Communications Research Centre Canada
An Agency of Industry Canada

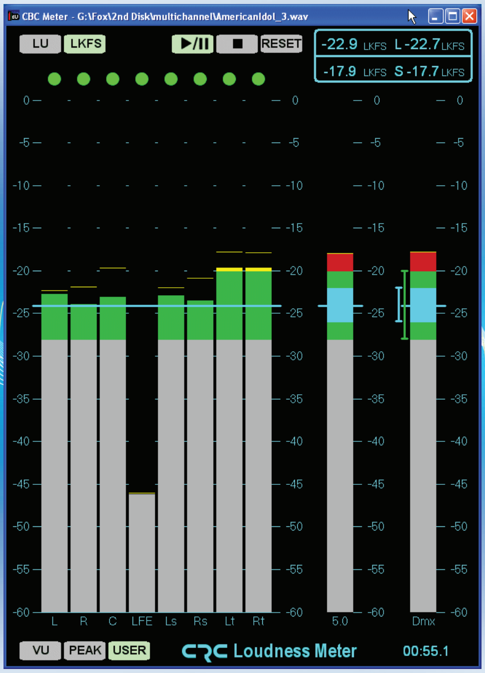
Centre de recherches sur les communications Canada
Un organisme d'Industrie Canada

Eye on Technology

ISSN 1717-7294

Issue No. 10 - Spring 2009 | www.crc.gc.ca

In This Issue...



CBC Meter - G:\Fox\2nd Disk\multichannel\AmericanIdol_3.wav

-22.9 LKFS L -22.7 LKFS
-17.9 LKFS S -17.7 LKFS

This display, of the new ITU-R loudness meter developed at CRC, is the result of CRC's collaboration with CBC/Radio-Canada. CRC is assisting Canada's national public broadcaster in the integration of the new loudness meter into its operations.

CRC Loudness Meter Chosen as International Standard

The detective creeps forward, gun drawn, barely a shadow against the dilapidated wall. Above him the clouds break, sending down a shaft of moonlight. He flattens himself against the wall knowing, just as you do, that if he's seen, if he's caught, the outcome will be death. The music, quiet and intense, builds slowly in the background. Suddenly, in the darkness, a twig snaps behind him. He whirls around … and the program cuts to a commercial that sends you shooting from the couch. You, and a million other viewers worldwide, dive for the remote to turn the volume down.

You can subscribe free of charge to this newsletter by e-mailing eye-on-technology@crc.gc.ca with the word "SUBSCRIBE" in the subject line.

If this scene sounds familiar it's not surprising. Radio and TV audiences routinely complain about jarring changes in loudness between commercials and programs; when switching from one station to another; even between different programs broadcast on the same channel. As of this spring, though, thanks in part to a new loudness meter developed by the Advanced Audio Systems group of the Communications Research Centre (CRC), lunging for the remote may soon be a thing of the past.

The Highs and Lows of Digital Conversion

Controlling loudness levels in broadcast media has always been a challenge, explains Anthony Caruso, Director of New Broadcasting Technology at the Canadian Broadcasting Corporation (CBC), but with the advent of digital technology broadcasters realized that a solution had to be found.

"When we began to migrate television from analog to digital we realized that the audio signal couldn't be carried separately from the video signal. It had to be embedded in the video stream."

This created a problem, says Caruso, because broadcasters get product – TV and radio programs as well as commercials – from producers around the world, and what is an acceptable loudness level in one country may be too loud or too soft in another. With the audio embedded in the video stream, however, the only way to "turn down the volume" is to decode or decompress the signal, readjust the audio portion, then recompress the whole thing. Not only is the process expensive, but it degrades the signal – especially the video signal – to an unacceptable level.

By the year 2000, broadcasters realized that the solution was to control loudness at the production stage, and the best way to do this was for the International Telecommunications Union (ITU) to set a standard – a sound level that all members would adhere to when producing broadcast material. But for all the members to adhere to a standard, they needed a uniform way to measure loudness and that, says CRC's Louis Thibault, Manager of the Advanced Audio Systems group, is not as straightforward as it first might seem. Take *Batman*, for example: a scene where he blows up a car is significantly louder than the romantic interlude where he holds his love-interest in his arms. Viewers don't leap to adjust the volume, however, so how exactly is the audience deciding if a program is too loud or too soft? What the ITU needed, says Thibault, was a loudness meter that accurately mimicked how people perceive loudness when watching TV or listening to the radio. While there were several meters on the market that purported to do just that, the ITU required solid scientific data to determine which one did the best job, and that task fell to CRC.

