

Automated Learning for Effective Surveillance: A Strategic Imperative for National Security

Brainlike Surveillance, Inc.

www.Brainlike.com

Copyright© 2004 by Brainlike Surveillance, Inc.

1. The Problem

This paper introduces automated learning as a strategic imperative for national security. In a world of exponentially increasing data, generated under continuously changing circumstances, conventional surveillance methods are not working well. Conventional surveillance methods, which are based on manual data analysis, have the following limitations:

- **Preventable incidents go unnoticed**, they endanger citizens, and they cost money. Preventable incidents include frequent events like border crossing and drug activities, occasional but more costly events like submarine collisions and terrorist bombings, and rare but catastrophic events like the 9/11 tragedy. Conventional methods cannot identify preventable incidents well because they cannot automatically adapt to changing conditions. Hour to hour changes in ticket counter activity that masked significant security delays on the morning of 9/11 offer a prime example [1].
- **False alarm responses take heavy tolls**, including huge equipment deployment and staffing costs. They also distract operators from noticing preventable incidents. Conventional methods produce huge numbers of false alarms, because they cannot automatically shift alarm set points as conditions change. The only way conventional methods can avoid false alarms is to make alarm thresholds so high that damage has been done by the time alarms have been sounded.
- **Conventional data analysis delays preclude preventive actions**, because they produce alarms only after costly incidents have already occurred. The conventional alternative to fixed threshold alarms is manual analysis, which cannot keep up with massive amounts of continuously arriving data. Again, airport check-in data analysis offers a prime example.
- **Conventional surveillance training costs too much money**, trainable personnel are hard to come by, and retaining armies of them depletes limited resources. Staffing surveillance operations centers to sift through even moderate proportions of all available data is out of the question.

Automated learning offers a low cost solution to conventional surveillance problems, along with huge overall savings. All surveillance systems, from the simplest dash board displays to the most complex decision processes, initiate preventive actions when evidence exceeds a threshold. Conventional methods are based on either manual analysis of historical data to establish fixed thresholds, or real-time analysis of raw data by operators, or both. In either case, manual methods cannot keep up with changing circumstances. Conventional alarm thresholds must be set either at very high cutoff levels leaving preventable incidents unnoticed or at very low cutoff levels that generate

frequent false alarms. Either conventional alternative is unaffordable under the differing and changing environmental conditions that usually occur in practice.

Automated learning alternatives continuously adapt alarm thresholds to changing baseline conditions, automatically and in real time. Automated learning solutions are emerging commercially and are common to animals, but novel to surveillance practice. Animals can effectively pinpoint intruders or prey during the day or at night, in fair or foul weather, and under many other changing background conditions. Animals can also automatically adapt their behaviors to ensure their own survival. By contrast, surveillance operators base their operations either on manual data analysis or on historical data analysis methods such as artificial intelligence, artificial neural network, and statistical analysis. Conventional data analysis was adequate when rules of engagement were stationary and leading indicators of developing attacks were manageable. In these days of asymmetric threats and massively available data, however, much can be gained from concurrent learning and information processing (CLIP) methods [2].

2. Impact

CLIP methods offer superior monitoring technology to meet key homeland security needs, including the following:

- Bio-terrorism early warnings. The best response to bio-terrorism will be preventing attacks from reaching epidemic proportions, which in turn will require detecting unusual disease patterns at once. Delivering early warnings will require automated computer networks that will deliver comprehensive disease incidence data to central locations in real time. Converting incidence data to *valid* early warnings will also require CLIP methods to separate true disease outbreak leading indicators from the many false indications that could be misinterpreted as such [3].
- Unexpected airport activity. Suppose that several unexpected activity indicators were recorded and supplied to an airport security operations center every few minutes. Such recordings might include the average time spent inspecting each piece of luggage and the average time spent screening each passenger at the ticket counter — the kind of information that could have pointed toward terrorist activity at Logan Airport on the morning of 9/11. Then subtle signs of unusual activity could be detectable using CLIP methods and preventive action could be initiated accordingly. On the morning of 9/11, nine hijackers were briefly detained and screened as potential threats at the Logan Airport ticket counter. Could CLIP methods have shown that nine strange things were happening at once and prompted immediate preventive action? Perhaps [1].
- Unexpected traffic activity. Suppose that a variety of surface, sub-surface, and airborne sensors were supplying correlated activity information to a traffic monitoring center. In that case, CLIP methods might detect subtle changes that would otherwise be undetectable, so that preventive action against terrorist threats could be initiated accordingly [4].

