Brainlike Enabling Technology Basics

Overview

Brainlike offers a unique monitoring system based on an automated kernel module. In its simplest form, the Brainlike kernel "sniffs" input data in real-time. Whenever computer input data values are unexpected, the kernel sends an electronic alert signal. The Brainlike kernel offers a huge technology advantage: the capacity to "sniff out" truly unexpected events in a sea of changing background activity — with high precision and complete automation.

Animals routinely and automatically sniff out opportunities or dangers in novel and continuously changing environments. They do this by continuously adapting their alertness threshold levels to surrounding conditions. Likewise, the Brainlike computing system employs continuous learning of expected background conditions for identifying developing problems from real-time data.

Since background noise levels are always changing, effectively sensing what's unexpected requires that sensed activity levels be compared to background baseline levels. Under novel or changing background conditions, these baseline comparison levels should be continuously and efficiently updated. The Brainlike kernel has been carefully designed to do just that — far more effectively, automatically, and efficiently than any available alternative.

The key Brainlike benefit is greatly reduced total operating cost, which results directly from superior monitoring precision and efficient learning automation. Operational monitoring costs are directly tied to false alarm rates and target hit rates. The monitoring community complains most loudly about excessive false alarm rates. Every false alarm response costs money. Not responding to a real target event costs much more. Time and money wasted chasing false alarms could be better spent attending to real threats.

Responding or not responding to questionable alarms represents a tradeoff. Monitoring managers must decide how much they can cut costs by responding to fewer questionable alarms, at the expense of failure to prevent costly incidents. Insofar as a monitoring system is precise, fewer questionable alarms result and fewer leading indicators of developing problems will be missed. Brainlike technology can add major value over non-adaptive alternatives — by greatly improving both false alarm and target hit rates through adaptive alarm threshold monitoring.

Maintaining monitoring precision under changing conditions thus requires continuous learning. Continuous learning without automation can be expensive or even impossible. Precise monitoring requires comparing observed input values with precisely estimated expected alarm thresholds. Creating and maintaining mathematical models that precisely compute expected alarm thresholds costs money. Building, deploying, and updating monitoring estimation models that reflect all anticipated field conditions requires expert analyst resources — often far too many resources to be affordable.

Brainlike technology offers a far cheaper alternative to expert data analysis. Using a unique process that has been patented and commercially proven, the Brainlike kernel removes estimation costs by learning continuously and automatically. Each time a set of input values arrives, the kernel automatically updates its learned parameters very quickly. It also uses its learned parameters to compute estimated input values that are compared with actual values in order to assess deviance.

Figure 1 illustrates monitoring applications for Brainlike kernel technology. In monitoring applications, kernel processing units (KPUs) reduce sensor selected array data to anomaly alerts at each sensor array buoy shown in the figure. Alerts are sent only when sensor levels deviate significantly from their expected values. By continuously adjusting expected values for changing conditions, alerts are transmitted sparingly, resulting in high selectivity, sensitivity, and signal-to-noise ratios. Alarm thresholds are automatically adjusted for changing ambient temperature, salinity, sensor calibration drift, and even target characteristics.