Perceived Loudness

"What we needed to do," says Thibault, "was to compare the loudness values calculated by the meters against the subjective values of loudness perceived by real listeners, so we needed a database on how people hear radio and TV."

The ITU asked five institutions around the globe – including CRC's Advanced Audio Systems group – to act as test sites to create such a database. Subjects were brought into a specially designed listening room and asked to match the loudness of a series of audio clips to the loudness of a reference clip. Test clips were taken

from real broadcast material provided by ITU partners and ranged from newscasts, to classical music, to gun battles. When completed, the test data from all sites were then sent to CRC.

"The first thing we did," explains Thibault, "was compare the data to see if all the different sites got similar results. Once we knew that they had, we averaged across all the labs and calculated a subjective loudness gain or loss for each particular clip."

In other words, they figured out how much the subjects turned the volume up or down to match a particular clip to the reference-clip volume. This gave them a subjective measure of the perceived loudness for each of the clips against which they could compare the objective measure calculated by the meters. If a meter was good, it would score the clips in the same way the study's human subjects had.

Testing Meters

With the database established, Dr. Gilbert Soulodre, the CRC researcher then in charge of the study, set about to test the 10 loudness meters that had been submitted to the ITU. But in addition to the 10, he threw in two of his own. His extensive experience dealing with objective and subjective audio testing told him that these two very simple meters – computer-based algorithms – would provide results that were at least close to those of a human listener and, if nothing else, would act as a baseline or reference to ensure that all the equipment and test meters were functioning as they should.

"The study's results – the comparison of all the meters – were presented at an ITU meeting in Geneva," says Thibault. "Gilbert presented his findings and when the committee saw them it was really quite clear. One of Gilbert's meters had a correlation of 0.98 with the listener results. A perfect match would be a correlation of 1.0, so 0.98 is incredible. Gilbert's meter was the best of them all."

Thibault says that what made the finding so surprising was that Soulodre's meter was so simple. While some of the meters modeled the complex interactions between sound waves, the ear and the brain, Soulodre's algorithm filtered out low frequencies from the loudness calculation and averaged the power of what was left.

"What it means," says Thibault, "is that when you're adjusting the volume on the TV your ear acts as a high-pass filter: it's less sensitive to the low frequency sounds. Because your ear is more sensitive to the higher frequencies, especially those between 100 Hz and 8 kHz – the dominant frequencies in human speech – you base your volume calculation on the loudness of these higher frequencies."

Public Domain

CRC published the findings and placed them in the public domain. This allows audio manufacturers, broadcasters and production houses – even small companies in poorer countries – to use the loudness meter without royalty fees.

In April 2006, the ITU adopted CRC's loudness meter as the international standard to measure loudness in broadcast productions. Integration into operations is ongoing.

Having the meter, says CBC's Caruso, will have a big impact on their operations. "The fact that we can now measure loudness is a quantum leap. The next big step will be adopting a loudness level that everybody agrees on." And that, he is hoping, will happen in late April 2009 at the ITU meeting. As part of the agenda, delegates will vote on a standardized level – most likely -24 LKFS – for all broadcast production. While the number may not mean much to the listening audience, the result will. If that vote passes, your days of scrambling for the remote will soon be over. Stay tuned.

For more information contact Louis Thibault, Research Manager, Advanced Audio Systems, at 613-990-4349 or *louis.thibault@crc.gc.ca.*

Eye ON Technology

CRC Reaches New Heights in Delivering Wireless Capability

More and more, users demand that wireless technologies provide high availability, ubiquitous communications over large areas. This becomes increasingly difficult as the distance between end users grows, as is the case for many military operations. They require reliable, strategic and tactical long-range communications even in the most challenging environments where difficult terrain is the norm.