- Unexpected computer network activity. Products using CLIP methods have already been delivered that identify subtle computer problems under dynamic operating conditions [5].
- Unexpected power consumption. Suppose that CIA reports uncovered a terrorist plot to launch a laser-based attack on a passenger jet landing at a U.S. airport. Anti-terrorism units might then be able to pinpoint and neutralize the attack if they could quickly recognize unexpected increases of energy usage in the region. In closely related incident monitoring settings, CLIP methods have been shown to add substantial precision and lead time value [6].
- Reduced anti-terrorism operating costs. Regional, state, and national governments are acutely aware that anti-terrorism operating costs can be enormous. Key to cutting such costs is reducing false alarms. False alarm response costs can be so large that officials may be forced to ignore alarms entirely. Los Angeles County electronic break-in alarms is a recent case in point. High costs also result from major time and effort associated with delivering effective monitoring systems. The kind of effort needed to anticipate all possible attack contingencies is simply out of the question, because some of them haven't even yet been imagined. CLIP monitoring offers huge cuts in total operating costs along both false alarm and product cost reduction lines, by continuously learning what to expect [7].
- Tragedy prevention. CLIP methods offer huge value by identifying developing problems immediately so that action can be taken to prevent costly incidents of tragic proportions[7].

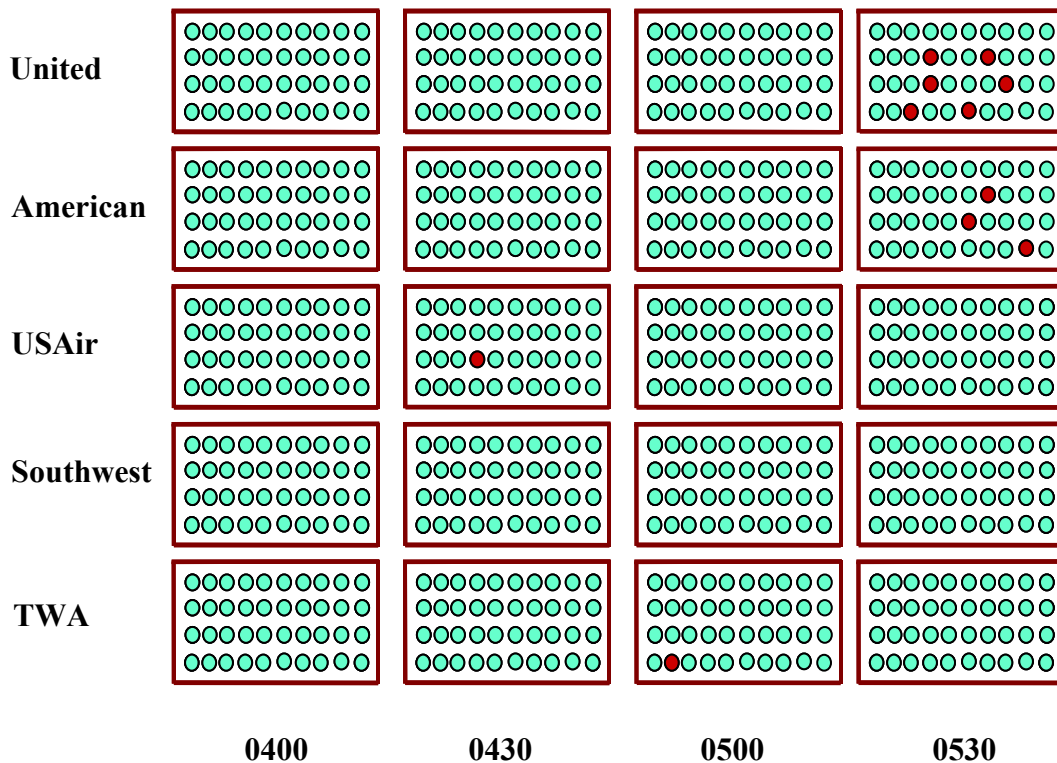


Figure 1. Ticket Counter Activity Monitoring

Figure 1 shows a ticket counter monitoring display panel that suggests an intriguing possibility: if this panel had been installed and integrated with CLIP monitoring technology on the morning of 9/11, the tragedy might have been prevented. Each light in the display panel represents activity at a particular ticket counter during a 30 minute period. If passengers were being processed at that ticket counter in an unusually careful way, a red light would be displayed. The