JOURNAL OF AEROSPACE COMPUTING, INFORMATION, AND COMMUNICATION
Vol. 7, June 2010

Preemptive Response to Missile Threat Using Intelligent Video

Peter Leed*
BSEC Planning Corp, Andover, Massachusetts

Alan Fulton and Kamal Raychaudhuri
EMW, Inc., Herndon, Virginia

and

Adrian Esquivel
TechPerk, Miami, Florida

DOI: 10.2514/1.38044

Recent advances in computer vision have brought along new revolutionary changes in applications and products within the growing industry of security technologies. This technology introduces video detection capabilities, which have been envisioned in laboratories, to the realm of real-world physical security deployments. At the same time, video analysis—or as it is commonly known, "intelligent video"—is being introduced as an affordable, practical, and effective security layer in any physical protection system. In this paper, we review briefly how motion detection works, how it is applied to threat detection and prevention, and its integration with information technology to produce a sophisticated intelligent video system. We discuss an application of the technology, focusing on a specific proposal to combat the modern scourge of missile threat to civil aviation. Intelligent video systems integrated with high-value video surveillance equipment and computer-aided dispatch servers are proposed as a methodology to detect and dispatch effective pre-emptive responses to the threats of shoulder-fired missiles directed against commercial airlines operating out of airports in densely populated areas.

I. Introduction

THREATS from shoulder-fired missiles (SFMs), more formally called man-portable air defense systems, directed against commercial airlines operating out of airports in densely populated areas are a very real problem. The threat is widely referred to as the aviation industry's "dirty little secret." Paul J. Caffera reported back in November 2002 that, as of August 2002, a Pentagon spokesman said U.S. forces in Afghanistan had captured 5,592 SFM during operations to destroy al Qaeda bases there [1].

According to a recent article in "The Globe and Mail"

> Passengers aboard Israeli jetliners will be the first to gain protection against the small, portable surface-to-air missile, which security experts fear will become the weapon of choice for terrorists targeting civilian aircraft. The El Al airline announced this week that it will equip its jets with anti-missile detection systems and flares designed to lure heat-seeking warheads away

Received 12 April 2008; accepted for publication 7 May 2009. Copyright © 2010 by Peter Leed, Alan Fulton, Kamal Raychaudhuri and Adrian Esquivel. Published by the American Institute of Aeronautics and Astronautics, Inc., with permission. Copies of this paper may be made for personal or internal use, on condition that the copier pay the $10.00 per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923; include the code 1542-9423/10 $10.00 in correspondence with the CCC.

* BSEC Planning Corporation, 35, New England Business Center, Andover, MA 01810, USA, peter.leed@comcast.net

> from their targets. It is the first airline to announce plans for anti-missile measures despite mounting fears that the small, inexpensive shoulder-fired weapons—easily hidden in a vehicle—will be used to shoot down airliners as they land or just after they take off. The Israeli system—a modified version of the protection many military aircraft employ—is expected to cost more than $1 million per plane, even if it goes into large-scale production [2].

The reported cost to retrofit most common commercial jets with the most effective system is approximately $3 million. Even these systems may not be enough as currently produced SFM are programmed to evade existing countermeasures applied against them [3].

According to another report published 12 December 2005, an American Airlines 767 outfitted with BAE's JetEye system flew from Forth Worth, while Grumman's Guardian system was tested on an MD-11 that took off from the Mojave airport in California. Both systems use lasers to jam the guidance systems of incoming missiles. Government contracts call for systems that cost under $1 million each, are easier to maintain, and more reliable than current military versions. Congress is pushing the program, but airlines, concerned about cost and maintenance issues, are less enthusiastic. "It's a huge expenditure of resources to deal with one type of threat," says John Meanen, executive vice president for the Air Transport Association. Some estimates of the cost are given as $10 Billion and more [4].

The threat posed by the SFM to commercial aviation is a complex and technically challenging problem. Shoulder-fired missiles are lightweight (35 pounds), are easily set up, and they reach their operating speed of Mach 2 within seconds. Traveling at 25 miles per minute, an SFM can reach an airplane 4 miles away in less than 10 s. These and other reports point to the very real threat of SFM to commercial aviation and the extraordinary costs to detect and respond to the threat [5,6].