Delivering this wireless capability can be very challenging. To help overcome the challenges, the Wireless Applications and Systems Research group (WASR) of the Communications Research Centre (CRC) has been working with the Director Land Command Systems Program Management 3 (DLCSPM 3) of the Department of National Defence (DND) on the use of aerostats to enhance wireless communications. Essentially, an aerostat is a lighter-than-air object that can be raised significantly above ground while remaining in a relatively fixed position. It can then be used to greatly improve the line-of-sight coverage of a base station radio to a number of end users located at ground level.

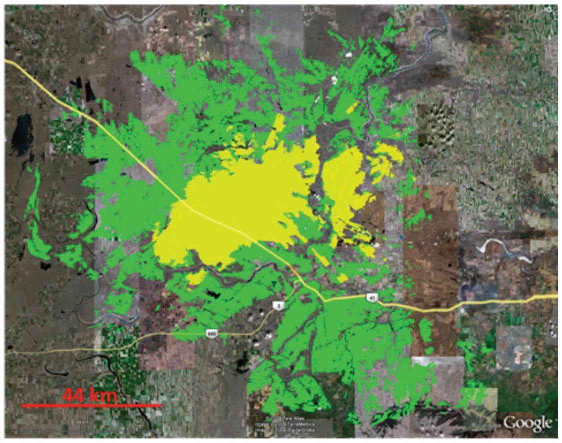
“The Canadian Military continuously searches for new technologies that can lead to innovative approaches for modern day operations. In the area of wireless communications, the aerostat is one of these technologies that is showing promise,” explains Cy Aiken, Senior Systems Engineer of DLCSPM.

Researchers conducted the first phase of this study at Canadian Forces Base Suffield, Alberta in December 2008, where DND launched an aerostat for the first time. They chose a rapidly deployable 17-meter long tethered balloon. Researchers raised the aerostat to 180 meters above ground level while it carried a variety of wireless technologies in a payload container suspended beneath the balloon.

WASR evaluated one of these technologies, an 802.16-based broadband wireless fixed WiMAX system. CRC researchers integrated a WiMAX base station and omni-directional antenna into the aerostat payload. Once the aerostat was raised, they conducted a series of tests at ground level using up to 10 subscriber units that communicated with one another via the base station on the aerostat. Researchers were particularly interested in the increased range among subscriber units as a result of the elevated base station on the aerostat, the increased throughput amongst users as a result of improved line-of-sight conditions, and improved coverage ubiquity.

The preliminary results of this work indicate that aerostats may indeed be a viable technology to improve wireless communications for military operations. WASR will continue to work with DLCSPM in this promising area.

Researchers launch an aerostat.



This diagram highlights the improved coverage resulting from the aerostat. The yellow area indicates the predicted coverage of a base station located approximately 30 meters above ground level using a sophisticated RF planning tool. The green area illustrates the coverage improvement achieved by raising the base station to 180 meters above ground level using an aerostat. The improvement is significant, with up to 50 kilometers more range in some directions.

For more information contact Joe Fournier, Senior Research Engineer, Wireless Applications & Systems Research, at 613-949-0175 or *joe.fournier@crc.gc.ca.*

Steganalysis: Detecting the Invisible

Steganography, the art and science of hiding communication, has been a part of spy craft and military strategy for millennia. In the *Histories of Herodotus*, written in 440 BC, the author recounts the story of Histiaeus, who shaved the head of his most trusted slave, tattooed a message on his scalp and, once the hair had grown back, sent the man through enemy lines to deliver the message. Unlike cryptography, where the message is evident but its meaning is obscured, the goal of steganography is to hide the message entirely so only the sender and the recipient know of its existence – what the Communications Research Centre's (CRC) Dr. Ken Sala refers to as "hiding in plain sight." And, like all things in the modern world, steganography has gone digital.

"Most people don't understand that each time you visit a website the photographs from that website are downloaded to your computer," explains Sala.

That, added to the recent proliferation of cheap, accessible steganography software, means you may already have altered or "dirty" files on your computer with no knowledge that they're there, and this has some companies and government departments concerned. While most steganography software is used for legitimate purposes, the fear is that these powerful programs could be used to mask illegal activity such as the theft of trade secrets or the exchange of child pornography. Both private companies and government departments are looking for ways to ensure their computers and websites are free of corrupted files.