pattern of red lights in Figure 1 has been created to show the kind of ticket counter activity that reportedly took place prior to the 9/11 hijackings. In particular, nine of the 9/11 terrorists were retained for an unusually long time at ticket counters during check-in, as indicated in the figure by 0530 red lights at United and American airline ticket counters. If this display had been available at a Logan Airport surveillance operation center (SOC), the 9/11 tragedy may not have gotten off the ground [1].

While this section has outlined the relevance of CLIP for HLS, its real strength comes from years of prior effort that have produced a broad body of successful case studies [2], along with working commercial products [5]. The potential for positive impact on defense and homeland security, both near-term and long-term, is huge.

3. Concurrent Learning and Information Processing Technology

CLIP methods uniquely identify sharp changes as anomalies, even if they occur as low level leading indicators in a sea of changing background activity. By contrast, conventional monitoring alternatives either produce far more false alarms, or they identify fewer anomalies before they become costly incidents, or both. The distinction between CLIP and conventional monitoring is illustrated in Figure 2 and Figure 3. The wavy black plot in Figure 2 shows how typical observed values, plotted on the vertical axis, vary over the horizontal axis time line. For example, the plot could represent ticket counter activity as it changes over time.

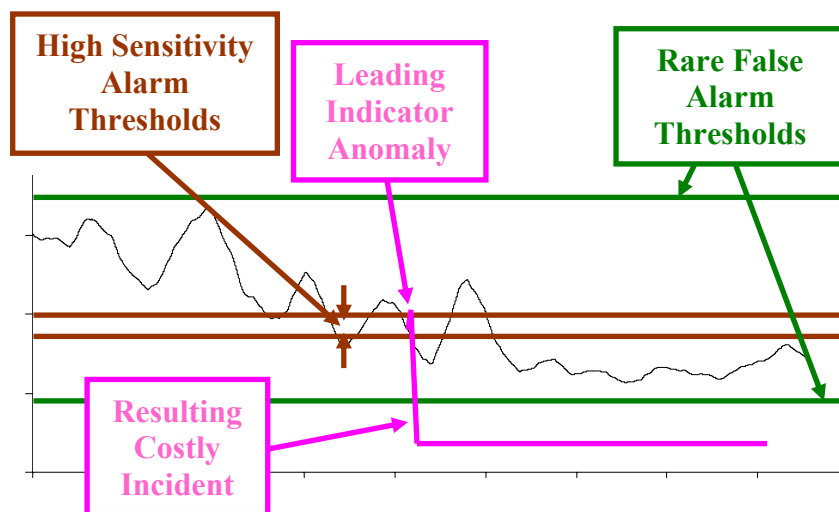


Figure 2. Changing Data with Fixed Alarm Thresholds

Anomaly alarms are produced when input values exceed alarm thresholds. Conventional alarm thresholds are fixed over time, as shown by the green pair of lines and the brown pair of lines in Figure 2. If the wide, green pair of thresholds were used for anomaly detection, an alarm would be generated whenever input values were either above the top green value or below the bottom green value. Likewise, for the narrow brown pair of thresholds, an alarm would be generated whenever input values were above the top one or below the bottom one.