In the rest of the paper, we provide a brief review of an intelligent video system (IVS) and discuss our proposal to integrate an IVS with computer-aided dispatch (CAD) servers as a methodology to detect and dispatch effective pre-emptive responses to the threats of SFM directed against commercial airlines operating out of airports in densely populated areas.

II. Intelligent Video Surveillance

Traditional video surveillance systems, from small to large, incorporate an infrastructure where the video is centrally monitored and recorded. In this scenario, security personnel are responsible for watching multiple video feeds and interpret threats as they present themselves in real time. However well trained or dedicated these employees are, it is impossible to expect persistent concentrated attention to a video feed, not to mention to two or more. After just 20 min, human attention to video monitors degenerates to an unacceptable level. Providing an effective method to automate the viewing of the video and detecting threats in order to provide a reactive tool is the desired solution to any video surveillance system. IVSs allow the operator to define the surveillance area, support consolidated "watches" of multiple video feeds, and enable the classification of objects detected in the field of view. An IVS generates real-time alerts when objects selected begin to behave as potential threats.

Examples of the types of behavior detectable include: a person appearing in a secure area after hours, a vehicle loitering outside a perimeter fence line, an unidentified object left behind on a railroad track, or a boat entering a secure waterway. When a pre-defined rule is violated, the IVS sends alerts to security personnel, which assure real-time notification. IVSs support object classification, which enables operators to classify a threat as a person, small boat, large van, or suspicious bag. Accurate threat detection using an IVS increases the time available for security personnel to evoke the necessary protocols to respond and counter threats in real time.

Over the past 10 years, video motion detection (VMD) has been the only technological solution commercially available to enhance traditional video monitoring systems. The obvious shortcomings of VMD include high false and nuisance alarm rate (FAR/NAR) and the relative ineffectiveness of motion detection in outdoor environments mainly due to naturally occurring phenomena (e.g., waves in water, leaves, blowing sand). Another, and most often noted, shortcoming of VMD is its inability to detect the behavior of objects as they interact in a video scene [7,8].

III. How VMD Works

Video motion detection works by analyzing the video stream for pixel changes in consecutive frames. Fundamentally, VMD technology is simple technology that generates alarms based on discontinuous pixel changes in video frames. When the number of pixel changes exceeds a specified threshold, the VMD system generates an alarm. IVSs use a content analysis algorithm which classifies and analyzes a scene's content and uses an inference engine to detect, track, and classify objects [7]. This allows the IVS to distinguish between threatening vs non-threatening behavior in a video scene. For example, transient motion of objects like tree branches and leaves, waves in water, or flying birds do not generate false alarms in an IVS. Content analysis determines the likely behavior of objects like a person, a vehicle, a bag, or an unknown object. This method permits the system to prioritize and monitor these objects in a video scene. The IVS inference engine component analyzes the video scene's content and determines if an alarm event has occurred based on object behavior such as:

1) If a person crosses over a line in a certain direction.
2) A vehicle stays in a certain area for a pre-defined period of time.
3) An object is inserted into an area.
4) If a large vehicle moves too fast down a road.
5) A person enters an area after a certain time.

A well-implemented video content analysis algorithm combined with a high-performance inference engine is the core of a successful intelligent video solution.

IV. Application to SFM Threat

We propose a methodology to detect and reduce the threat of SFM. The approach described here is based on the nature of the urban areas surrounding commercial airports with high traffic density. Many of the busiest commercial airports are located in densely populated urban areas. Unlike airports in less populated areas, the density of buildings and population tend to limit the areas where an SFM can be operated effectively and still provide the SFM operator a reasonable escape route. Even though an SFM is easy to transport and operate, an operator must have a clear line of sight (LOS) and adequate time, measured in minutes not seconds, to set up and deploy the weapon. It is these aspects of weapon use which offer an opportunity to counter the threat.