"When you consider that there are over 2.5 trillion images exchanged through the Internet on a daily basis," says Sala, "the potential scope of the problem becomes clear."

Most steganography software is used lawfully for securing computer files. In the age of the laptop, where a hard drive may contain secret company files as well as bank passwords and personal information, the software can be employed to hide sensitive material and thus protect it in the event that the laptop is lost or stolen. Many companies also want to secure desktop computers within the workplace, especially those of people working on classified projects.

Sala's interest is the flip side of steganography, the science of steganalysis. While the steganographer's goal is to hide the message, Sala's research focuses on ways to detect altered files. All digital steganography involves one or several carrier files – often image files – as well as the image or message the sender wishes to hide. What is important to understand, says Sala, is that the steganography software embeds the hidden image in the binary code of the carrier file. There is no "picture-within-a-picture," so no matter how hard you stare, the faint outline of the hidden image will never emerge. Rather, says Sala, digital steganography uses binary code to exploit a weakness in the human eye.

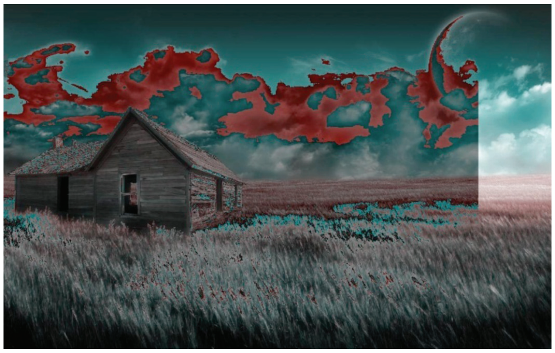
Each pixel within a digital image is made up of 24 bits of information – a string of zeros and ones that translate into the pixel's colour. But with 24 bits, a computer can generate over 16 million colours, far more than the eye can distinguish. To embed the hidden message, then, the steganography software "steals" bits from each pixel and replaces them with the binary code for the secret digital file. By stealing only the least significant bits within any pixel, the very slight alteration in hue can't be detected by the human eye. So how much information can you hide in a snapshot?

"Just think of a common digital camera," says Sala. "You have 3600 x 2400 pixels in each image, and each pixel is coded by 24 bits. I can easily steal six bits from each pixel and not noticeably alter the colours. That means I can commandeer over 50 megabits for my hidden message in only a single image. I can put the whole text of the Bible in 50 megabits."

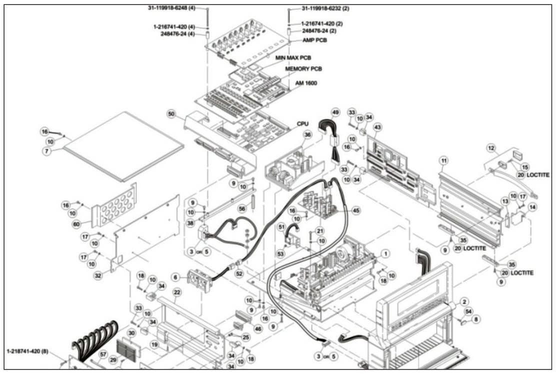
To extract the hidden image or message, the recipient then uses the software to strip away the code for the carrier file, leaving only the code for the secret message. These bits are then reassembled into an array that can be displayed as a JPEG, GIF or other file. While this simple substitution of the hidden-message code for least-significant-bits (lsb) is relatively easy to detect, says Sala, the new, more sophisticated steganography tools now allow users to encrypt their code before embedding it in the carrier file, as well as spread it out across multiple files. Each picture in the "family album" could thus contain an encrypted section of code from the hidden message or image, and this, says Sala, makes the altered files extremely difficult to detect.

Sala's research focuses on the use of neural networks to detect hidden files. Neural networks, he explains, are computer networks made up of simple "artificial neurons" that process information. Working together, these "artificial neurons" function much like a human brain, learning from past experience and coming up with novel ways to solve a problem. According to Sala, the advantage of using a neural network to search for altered files is two-fold. First neural networks can process vast amounts of information.

Original image concealing hidden image data



Original image showing the portion containing the hidden image data



Extracted file

"You can throw tens of thousands of images per second at these neural networks and they just spit out an answer: clean or suspect."