Using fixed alarm thresholds to monitor changing data poses a basic problem. If the thresholds are set too far apart, such as the green pair of thresholds in Figure 2, then leading indicators of problems such as the brief upward spike in Figure 2 will not generate alarms before the problem turns into a costly incident, as shown by the steep downward spike. If, on the other hand, the thresholds are set too close to each other, such as the brown pair of thresholds in the figure, then the brief upward spike would generate an alarm. However, because so many other values fall outside the narrow brown tolerance band, many false alarms would occur as well — so many that either responding to each would be costly or ignoring them entirely would become routine. Thus, no matter how thresholds are fixed at constant values, costs of responding to false alarms, coupled with prices of costly incidents, can be prohibitive.

Figure 3 shows light green alarm thresholds produced by a currently available CLIP method [8]. As the figure shows, CLIP alarm thresholds track smooth input value changes very closely, so closely that sharp changes appear as anomalies immediately without generating a large number of false alarms.

Notably, the CLIP approach identifies anomalies without expensive and time consuming prior analysis of historical data. Moreover, it requires no prior analysis to determine how the software should be configured.

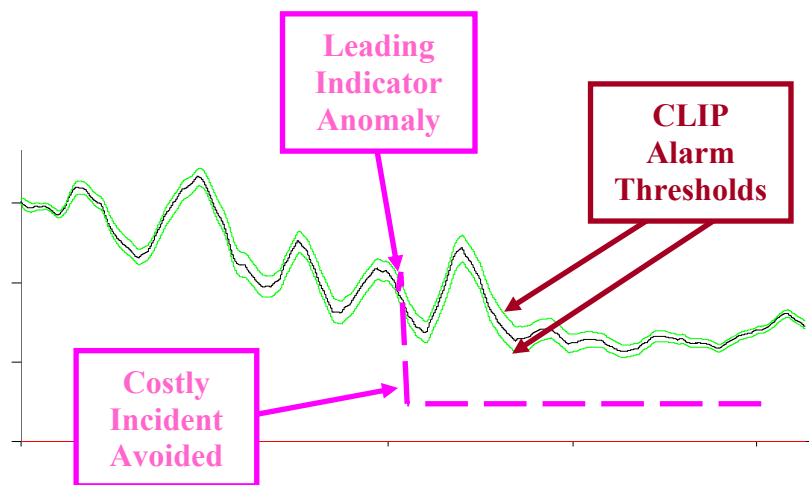


Figure 3. Volatile Data with CLIP Alarm Thresholds

4. A Key Issue

Concurrent learning and information processing has progressed to the point where automated learning tools are now available, and they have already shown substantial added value commercial monitoring applications. The key remaining issue is how to expedite their rapid insertion into the defense and homeland security surveillance arena. The quickest way to resolve this issue is to demonstrate huge added value in a variety of operational surveillance settings — the sooner the better. To set up a demonstration, contact Brainlike Surveillance, Inc., at 619-299-5139.

References

1. [Brainlike Homeland Security Relevance.](#)
2. [Concurrent Learning and Information Processing Reference List.](#)
3. [Brainlike Anti-Bio-terrorism Relevance.](#)
4. [Brainlike Shallow Water Intrusion Detection.](#)
5. [www.Netuitive.com.](http://www.Netuitive.com)
6. [Brainlike Monitoring Improvement Illustration.](#)
7. [Brainlike Return on Investment Analysis.](#)
8. [Brainlike Product Overview.](#)

Brainlike Surveillance, Inc.
3911 Pacific Highway, Suite 213
San Diego, CA 92110
619-299-5139
www.Brainlike.com