For urban airports many of the standard approach paths cross over apartment buildings which would make excellent launch areas for SFM. The rooftops of most urban industrial buildings are often protected by integrated security systems and are often are lower than the average and so would not have as good an LOS as the typical apartment complex rooftop. The rooftops of apartment complexes are in many ways excellent locations for deploying and launching an SFM. Aside from the clear LOS, the normally vacant rooftops of these buildings afford the operator of the SFM the time to deploy, excellent cover, and an effective escape route. There is often direct access to the roof from common hallways. Additionally, adjacent rooftops often are connected and rooftop surveillance of any kind usually is non-existent. For these reasons, perhaps the only place where an SFM can be deployed in an urban area is from such rooftops; and yet in urban areas, the large number of apartment buildings would seem to make an SFM countermeasure methodology based on video surveillance impractical. However, it is the sparseness of the rooftop environment which makes our proposed methodology reasonable.

Note, in Fig. 1, the area north of JFK International Airport, with the relative small area of suitable rooftops compared to that of the ground level areas. One can easily imagine that the ground level areas would be far riskier for SFM operators than the normally vacant rooftop areas. Many of these areas are residential and so it is reasonable to expect there will be too many people present for these areas to be viable for SFM operations. Most of the ground level areas are visible from wide angles, have obstructed views of airport glide paths, or for other obvious reasons are clearly unsuitable for SFM operations. Additionally, many open areas are probably covered at least partially by existing anti-crime and various facility video surveillance systems.

A rough comparison of the heavily industrial and commercial area north of Newark International Airport, shown in Fig. 2, with that shown in Fig. 1 reveals what would appear to be a different situation. In the Newark Airport area there appear to be more rooftop areas than in the selected area north of JFK. However, the rooftops north of Newark Airport are primarily commercial. It is highly likely these will be securely monitored and thus will unsuitable as potential SFM launch sites. Also heavy commercial daytime traffic of people and vehicles probably greatly reduces the probability of the ground level areas in Fig. 2 being viable choices for SFM operations. As in the Fig. 1 areas, most of all the ground level areas in Fig. 2 are also visible from wide angles, have obstructed views of airport glide paths, or are clearly unsuitable for SFM operations. Additionally, many areas are even more likely to be covered by existing facility video surveillance systems.

Video surveillance using traditional CCTV systems are well known and widely deployed. Typically, security personnel are integrated into the system and are responsible for adding the intelligence required to monitor and

Fig. 1 Area north of JFK International Airport. (Image from 2006 Europa Technologies from Google Earth).

interpret incoming video data. Even in small systems, the attention span of the security personnel degrades to unacceptable levels in a relatively short time. In larger systems, the problem is more severe and chronic. Even with the addition of VMD technology, the problem continues.

The most obvious shortcomings of VMD include a high FAR/NAR and the ineffectiveness in outdoor environments. Naturally occurring phenomena such as waves in water, wind blowing across tree branches, leaves, and sand, animals, and wind-caused motion of fences are large and difficult-to-handle contributors to the FAR/NAR. There is also no way to detect the interaction of objects in a video scene. Video motion detection cannot answer the question if a person picked up or moved an object.

In low threat activity environments, the typical commercial video surveillance system designed for proactive surveillance is really a reactive video recording system. To combat the problem, various technology-based strategies are available.

One such strategy is the IVS. An IVS uses content analysis and a powerful inference engine to detect, track, and classify objects while analyzing their behavior for threatening behavior in a given video scene. Boundary lines, duration times, and insertions can be detected, tracked, and accurately alarmed. Effective integrations of IVS systems to IP-based CAD systems have been accomplished and are available commercially [9,10]. The available systems can detect the threat and dispatch in real time effective countermeasures.

Applying an IVS and CAD to counter the SFM in urban airports requires one other technology. High-value long-range (HVLR) video cameras are the missing piece. Programmed to scan the rooftops of high-probability launch SFM sites, HVLR video surveillance data combined with an IVS can effectively scan the normally vacant rooftops. The centrally located, rotating HVLR asset could be used to sweep the rooftops miles away from the airport. This would enable a virtual perimeter to be set up which could be scanned several times a minute.