Second, they learn, so as steganographers come up with increasingly convoluted ways to hide information, the neural network will evolve and adapt. But to carry out a complex task like detecting hidden files, the neural network, says Sala, must be trained, and this involves presenting the network with as many varieties of clean and altered files as possible.

"It's like training a child. You start with the easy stuff and progress to the hard stuff, giving feedback along the way."

Sala is currently building a database of clean and dirty files, trying to develop the most nefarious ways imaginable to embed hidden messages. These files will then be used to train a neural network to detect anomalies in a file's structure that would indicate a hidden message. If he succeeds – if he is able to train a neural network to flag suspect files – he'll have, he says, the electronic equivalent of a sniffer dog. With this powerful tool, able to scan large numbers of files in a short period of time, resources can be focussed on cracking open only the suspect files.

"To do this kind of work," says Sala, "we need something fast, that can evolve and learn, but we also need something that is in-house, not in the public domain. Once a new kind of steganalysis software is on the market, the people who are using this kind of technology for illicit purposes have already figured out a way to get around it. With neural networks, that's almost impossible."

For more information contact Ken Sala, Research Scientist, Integrated Electronics, at 613-998-2823 or *info@crc.gc.ca.*

One Step Closer to the Wireless World

In October 2008 the Communications Research Centre (CRC) hosted the 4th Optimized Link State Routing Protocol Workshop (OLSR), drawing participants from Europe, North America and Asia. They came with a single purpose in mind: to discuss and test the next generation of software that will lead to a truly wireless world. The software, being developed in part by CRC, will allow computers to communicate – to form networks – in the complete absence of infrastructure.

These mobile ad hoc networks (MANETs), explains Maoyu Wang, a research engineer with CRC's Mobile Ad hoc and Sensor Network Systems group, have tremendous potential for use in situations where the infrastructure has been destroyed by natural disasters or war. But they also have a distinctly Canadian context, she points out. MANETs could be used to link people in rural communities and, in some cases, even link those communities to the Internet by "stepping stone" nodes. While several prototype MANETs are up and running in Europe, the current version of routing software (OLSRv1) places limitations on their usefulness in real-life situations, something Wang and her CRC colleagues have set out to change. At CRC's October workshop, Wang showcased the lab's OLSRv2, a new version of the routing protocol that allows for fast and accurate movement of data within a mobile ad hoc network, but without the problems and limitations inherent in the earlier version.

"When you form a network via the Internet," she explains, "you require infrastructure. You have routers and communication beacons, fixed points that direct the flow of data packets to the various addresses. In a mobile ad hoc network you have no fixed points, so each computer must act as a router as well as an end host."

But, says Wang, getting each computer to act as a router is a complex problem. To function as a network router each computer must "know" how to send, receive and forward data packets such that they arrive at the right computer by the most efficient route, even if the end node is several "hops" away – meaning the packets must be routed through several other network computers to arrive at the end host. Each computer in the network, therefore, must be constantly aware of the network topography, and able to calculate the best possible route for a packet to travel, but the calculations must be made without using excessive memory or processing power since this is background activity invisible to the user. To complicate things further, the topography of the network is fluid. In the aftermath of a natural disaster, for example, new rescue teams may arrive by the hour and join the mobile ad hoc network to coordinate their efforts. In a peacekeeping or battle situation, a group of troops may secure an area then rapidly move on to the next village several kilometers away, all the while remaining an active node that must be coordinated with other troops.

While the first version of OLSR allows for the successful transfer of data packets within a mobile ad hoc network, says Wang, the system lacks the flexibility needed to accommodate real life applications. Compatibility is one of the issues.

"With the first version," Wang says, "if my computer sends a packet to you, your computer can only read the packet if it understands its strict definition. If there is even a little bit of the packet the computer doesn't understand, it rejects the whole packet and we can't communicate."

In addition, she says, the first version software is inflexible. To change one part of the software you have to change it all, which makes it difficult to add the features that researchers now know are necessary, such as network hierarchies and security.

"We needed a new type of protocol capable of supporting a new type of network that would be more flexible and could be easily extended."