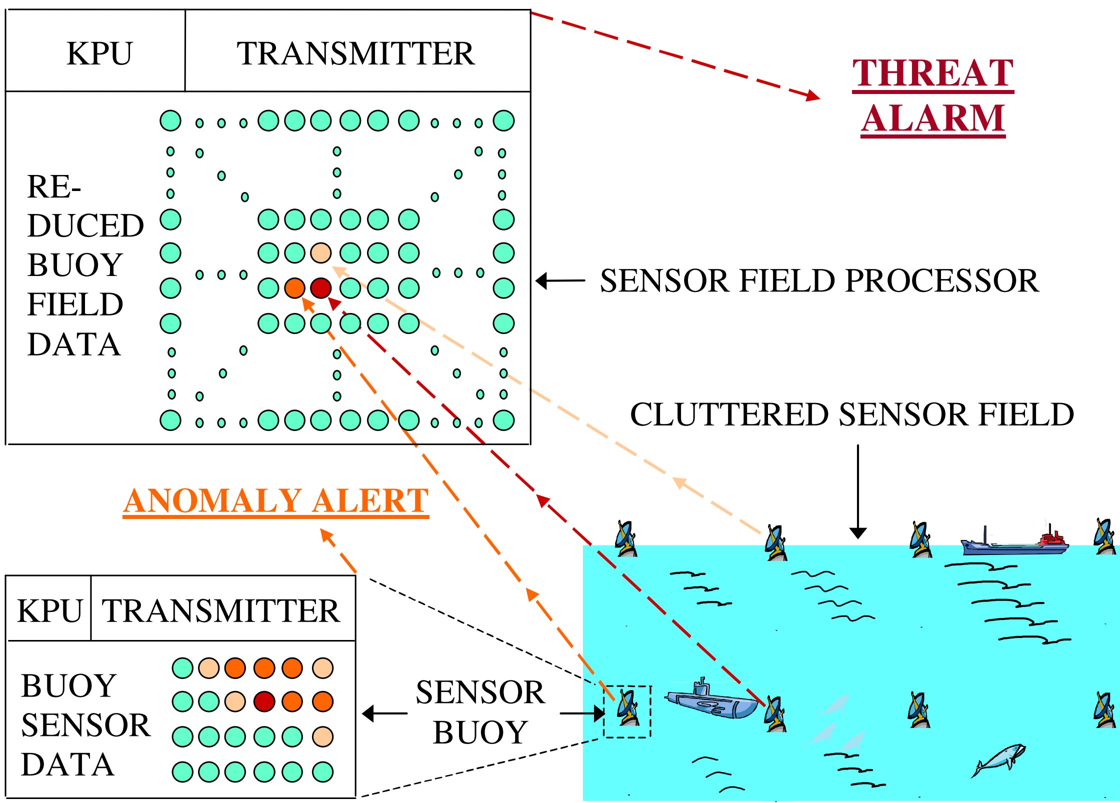

Figure 1. Monitoring Application Illustration

In it current form, the Brainlike kernel operates as a software module, which is integrated into a real-time data acquisition platform. For example, one version is being used for monitoring server farm performance. This version is implemented in conjunction with standard application performance monitoring platforms such as BMC Patrol and NETIQ AppManager. For each server being monitored, the kernel operates each time it's called by comparing about 100 counter values for the server to the values it has learned to expect. At the same time it returns counter level and server level alert values accordingly, and it updates its learned parameters, after which it awaits the next monitoring call.

For the above monitoring example, the Brainlike kernel would operate in a similar fashion, in real-time and in conjunction with a data acquisition processor such as the QUIPS system. The kernel would be called at each time point by comparing actual against expected values, returning alerts accordingly, updating its learned parameters, and awaiting the next call. The platform could be a central processor receiving multiple buoy information, a single buoy receiving multiple array information, or a single array receiving multiple sensor information.

Specific Technology Benefits

This section outlines how Brainlike solutions could meet key surveillance needs that were listed in a recent NASA solicitation. The reports that are cited below review specific monitoring case studies and provide basic Brainlike technology details.

<u>Minimizing the time between data acquisition and decision making: equipment health monitoring</u>. The Brainlike Equipment Monitoring report describes a structural test of an expensive aircraft wing. During a structural test of an expensive aircraft wing, the wing broke. The structural test engineer showed that with Brainlike strain gauge monitoring, the test would have been stopped and huge losses in time and money would have been prevented.

<u>Minimizing the time between data acquisition and decision making: sonar sensor monitoring</u>. The Military Attack Prevention report describes a case study where the Brainlike kernel converted hard-to-interpret sonar information into easy-to-understand form, in real time. Without the Brainlike kernel, subtle leading indicators of a submarine attack would not have been noticed.

<u>Minimizing the time between data acquisition and decision making: power system monitoring</u>. The Brainlike Monitoring Improvement Illustration report shows that the Brainlike kernel can identify developing electrical problems early enough to take effective action. Without Brainlike technology, such problems would remain unnoticed and cause result in major breakdowns.

<u>Minimizing the time between data acquisition and decision making: cyber security</u>. Brainlike is assisting an ARDA funded effort to establish effective responses to sophisticated cyber attacks. Part of that effort will require Brainlike monitoring for unexpected activity at very low levels.

<u>Minimizing the time between data acquisition and decision making: disease surveillance</u>. Brainlike is assisting in a study to identify causes and remedies for a major national health epidemic. Brainlike technology will figure heavily into identifying unexpected survey responses as they are being gathered, and in quickly identifying risk profiles that are most dangerous. Without Brainlike technology, data analysis turnaround for the study could take months. With Brainlike technology data analysis updating will be immediate and continuous throughout the study.

