CONF-950787--58
SAND95-1329C

A Survey of Early Warning Technologies

G. Dan Smith
US Department of Energy
Washington, DC

H. Duane Arlowe
Sandia National Laboratories
Albuquerque, NM 87185-0765
505-844-3416 hdarlow@sandia.gov

James D. Williams
Sandia National Laboratories
Albuquerque, NM 87185-0765
505-845-8766 jdwilli@sandia.gov

Abstract

This paper presents a survey of technologies useful in providing early warning in physical security systems. Early warning is important in virtually all types of security systems whether they are used for temporary (tactical, portable, or semi-permanent) applications, border warning, fixed-site detection, or standoff surveillance detection.

With the exception of the standoff surveillance detection systems, all systems discussed in this paper usually involve a moving target. The fact that a person(s) to be detected in a standoff surveillance scenario is not moving presents challenging problems and requires different applications of technology. The technologies commonly used to detect moving targets and some suggestions for detection of stationary targets are addressed in this paper.

This work was sponsored by the Office of Special Technology, Naval Explosive Ordnance Disposal Technology Center under DOE/AL proposal number 959 013D and the US Department of Energy under Contract DE-AC04-94AL85000.

Introduction

Some features of physical security systems are highly desirable, but very difficult to achieve. One of these features is "early warning." Early warning, as the name implies, is any method used to alert security personnel that an unauthorized intrusion is about to occur or that the protected site is under surveillance. Intrusions may occur into areas temporarily occupied by personnel or high-value assets, along national borders, or into a fixed site. Fixed sites or public gatherings (e.g., a "VIP" is speaking) can also be under surveillance by persons gathering unauthorized information or who are planning a standoff terrorist attack.

Both similarities and differences exist in the types of systems needed to detect intrusion and surveillance. The major similarity is that the farther away the detection occurs (i.e., the earlier the warning), the harder it is to determine what caused the alarm. Because early detection is often desired on real estate not controlled by the person(s) desiring early warning, a high incidence of

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED
GH

MASTER

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

nuisance alarms is likely. Unless security personnel can distinguish between actual alarms and nuisance alarms, early warning is not truly achieved. The major difference between intrusion detection and surveillance detection is that intruders are usually moving whereas persons conducting surveillance are generally immobile.

Temporary Security Systems

All security systems can be categorized into one of four types. They are:

- Tactical
- Portable
- Semi-permanent
- Fixed

These four types of systems may be grouped in different ways. In the terminology of the US Air Force, the portable and semi-permanent systems are called "relocatable." For this paper, tactical, portable, and semi-permanent are grouped together a temporary category to distinguish them from the fixed sites. These fixed sites are concrete- and cable-intensive and may have guard and camera towers, fixed lighting (possibly both visible and infrared), permanent delay elements, isolation zones with several layers of "protection in depth," well-understood site phenomena which cause nuisance alarms, and a better response capability.[1]

Terrorism and other aspects of world political instability have created a high demand for temporary physical security systems. These systems can be used when vehicles carrying important assets are away from their permanent fixed-site location, around constructions areas, and on portions of a fixed-site physical security system which may be temporarily inoperable. They are also used by the military in situations in which personnel are deployed into remote areas on temporary missions. Systems used in this manner are known as unattended ground sensors (UGSs) and employ breakwire, seismic, magnetic, acoustic, and active and passive infrared sensors. Such sensors are installed in or near the ground and may require a few hours to install.

Other temporary sensors may be carried with the resource requiring protection and can be rapidly deployed in a matter of minutes. A number of different bistatic and monostatic microwave sensors are available for temporary system use. Most of the temporary sensors are battery-powered, and their alarm outputs are transmitted by radio links.

Border Security Systems

Today's global scenario is a dynamic one. While geopolitical changes are essentially redrawing the world map, smugglers, intruders, and other illegal activities are an increasing concern to many countries. As a result, substantial manpower and resources are being allocated to border security. If the border is relatively short and the likely points of intrusions are well known, sophisticated border systems may be a cost-effective solution to provide anti-threat measures and detection capabilities. If the border is long and intrusions could occur at many locations along its length, total electronic coverage may not be practical.