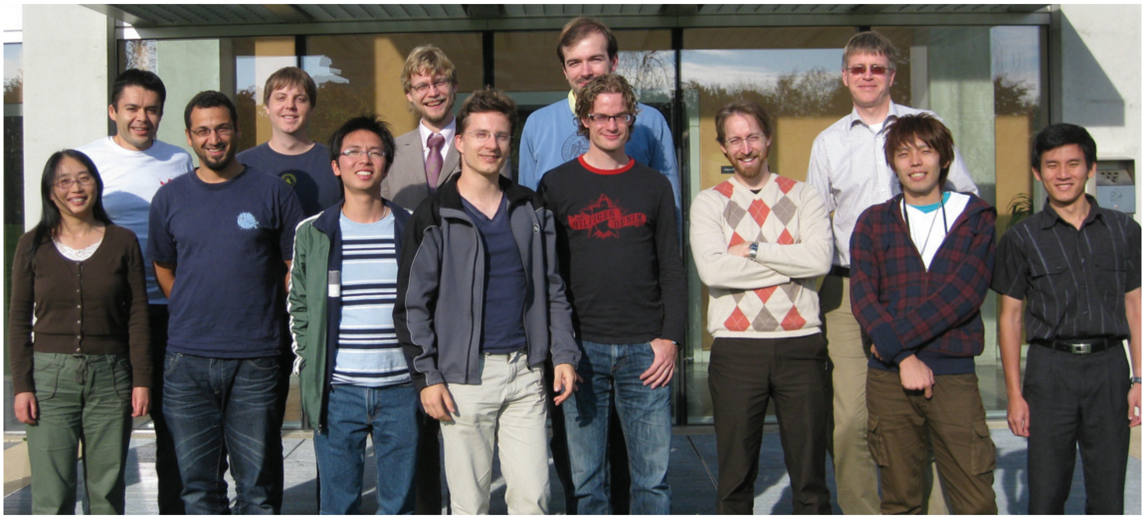
To develop the new OLSRv2 Wang and her colleagues made some conscious decisions early on. First, she says, they chose to design the new software using object-oriented programming. This would allow them to build it in modules or components. The result would be a much more flexible implementation where one component could be changed while leaving all others intact.

"This way, the software can be ported from one operating system to another. All that's required is a change in the component that communicates with the operating system."

Wang also decided to program the new OLSR in C++. While this made the actual coding of the protocol more difficult, it gave the end product much better performance than could be achieved using other languages, and increased the flexibility.

"If you receive a packet using this second version of the routing protocol, your computer just throws away the part it doesn't understand but uses the part is does understand. That's the first level of flexibility," says Wang, who adds that features can be included and the networks can be scaled up as needed.

Because the new OLSR can be easily extended, she says, it allow for the creation of hierarchies – in other words, the most powerful machines will be designated as hub or beacon nodes thus improving the efficiency and data transfer rates. The flexibility to add components will also allow designers to incorporate security tools into a mobile ad hoc network, tools that allow the network to recognize an intruder or alert network users to suspicious activity. Adequate network security is a critical feature in almost all real-world applications.



Participants at the October 2008 OLSR Workshop. Back row, left to right: Pedro Villanueva-Pena, Canada; Justin Dean, U.S.; Thomas Heide Clausen, France; Henning Rogge, Germany; Joakim Flathagen, Norway. Front row, left to right: Maoyu Wang, CRC, Canada; Aaron Kaplan, Austria; Jiazi Yi, France; Ulrich Herberg, France; Ronald in 't Velt, Norway; Yannick Lacharité, CRC, Canada; Toru Matsuda, Japan; Dang Nguyen, CRC, Canada.

The October seminar was a milestone for Wang and her colleagues. Along with several other groups developing second generation OLSRs, Wang unveiled CRC's work-in-progress. After only four months of development time they arrived with the only fully functioning software package ready for the test bed. Using the new software, workshop participants set up a 10-node mobile ad hoc network and took the new OLSRv2 out on its first trial run.

"We wanted feedback," says Wang with pride. "We were told that our implementation was the best – with the best structure, best scalability, and best extendibility – of any of the implementations at the workshop."

With the trial run under their belts and valuable feedback from workshop colleagues, Wang expects the new OLSRv2 to be ready for practical use sometime next year, a feat made possible by the unyielding support of her lab head, Louise Lamont, Research Manager for Mobile Ad hoc and Sensor Network Systems. And there is, says Wang, already considerable interest from military and civilian quarters.