Testing and evaluation. With a mission of maintaining inter-command communications integrity, units like the Navy Center for Tactical Systems Interoperability (NCTSI) continuously test and evaluate electronic message communication quality. Units like these seek monitoring solutions that are both highly accurate and fully automated in order to minimize its total operating costs. Brainlike intends to deliver solutions that will do just that.

Monitoring on data acquisition and management platforms. Brainlike kernels reside on existing data acquisition and management platforms in the form of subroutines. For server farm monitoring, Brainlike kernels add value to commercial application performance monitoring platforms such as BMC Patrol or NetIQ AppManager. For submarine monitoring, they would reside on a platform like the QUIPS System (see Military Attack Prevention). For condition monitoring, they would reside on a system such as National Instruments LabView or a suitable alternative.

Sensor validity monitors. Brainlike kernels have been implemented as compact subroutines for implementation in special-purpose, on-board microprocessors. In one application, Brainlike monitoring showed when novel contamination sensor readings from photonic arrays should be transmitted. In related applications (see Technology Details below), Brainlike monitoring on nano-sensors will identify when novel sensor readings should be sent from computer chips.

Electrical system monitoring and fire prevention. See the Brainlike Monitoring Improvement Illustration report.

Autonomous model updating. As illustrated in the Brainlike Advantage, report, autonomous model updating is the key Brainlike feature.

Lowering the cost of online equipment health monitoring applications. The Huge Overall Savings report contains a detailed return-on-investment (ROI) analysis of Brainlike technology from a financial perspective. Major gains can be expected in Brainlike solutions, because false alarms, manual efforts, and missed target events can be enormously expensive in the long run.

Modular use of the same technology at multiple decision-making levels, and for many applications. Figure 1 illustrates how Brainlike kernels will be distributed over a multi-layer network. While the figure applies only to shallow water detection, the system it describes is very general, and it could be applied effectively in a variety of applications that are unrelated to submarine detection.

Costly incident prevention. One of the key themes underlying the Brainlike value proposition is identifying developing problems early enough so that preventive action can be taken prior to catastrophic failure.

Technology Details

The following technical explanation summarizes an extensive research and development bibliography [1-17]. Brainlike kernel technology adapts to changing conditions automatically and continuously. Monitoring systems based on the technology produce alarms only when observed sensor levels differ significantly from their expected values. Expected values are updated continuously in order to reflect changing conditions. By adjusting expected values continuously, the technology reduces false alarms and reduces information to its monitoring essence. It also operates automatically, removing the need for re-tuning.

Resulting precision improvements and cost reductions have prompted significant venture funding for commercial development of software products that monitor computer servers. These products, which are currently satisfying corporate server farm customers, receive multiple performance indicators arriving in arrays containing up to several hundred values at each arrival time. Arrival times for each array may be separated by a few seconds or less.

Along with its proven advantages when implemented as software, the technology offers larger — thus far unexploited — advantages when implemented as hardware [1-2]. Kernel technology is based on an algorithm that is compact, separable, fast, and designed for on-chip implementation [3-4]. When implemented in hardware, the kernel algorithm can receive multiple sensor outputs arriving as arrays, just as in software. However, hardware arrival times for each array can be only a few microseconds or less.

When implemented in either software or hardware, the kernel algorithm performs three basic operations between each sensor array arrival time. First, it computes expected sensor array values. Second, it determines if the sensors' expected values differ significantly from their actual values, and produces alarm signals accordingly. Third, and most important, the kernel algorithm updates its learned parameters efficiently.

<u>Efficient, real-time learning operation distinguishes Brainlike technology from all alternatives. Learning is most important because it allows monitoring and control systems to operate more effectively by adapting to changing conditions. Efficient learning is especially important for data reduction at the micro-electronic level, because it can be implemented on a chip for fast, compact, and rugged operation. Data reduction at the micro-electronic level is critically important because sensor array transmission capacity is often limited and inter-chip transmission capacity is extremely limited.</u>

Learning is also important for control at the micro-electronic level, because it can be tailored to suit numerical optimization. When implemented in this way, the kernel algorithm can identify optimal parameter values far faster than conventional methods. Related applications include electronic antenna and sensor array pointing, among many others inside and outside the shallow water intrusion detection domain.

Brainlike enabling technology resembles regression analysis in that it computes the expected value of each monitored variable as a function of all other current values of other monitored variables. It resembles auto-regressive, moving average analysis in that it also uses recent values to compute expected values. It also resembles empirical Bayes methods in that it updates learned parameters by combining current information with prior information at each time point. It resembles Davidon-Fletcher Powell numerical optimization as well, in that it operates efficiently on the inverse of correlation matrices instead of requiring conventional matrix inversion. The technology combines these features to produce a robust, efficient, and fully automated monitoring process.