The technologies used are essentially the same as those used for the temporary security systems. If the procedures for dealing with illegal aliens are so lengthy as to saturate the legal system, the only practical solution may be to erect barriers to virtually prevent entry or establishing containment areas that would be very difficult for an intruder to leave if border crossing itself is achieved. [2]

One major problem in protecting borders that are so extensive they preclude continuous human and electronic surveillance and response is that ground-based early warning sensors must be completely covert. Covertness is required to prevent the sensors and surveillance equipment from being bypassed, stolen, or destroyed by intruders. Because borders are often under surveillance by those desiring to illegally cross the borders, covertness can be difficult to achieve. Oftentimes, systems must be installed at night.

Supplying power to the sensors and communicating the alarm information to a data gathering point are also difficult. On large borders power is often supplied by batteries and communication is accomplished by radio frequency transmission. Completely covert systems are difficult to service.

On shorter borders or on selected portions of long borders multi-sensor early warning systems are useful. The systems continuously monitor and surveill for potential intruders. Such systems may consist of early warning sensors such as UGSs, ground surveillance radars, day and night observation devices (which may include image processing and video motion detection and tracking techniques), and mobile patrols. All of these items, including a central command and control center, must be integrated into a complete site security system.

Fixed-Site Security Systems

Conventional intrusion sensors (e.g., microwave, buried-line, fence-disturbance, infrared, and taut-wire) used at site perimeters do not provide adequate early warning notice for potential site intrusion. Optical detectors, software algorithms, computer processors, and all other components of an electro-optical sensor system have recently been improved. Anti-personnel radars and automated thermal imaging and detection systems have been developed [3–11] to provide early warning outside a perimeter intrusion detection and assessment system (PIDAS). Thus far, however, they have not been accepted for broad applications. High cost and nuisance alarm rates contribute to this lack of acceptance. Ironically, the fact that they are continuously being improved also negatively impacts their acceptance: potential customers are always anticipating even better performance of newer versions.

The Defense Nuclear Agency funded a three-phase effort to develop an advanced exterior sensor system to overcome the above problems. In the first phase, an extensive literature search and broad survey of state-of-the-art electro-optic sensors, target detection and tracking algorithms, and computer processing equipment was conducted.[12] No systems were found that provided the desired day/night detection and assessment capabilities. A system employing radar techniques and thermal and visible optics with motion detection, tracking, and advanced signal processing is currently being developed.

Standoff Surveillance Detection

With the increase in terrorism in the United States and around the world, legitimate concerns for the security of individuals, valued national assets, and infrastructure have evolved. As mentioned previously, systems have been developed to help protect fixed and temporary sites against the threats of direct vandalism, theft, sabotage, and direct attack. Another type of threat, known as the standoff threat, is also of concern. Generally, terrorists will commit their standoff terrorist acts from a distance, beyond the limits of conventional physical security systems. These locations are usually chosen to afford the terrorists a reasonable chance of escaping from the scene. The standoff attack can be committed from a crowd, a vehicle, (ground, water, or airborne), structures (buildings, towers) or surrounding real estate (flat, rolling, mountainous, bare, vegetation, or tree-covered from sparse to heavy) outside the normal area covered by physical protection procedures or systems.

The standoff attack may be launched from a position which may or may not be under the control of those persons providing the normal physical protection. In general, the attack position is not under their control, and any detection system deployed must be on real estate controlled by the protective force or for which permission to permanently or temporarily locate systems has been previously granted.

Most of the human detection systems mentioned above require that the human be moving. Of major concern are terrorists who are immobile and partially concealed in trees or behind rocks, i.e., in a sniper position. Sniping with a rifle or other weapon requires that the terrorist have a view of the intended target. To attain this view and be able to aim the weapon requires some portion of the body be exposed. This aiming requirement thus provides the potential for detection if a means of detecting stationary targets can be found or developed.

Currently available and evolving technologies that could be used to detect terrorists with standoff weapons were reviewed. A detailed evaluation of the problem and a review of many technologies resulted in a parametric study of two possible hardware designs for detecting stationary targets: (1) existing battlefield surveillance radars will detect moving intruders under open field conditions, and (2) several concepts for foliage-penetrating radars for detecting moving human intruders have been demonstrated.