"We're very proud of the new OLSRv2," says Lamont. "Here at CRC, we see a bright future for the use of the OLSRv2 protocol in tactical mobile ad hoc networks because of its flexibility and versatility."

For more information contact Maoyu Wang, Research Engineer, Mobile Ad hoc and Sensor Network Systems, at 613-991-1671 or *maoyu.wang@crc.gc.ca.*

Licensing Corner

The Value of Patent Pooling

What does 1850s sewing machine technology have in common with modern fibre Bragg grating (FBG) technology? In each case, licensing blossomed after key patents were pooled.

Patent bundling has been around since 1856 when the Sewing Machine Combination pooled various sewing machine patents. In the early 1990s, CRC and the American company United Technologies Corporation pooled their respective FBG patents into a single bundle through cross licensing. Since pooling all 11 patents that potential licensees need to employ this technology, the package has been licensed to more than 40 companies worldwide, resulting in over $10 million in intellectual property (IP) revenue to CRC alone.

After the success of FBG patent pooling, CRC signed its second cross license agreement with Toshiba to bundle their respective fused coupler technology patents, again leading to increased commercial success.

Recently, CRC has even sold some bundled, older patents, which had achieved limited commercial success. Two patent bundles were sold in the last two years, earning nearly $1.7 million. Along with this revenue, CRC will see savings in patent maintenance costs.

"Securing sales was no easy feat," says Jeet Hothi, Director of CRC's Technology Transfer Office (TTO). Its mandate is to protect, manage and exploit CRC's IP portfolio, and maximize value for CRC and Industry Canada, while providing industrial benefits to small and medium sized Canadian companies.

"After lengthy financial and legal negotiations, agreements were signed," says Hothi, "but receiving the money proved problematic." Because federal contracting regulations do not make provision for commission-based remuneration, CRC had no simple mechanism to collect the gross amount and pay the broker's commission. It had to complete the transaction through an escrow agent.

Despite the difficulties, CRC remains dedicated to ensuring that reasonable resources are committed to seeking the commercial success of all its patents. "In government labs, patents are granted only after spending considerable public funds on R&D," says Hothi. "If no Canadian licensing prospect is available, it's prudent to try to sell these potentially valuable Crown assets on the world market." Hothi explains that the net benefit is the additional funding raised by the lab, which is reinvested in the research programs and shared with the researcher(s) to reward innovation as per the Public Servants Invention Act.

CRC's Technology Transfer Office is the primary contact point for companies and other entities that wish to engage CRC under various forms of collaborative agreements and license arrangements. For more information contact Jeet Hothi, Director, Technology Transfer Office at 613-990-2089 or *jeet.hothi@crc.gc.ca*.

Software Defined Radio Success Story Now Online

Who doesn't enjoy a good story, particularly when it showcases a Canadian success? The story of CRC's involvement in software defined radio (SDR) is an inspiring account of the organization's contribution to a technology that holds great promise.

The story opens with drama: rescue crews can't communicate in an emergency situation; and quickly moves to identify the culprit: radios designed to send and receive only the respective manufacturer's waveform, using proprietary hardware. It then introduces the protagonists: the team from CRC's Advanced Radio Systems Laboratory; and it details their efforts to realize the solution: developing software to process signals, rather than dedicated hardware.

Along the way, the story tells of struggles, such as the two months spent pouring over the early military standard specifications, only to find there were too many missing pieces to design a functioning radio. It shares successes, including international acceptance of the team's proposal to help solve the problems. This turns out to be the story's pivotal point, as it leads to the team's ultimate success: designing a prototype SDR unit that can be easily replicated, and combining it with a tool kit that gives companies – including a number of Canadian companies – the chance to get started in SDR.

In short, this is a five star success story! Read the full text at **http://www.crc.gc.ca/en/html/crc/home/mediazone/success_stories/sdr_feb09**.

CRC's mission is to be the federal government's centre of excellence for communications R&D, ensuring an independent source of advice for public policy purposes. CRC also aims to help identify and close the innovation gaps in Canada's communications sector by:

- *engaging in industry partnerships;*
- *building technical intelligence;*
- *supporting small and medium-sized high technology enterprises.*