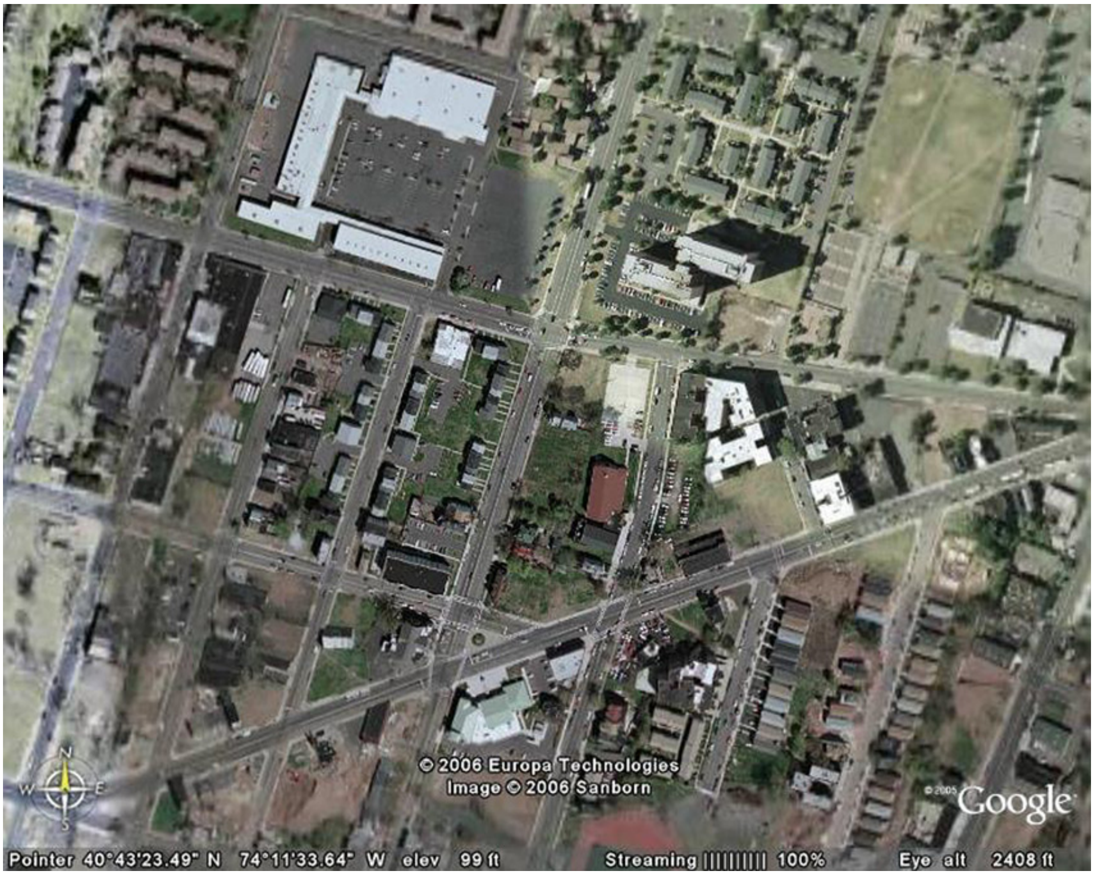

Fig. 2 Area north of Newark International Airport. (Image from 2006 Europa Technologies from Google Earth).

Figure 3 is representative of the available long-range Video Surveillance Camera commercially available [11,12]. According to published specifications, the device can recognize a known face at up to 2.4 km and detect human activity up to 12 km. This makes the device suitable for monitoring areas within the expected threat area for SFMs. More sophisticated multi-spectrum cameras such as the one shown in Fig. 4 are available.

The precise positioning of the equipment and wireless networking equipment can be done by using GIS modeling and simulation techniques. One such system is BSEC Planning Corp.'s SecurSoft Planning System. SecurSoft is widely used to plan complex border and other large-area integrated security and surveillance systems. The system uses precise terrain data and LOS-based equipment algorithms to optimize surveillance and wireless communication equipment layouts. Furthermore, EMW of Herndon, Virginia finds that it is possible to significantly reduce design costs and implementation schedules in security systems using SecurSoft.

Recent work reported by Carrano et al. of Lawrence Livermore National Laboratory entitled "Enhanced Video Surveillance (EVS) with Speckle Imaging" indicates that the technology for enhancing images from a long distance video camera is viable [13]. High-threat areas could be evaluated using satellite image analysis and selected site surveys of an airport's perimeter areas.

In addition, rooftop door sensors with radio frequency transmitters could be deployed selectively on the access doors of high-risk rooftops. The sensor's alarm signal would cue up a camera for immediate high-resolution imaging and evaluation by security personnel. Combined with digital framing of the images and algorithmic analysis of time of day shadows and weather conditions to lower false alarms, the system response to the possible SFM operations would be swift and accurate. The objective is to eliminate areas of low probability of potential SFM operations from routine surveillance.