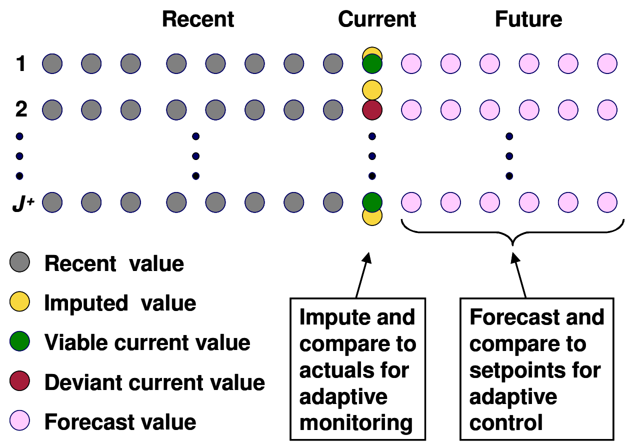

Figure 2. Data Layout

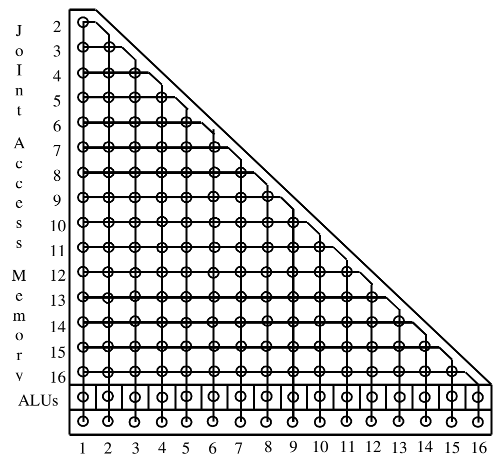

Figure 3. Chip Layout

As shown in Figure 2, at each array arrival time point the kernel receives a column of input values and imputes each current value as if it were missing. Imputed values are used to replace input values when they are missing or deviant. In addition, each imputed value is compared to its corresponding actual value to determine its deviance value, which is supplied by the kernel for monitoring purposes. Along with individual deviance values, the kernel supplies a global deviance value, which combines all input deviance values into a single number.

As also shown in Figure 2, at each time point and for each input, multiple kernels may compute one or more forecast values, which may be used for control and other purposes.

When used in this way, kernels can add monitoring value by increasing estimation precision in two distinct ways. First, each imputed value for each input is computed not merely as a function of recent values for that input only, as in typical time series applications. Instead, it is computed as a function of recent values for all inputs as well as current values for all other inputs. Second, and more important, at each time point the kernel continuously and automatically updates learned estimation model parameters including means, correlations, regression weights, and deviance metrics.

Kernel operation is fast and compact. When implemented in software, any given kernel can receive 100 inputs, produce estimates, and update learned parameters in less than 100 milliseconds, and over 5,000 kernel models can reside on a conventional server. When implemented on chips, kernels will operate orders of magnitude more quickly and reside in orders of magnitude less space.

The enabling technology has been developed to solve a variety of technical problems by performing certain technical correction functions automatically, without which auto-adaptive operations could not be sustained. Some functions correct for developing linear redundancies and related numerical problems. Others automatically identify and replace deviant and missing values. Others automatically reduce recent input values to smooth trend features that will not produce estimation excursions.

As part of successful efforts to develop the enabling technology into software products, a broad variety of such problems have already been solved. In the process, a scalable platform for hardware development, simulation, and testing has evolved as well. While other problems will emerge as part of developing operational hardware, extensive software development experience to date on essentially the same algorithms offers a distinct advantage.

Figure 3 shows a kernel chip layout [2]. Only 16 inputs are shown for clarity, but a kernel with several hundred inputs can reside on a single chip. Digital versions of the chip shown in Figure 1 can perform kernel operations much more quickly than its software counterpart, because each a distinct processor is dedicated to each input [3].

Analog chips corresponding to Figure 3 can perform kernel operations even more quickly by dedicating a separate analog component to each arithmetic operation [17].

Figure 4 shows how a kernel might be used to impute missing values and/or identify unexpected activity at one spatial node within a sensor array. Figure 4 shows how an array of Brainlike kernels might be used simultaneously to carry out the same operations for each node within the array. The practical implications of Figure 5 for meeting future defense needs, given kernel speed and compactness, are substantial.

