes the largest open collection of vulnerability tests, the daily updated OpenVAS NVT Feed with over 15,500 Network Vulnerability Tests (NVTs).

Blender

Blender is a 3D graphics application released as free software under the GNU General Public License. It can be used for modeling, UV unwrapping, texturing, rigging, water simulation, skinning, animating, rendering, particle and other simulations, non-linear editing, composing, and creating interactive 3D applications, including games. Blender is available for a number of operating systems, including Linux, Mac OS X, and Microsoft Windows.

To promote the development and use of open source software, Open Source Software Foundry (OSSF) provides a forum that facilitates interaction and collaboration between open source software developers, and serves as a bridge to link developers with industry and academia.

tel.: (02) 2788-3799 ext. 1469, 1477,

e-mail: contact@openfoundry.org

Web site: www.openfoundry.org

(cont'd from page 13)

my mind. His speech was powerful and clear. Even at the level of full professor and at the age close to retirement, he still wrote his own program. He could solve my technical issues faster them me. Often I would make up a solution, which always made him frown, and he would redo the problem from scratch, organizing everything in a clear and graceful way. Unlike most full professor in Asia who doesn't do their own research anymore, he is my idol. I wish that one day when I am at that level, I would still work on my own research. It was years later when I learned the truth, that it was due to lack of funding and resource that forced Bird to do everything by himself.

My other idol is Edsgar Dijkstra. His paper is direct to the point and such a pleasure to read. He makes you believe that you need computational science for the inspiration of mathematic.

Like his paper, he is a passionate and persevering person, and has a strong sense of right and wrong, which may be his major drawback too. A scholar who was a colleague of Dijkstra at a school in Holland asked me, "Do you teach Dijkstra's stuff in Taiwan?" The scholar told me "No one teaches his stuff at our school anymore. He had offended everyone before he left."

What is the goal of your study? What difficulties have you encountered and what part of human life do you want to improve?

This is a tough question. Knowing that there are many things out there that I still don't understand makes me extremely uncomfortable. When I was still a child, I often felt lost in many problems. Then gradually I understood more things and one program after another becomes clearer to me. That's when you realize how much you still don't know, so I keep pursuing the next goal till today.

People are born with curiosity and the sense of aesthetics. Curiosity often makes you sleepless. I often lay awake in bed at night, trying to figure out the answer to a problem, and once I had the answer, I would jump up and down with joy and couldn't wait to share it with someone else. I often told others that I'm in the entertainment industry. You can also interpret it as "research is the roots of happiness."

What advice would you give to prospective students of information technology?

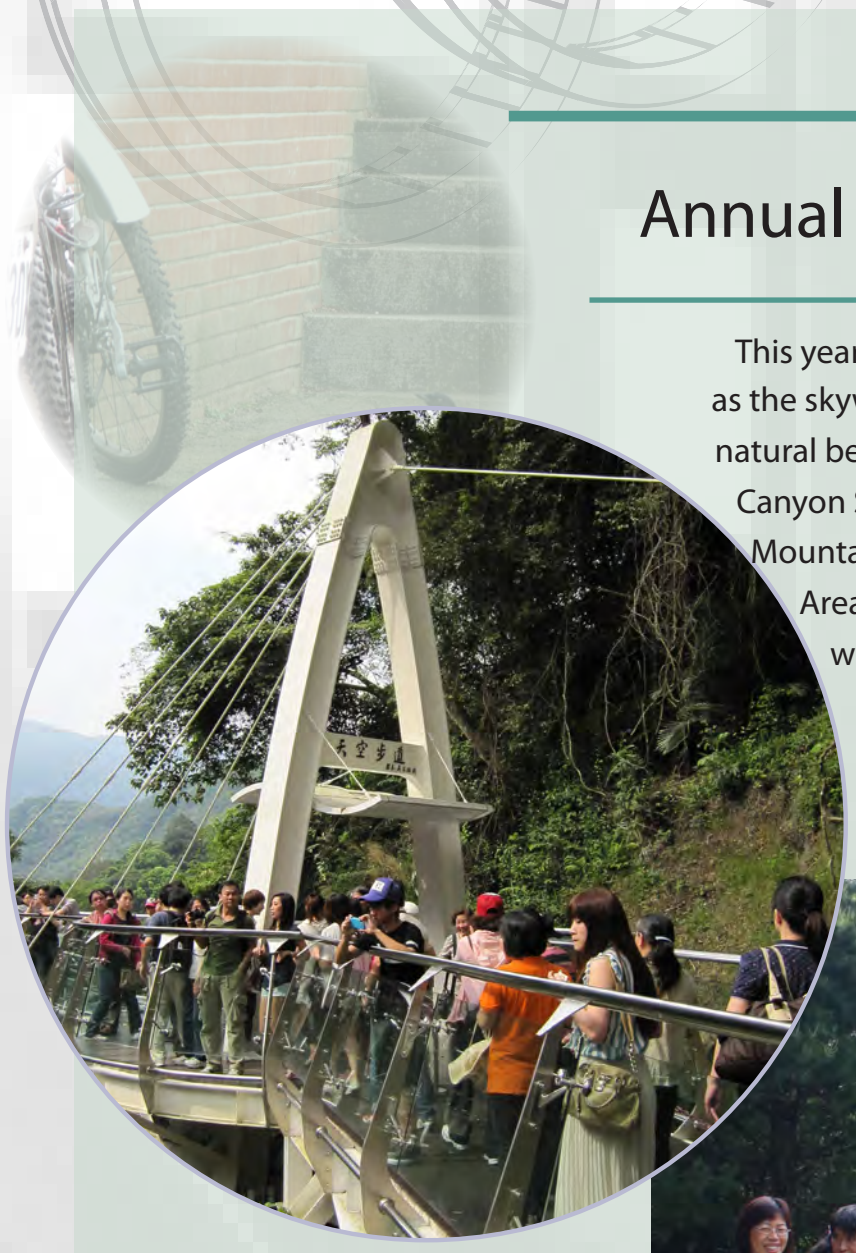
Recently, I truly felt that due to the training we have received, we are captivated deeply by our predecessors' achievement. Therefore, we regard those newly developed areas too "engineering-oriented," without the beauty and depth that we look for. But we have to understand, that the "beauty" which we have known and learned to appreciate resulted from the effort of our predecessors in organizing messy stuff.

What we should do is to concentrate on those unpolished areas and do our best to discover the hidden beauty. I believe this is exactly what Dijkstra means when he said "Beauty is our business."

ACTIVITIES

Annual Field Trip

This year's annual field trip included such sites as the skywalk in Fuxing, Taoyuan County, whose natural beauty is said that rival that of the Grand Canyon Skywalk in the United States; Jiaoban Mountain; and Taoyuan's Fairy Valley Scenic Area. The trip was a tremendous success, with the record number of participants all having a all great time.



Institute of Information Science
Academia Sinica
128 Academia Road, Section 2, Nangang, 115,
Taipei, Taiwan
tel.: +886-2-2788-3799
www.iis.sinica.edu.tw
Publisher: Director Wen-Lian Hsu
Editors: Pei-Chi Wang and Huey-Chyi Chris Tseng