Fig. 3 Typical long-range Video Surveillance Camera—Falcon LRS 2000 Image from Falcon Systems.

Fig. 4 Multi-spectrum long-range Video Surveillance Camera—Falcon LRS 3000 Image from Falcon Systems.

The seemingly complex video scene environment of the rooftops would be simplified by the IVS content analysis. With the bulk of the complexity of the rooftop video removed, the IVS inference engine will be directed to concentrate on the remaining and relatively sparse data of the video image of a potential SFM operator.

IVS-generated alarms could be rapidly and accurately evaluated by security personnel, and direct integration of the CAD system would enable a timely dispatch of law enforcement to disrupt and possibly capture the SFM operator. Also, the existence of an effective long-range video surveillance system might serve as a cost-effective deterrent.

Figure 5 is the system diagram of our proposed LRVISR_CAD system. Here one can see the net centric approach to system deployment and the close integration of the essential components. Field deployed door sensors and cameras,

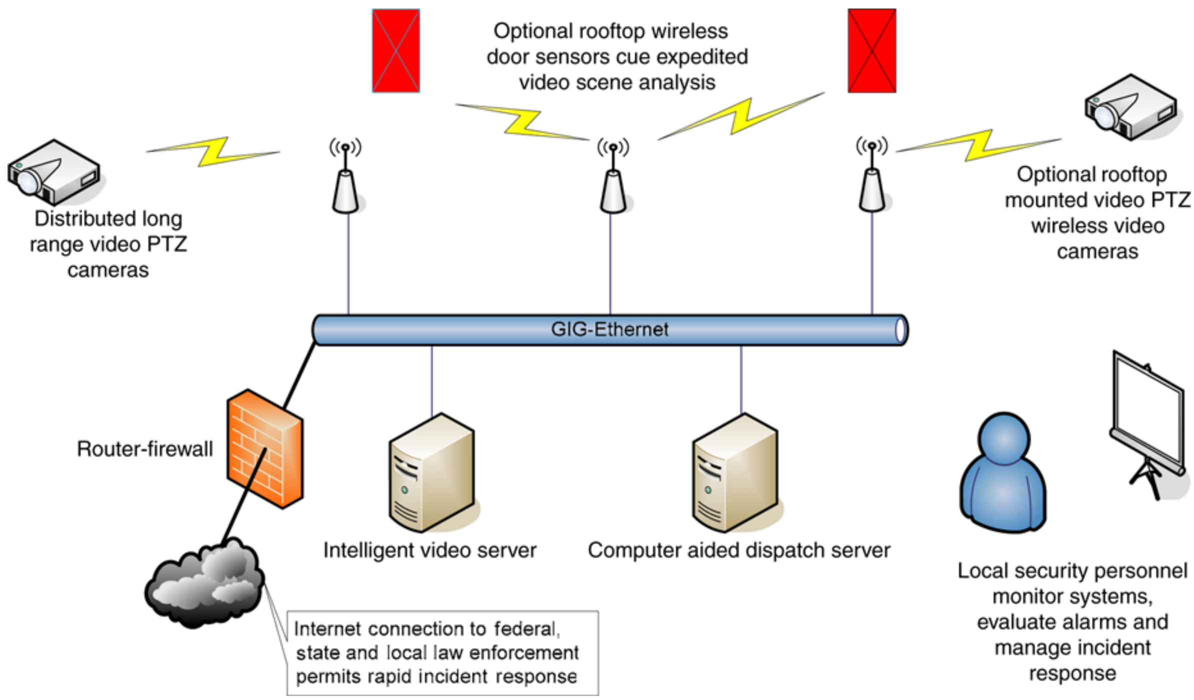

Fig. 5 LRV-IVS-CAD system diagram.

both long range and short range as required, are connected as wireless IP clients to the IVS and CAD servers. Video and control signal encryption and frequency-hopping technologies would be used to prevent signal interception and jamming.

The critical security functions of alarm analysis and crisis management would be under the full control of security personnel. There would be established links to external law enforcement and military resources as needed. It is anticipated that local law enforcement resources would be GPS enabled and fully interoperable with the LRV-IVS_CAD system.