The detection of stationary human targets in foliage is very difficult, and no technologies currently available will detect a terrorist partially hidden in a tree line. The study presumed that such terrorists would first observe a site for possible targets, vulnerabilities, and movement schedules before attacking. Detection during this period would allow security to intervene.

Two technologies that are expected to be useful for detecting stationary intruders have been identified:

(1) A scanning short-pulse laser radar

(2) An ultra-wide-band (UWB), very high frequency synthetic aperture radar (SAR)[13]

The foliage-penetrating SAR appears to have the best all-around performance for fixed sites, but it is not easily portable. The laser radar is a more compact system, and thus more suitable for protecting dignitaries, but requires some target exposure. The laser radar may have a higher nuisance alarm rate than the SAR in windy conditions.

Careful examination of the problem indicated that higher nuisance alarm rates can be expected for both systems when covering large areas where there is no control over animal or human access. This problem is further compounded by the difficulty in providing rapid visual assessment due to camera, visibility, and lighting limitations, as well as the longer distances that must be covered. However, such systems may be particularly useful for short-term protection, where every alarm can be reasonably assessed.

Considerable expertise exists in generating high-powered, UWB radar transmitter pulses. A preliminary design analysis [13] shows that a human 2 m inside a brushy tree line could be detected at a range of 500 m using SAR techniques. The main radiated frequency would be selected to coincide with the resonance of a standing human while providing good foliage penetration. The SAR technique would require that either the radar be vehicle-mounted and driven constantly around the area, or if a fixed system is desired, that a very large array of antennas be mounted just inside the site boundary. The UWB pulse can detect an intruder, even if completely hidden, but it generates signals in the band reserved for the Aircraft Emergency Locator Beacons. A UWB radar pulse can be digitally synthesized to produce "chirped" pulse radar that excludes these frequencies.

The advantages and disadvantages of the VHF SAR are presented in Table 1.

Table 1. Advantages and Disadvantages of the VHF SAR

ADVANTAGES	DISADVANTAGES
• Detects terrorists in the tree line, even if they are completely hidden • Minimal data processing as compared to a laser radar • Naturally tuned to detect humans and reject small animals, leaves, twigs, etc. • Low exposure levels to people and animals; no eye-safety problem • Not sensitive to windblown vegetation • All weather performance	• Will require licensing • Must be driven around or else a large antenna array must be used; if a moving vehicle is used, the terrorist must stay in one place during the drive-by • If a fixed antenna array is used, it should be as long as the sector covered (300–500 m); antennas should be mounted every few meters along the site boundary

The Laser Ranging and Imaging Detector (LaRID) would use a short-pulse laser radar to measure and map the range, azimuth, and elevation of each portion (detection pixel) of the tree line. These detection elements would be about 15 cm square by 30 cm deep in range. The reflected signal from objects in each of these detection volumes would be recorded so that any subsequent and significant changes would cause an alarm. This system could cover a 60°–180° perimeter sector from one spot. However, it could be very sensitive to false alarms from windblown vegetation.

The advantages and disadvantages of the LaRID system are presented in Table 2.

Table 2. Advantages and Disadvantages of the LaRID System

ADVANTAGES	DISADVANTAGES
• All detection can be done from a fixed point • May not require a separate assessment camera suite • No licensing or interference problems	• Very sensitive to windblown vegetation • Eye-safety concerns • Terrorist must be at least partly exposed or be using binoculars

Conclusion

Early warning, albeit highly desirable, is difficult to achieve. For portable systems, the technologies used in UGSs (break-wire, acoustic, seismic, magnetic, and active and passive infrared) are useful. Additionally, acoustic beam-forming listening devices and strain-sensitive cables attached to concertina rolls offer potential. Likewise, portable bistatic and monostatic microwave sensors (including radars) and optical radars (LADARS) and long-range observation posts should be considered. In addition to these sensors, buried-line sensors are also useful in border and fixed-site security systems.