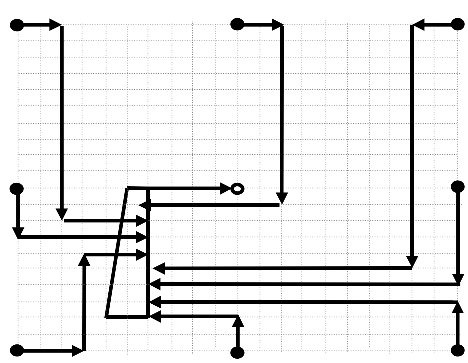

Figure 4. Spatial Imputing Layout

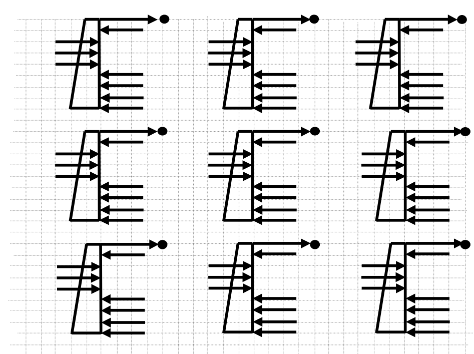

Figure 5. Distributed Spatial Processing

References

1. R.J. Jannarone, *Concurrent Learning and Information Processing: A Neuro-computing System that Learns* during *Monitoring, Forecasting, and Control.* Chapman & Hall, New York, 1997.
2. R.J. Jannarone, *Concurrent Learning and Performance Information Processing System*, U.S. patent #5,835,902, 1998.
3. K. Naik, *A Concurrent Information Processing Parallel Design Analysis*, Unpublished Masters Thesis, University of South Carolina, 1996.
4. R.J. Jannarone, “Conjunctive Item Response Theory Kernels,” *Psychometrika*, Vol. 51, pp. 449-460, 1986.

5. R.J. Jannarone, “Locally dependent models: conjunctive item response theory,” In W.J. van der Linden & R.K. Hambleton III (Eds.), *Handbook of Modern Item Response Theory*, Springer-Verlag, New York, pp. 465-480, 1996.
6. R.J. Jannarone, K.F. Yu, and J.E. Laughlin, “Easy Bayes Estimation for Rasch Type Models, ” *Psychometrika*, Vol. 55, pp. 449-460, 1990.
7. R.J. Jannarone, K.F. Yu, and Y. Takefuji, “Conjunctoids: Statistical Learning Modules for Binary Events,” *Neural Networks*, Vol. 1, pp. 325-337, 1988.
8. R.J. Jannarone, “Concurrent Information Processing, I: An Applications Overview,” *Applied Computing Review,* Vol. I, pp. 1-6, 1993.
9. G.E. Weeks, W.E. Daniel, R.E. Edwards, Jr., S.N. Palakodety, S.S. Joshi, D. Qian, & R.J. Jannarone, "Holledge Gauge Failure Testing using Concurrent Information Processing Algorithm," *Proceedings of the International Topic Meeting on Nuclear and Hazardous Waste Management*, American Nuclear Society, Inc., La Grange Park, IL, Vol. 1, 1998.
10. K. Ma, *Statistical Neural Network Models: Theory and Implementation for Visual Pattern Recognition*, Unpublished Doctoral Dissertation, University of South Carolina, 1991.
11. S.N. Joshi, *A General-Purpose Concurrent Information Processing Prototype*, Unpublished Masters Thesis, University of South Carolina, 1994.
12. S.S. Palakodety, *A Special-Purpose Concurrent Information Processing System*, Unpublished Masters Thesis, University of South Carolina, 1994.
13. Y. Hu, “Automated Real-Time Neural Computing for Defense Waste Processing,” *Proceedings of the International Topic Meeting on Nuclear and Hazardous Waste Management*, American Nuclear Society, Inc., La Grange Park, IL, Vol. 1, pp. 534-540, 1992.
14. R.J. Jannarone*, Multi-Kernel Neural Network Concurrent Learning, Monitoring, and Forecasting System*, U.S. patent #6,216,119, 2001.
15. R.J. Jannarone, *Concurrent Learning and Performance Information Processing System*, U.S. patent #6,289,330, 2001.
16. J. Voorhees. “The Limits on Wireless Security: 802:11 in early 2002,” SANS Institute (http://rr.sans.org/wireless/limits.php), January 30, 2002.
17. E. Amorso, *Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response.* Intrusion.Net Books, 1999.