This would allow real-time video feeds from the long range video (LRV) to be displayed on first-responder laptops. Also, the actual status of the deployed first responder would be visible to the system security personnel. System interoperability combined with a well-designed, effectively tested, and expertly administered security policy offers the best opportunity of countering a serious SFM threat.

All of the components required to do effective long distance rooftop surveillance are available and the overall solution is technically feasible. Eliminating low-probability areas of SFM operations would allow resources to be concentrated on high-probability areas. The goal of selective surveillance is to raise the risk to SFM operators and in effect deny them suitable launch sites. This should substantially lower the risk of SFM terrorism to the aviation industry and the traveling public at a cost-effective price.

V. Conclusion

Intelligent video presents a highly effective, preventive detection solution for any physical security system. The grave threat that SFM pose to commercial aviation in urban areas can be countered by intelligent threat analysis and the effective deployment of an IVS using long-range video surveillance and CAD of law enforcement responses. By concentrating on preventing SFM setup operations from taking place, LVR-IVS-CAD systems can shift the response time in favor of the security forces. It is also thought that the deployment of LVR-IVS-CAD systems will be an effective deterrent to SFM operators by denying them the most suitable areas for operation.

References

[1] Cattera, P. J., "Hand Held Terror," *Washington Post*, 5 Nov. 2002.
[2] Koring, P., "El Al to fit jets with anti-missile equipment," *The Globe and Mail*, http://www.globeandmail.com [retrieved 23 April 2004]. Additional commentary provided by Keithly, Beth, "Airport Security Issues"—*Friday FYI*, Vol. 4, No. 13, http://www.utdallas.edu/research/friday_fyi/040422/security.htm [retrieved 23 April 2004].
[3] Gould, S. C., and Schroeder, M., "Issue Brief #1—MANPADS Proliferation," *The Federation of American Scientists,* http://fas.org/asmp/campaigns/MANPADS/MANPADS.html [retrieved 13 June 2004].
[4] John Meanen quoted by Ben Frankel, "AirborneMissile Defense for Commercial Airlines Move up Security Agenda," *Homeland Security Daily Wire-Business Report,* Vol. 1, No. 93. Online edition [retrieved 14 Nov. 2005].
[5] Report of the Standing Senate Committee on National Security and Defense, "The Myth of Security of Canada's Airports," *Presented to the 2nd Session 37th Parliament*, Jan. 2003, Ottawa, Canada. Available online.
[6] Raytheon Corporation, Missile Systems Division "Vigilant Eagle Airport Protection System Ground Based Counter MANPADS Protection for Large Airports and Air Bases," Product Brochure and Specification Number RMS 4K 60259R, April 2006.
[7] Esquivel, A., "Threat Detection Using Intelligent Video," Phoenix IVS, Miami, FL, TP PIVS 1024 Published 19 April 2006, http://www.phoenixIVS.com
[8] Hampapur, A., et al., "Smart Surveillance: Application, Technologies, and Applications," *IBM T. J. Watson Research Center*, Hawthorne, NY, http://www.research.ibm.com/peoplevision/PCM03.PDF
[9] Motorola Corporation, "Motorola Computer Aided Dispatch Software," *Fact Sheet DJS-MCAD-2 Published 2005*. Other online brochures detail case studies.
[10] Intergraph Corporation, "Intergraph's Computer-Aided Dispatch (I/CAD) System," product specifications, http://www.intergraph.com/icad. Other online brochures detail case studies.
[11] Falcon Protec Corporation, "Long Range Surveillance," Falcon product specifications, provided by Mr. Mike Illingworth, 2006, Falcon Corporation, Tewksbury, Glos, UK, http://www.falcon-protec.com
[12] Falcon Protec Corporation, "Outlined Proposal for Long Run Surveillance System," Falcon Commercial in Confidence document, provided 2006 by Mr. Mike Illingworth, Falcon Corporation, Tewksbury, Glos, UK.
[13] Carrano, C., Brase, J., Poland, D., Olivier, S., and Silva, D., "Enhanced Video Surveillance (EVS) with Speckle Imaging," Lawrence Livermore National Lab., Rept. UCRL-TR-202256, 1 March 2004.

Gerard Parr
Associate Editor