Short sections of border security systems (those near permanently stationed border control personnel) may be overt (clearly visible for all to see). Longer sections not continuously manned must be covert. Fixed sites with a PIDAS are all overt. Systems (optical, radio frequency, and infrared) with motion detection and tracking can also be used for portable, border, and fixed applications, but they are usually constrained to fixed sites.

Standoff attacks on government facilities or other national infrastructures are a legitimate concern, and technology in this area is advancing rapidly. The fields of high-performance electro-optics radar and image processing for standoff attack application are particularly promising. Techniques are now available that we believe will detect partially hidden, unmoving terrorists who may be planning to launch standoff weapons.

From a technical standpoint, the results of this study suggest the benefits of experimenting with both the UWB and laser radar systems. Laser radar is recommended for the short-term protection of dignitaries speaking outdoors or other small, exposed assets because it returns the largest amount of information, does not need a secondary assessment system, and can be set up in a single location. Laser radars are still evolving, but advanced designs are currently able to detect very subtle movement and can possibly be trained to ignore blowing vegetation. For longer term protection at fixed locations, the UWB foliage-penetrating SAR would be preferred because it can preferentially detect humans over small animals, would have fewer false alarms under windy conditions, and is not dependent on partial exposure of the terrorist.

REFERENCES

1. J. D. Williams, D. J. Gangel, and R. W. Madsen, "Temporary Physical Protection Systems," *INMM 32nd Annual Proceedings,* July 1991, Vol. XX, pp 367-372.

2. Advanced Systems Integration Department 9561, "Systematic Analysis of the Southwest Border," Sandia National Laboratories, RS 9561/93/1, Three volumes, January 1993.

3. H. D. Arlowe and D. Coleman, "The Mobile Intrusion Detection and Assessment System (MIDAS)," SAND89-3016C, *IEEE Carnahan Conference on Security Technology*, 1990.

4. H. D. Arlowe and R. C. Dykhuizen, "Environmental Sensitivity of Thermal Intrusion Detection," *Proceeding—Annual Meeting of the Institute for Nuclear Materials Management*, 1992.

5. J. Beck et al., "240x1 LWIR Vertically Integrated Photodiode Focal Plane Array," *Proceedings—IRIS Specialty Group on Infrared Detectors,* ERIM, Ann Arbor, MI, March 1992.

6. J. P. Karins, "IRDOC, An IR Sensor Design Optimization Program," *Proceedings— IRIS Specialty Group on Passive Sensors*, ERIM, Ann Arbor, MI, March 1992.

7. C. J. Munno, "Automatic Video Image Moving Target Detection for Wide Area Surveillance," *Proceedings—IEEE International Carnahan Conference on Security Technology*, 1993.

8. D. A. Pritchard, "An Infrared Imaging Area Sensor for Tactical and Physical Security Applications," *IRIS Specialty Group on Passive Sensors,* ERIM, Ann Arbor, MI, March 1990.

9. D. A. Pritchard, R. F. Davis, and J. E. Simpson, "Evaluation of Automatic Detection of Humans and Vehicles," *Proceedings—IRIS Specialty Group on Targets, Backgrounds, and Discrimination*, ERIM, Ann Arbor, MI, January 1993.

10. *FLIR92 Thermal Imaging Systems Performance Model,* US Army Night Vision and Electronic Sensors Directorate, Document 5008993, Fort Belvoir, VA, 1993.

11. J. T. Vigil, "An Evaluation of Exterior Video Motion Detection Systems, Volume 1: Intrusion Detection Tests, SAND92–0108, Sandia National Laboratories, 1992.

12. D. A. Pritchard, "Panoramic Imaging Perimeter Sensor," *Proceedings—11th Annual Joint-Government-Industry Security Technology Symposium and Exhibition*, American Defense Preparedness Association, Virginia, Virginia Beach, VA, June 19–22, 1995.

13. H. D. Arlowe, Larry D. Bacon, Gary S. Phipps, and William C. Sweatt, "Detection of Terrorists with Standoff Weapons Final Report," SAND93–1034, Sandia National Laboratories, 1993. (Originally prepared by H. D. Arlowe as "Detection of Terrorists with Standoff Weapons," for Office of Special Technology, Naval Explosive Ordnance Disposal Technology Center [TSWG36–93])