REPORT D

AD-A265 003

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 1993	Professional Paper

4. TITLE AND SUBTITLE

INTELLIGENT SECURITY ASSESSMENT FOR A MOBILE ROBOT

5. FUNDING NUMBERS

PR: CH01
PE: 0602624A
WU: DN309216

6. AUTHOR(S)

R. P. Smurlo, H. R. Everett

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Command, Control and Ocean Surveillance Center (NCCOSC)
RDT&E Division
San Diego, CA 92152–5001

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U. S. Army
Army Armament R&D Command
Dover, NJ 07801

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

In many robotics applications the data from different types of sensors must be fused to provide useful information about the surrounding environment. The system described here uses sensor fusion to determine the probability that an intruder is present in the vicinity of a remote robot. Several of these robots are employed in an indoor security scenario, where each robot monitors a different region of a large building and reports back intruder information to a single operator. This paper examines the realtime security assessment algorithm used by each robot to fuse information from 82 sensors of five different types, and return a single composite threat value to the operator. The algorithm described has been successfully tested on a single robot with 99% probability of detection achieved. No nuisance alarms were recorded.

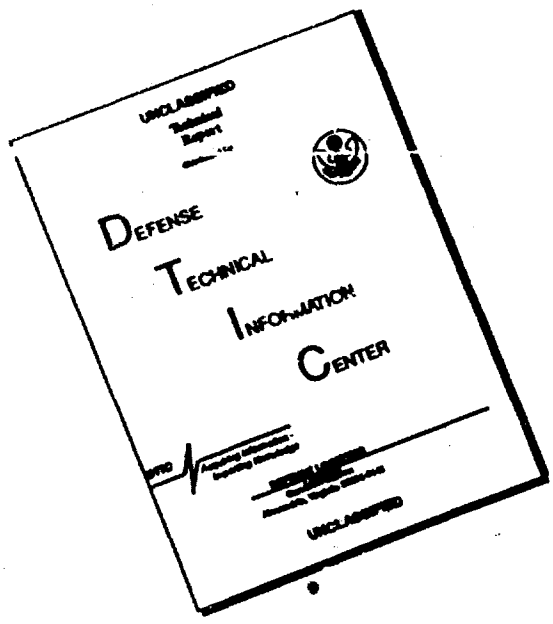
Published in *Proceedings*, Sensor Expo, Sep 1992, pp 125–132.

14. SUBJECT TERMS		15. NUMBER OF PAGES
robotics	sensors	
artificial intelligence	security	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAME AS REPORT

21a. NAME OF RESPONSIBLE INDIVIDUAL	21b. TELEPHONE (Include Area Code)	21c. OFFICE SYMBOL
R. P. Smurlo	(619) 553-3668	Code 531

DISCLAIMER NOTICE



THIS DOCUMENT IS BEST QUALITY AVAILABLE. THE COPY FURNISHED TO DTIC CONTAINED A SIGNIFICANT NUMBER OF PAGES WHICH DO NOT REPRODUCE LEGIBLY.

Intelligent Security Assessment for a Mobile Robot

Richard P. Smurlo
H. R. Everett

Naval Command, Control and Ocean Surveillance Center
Code 531
San Diego, CA 92152-5000
(619)553-3668

Abstract

In many robotics applications the data from different types of sensors must be fused to provide useful information about the surrounding environment. The system described here uses sensor fusion to determine the probability that an intruder is present in the vicinity of a remote robot. Several of these robots are employed in an indoor security scenario, where each robot monitors a different region of a large building and reports back intruder information to a single operator. This paper examines the realtime security assessment algorithm used by each robot to fuse information from 82 sensors of five different types, and return a single composite threat value to the operator. The algorithm described has been successfully tested on a single robot with 99% probability of detection achieved. No nuisance alarms were recorded.

Introduction

The security assessment algorithm was developed and tested on ROBART II, a prototype research platform, and is now being converted to run onboard the robot shown in figure 1. The sensors used in detecting an intruder include a video motion detector, an acoustic sensor array, a passive infrared (PIR) array, a microwave array and an ultrasonic (sonar) array. The information from the individual sensors must be fused together to determine the probability of an intruder, while effectively eliminating the occurence of nuisance alarms.

The algorithm employs a polar representation of the sensor data to establish the composite threat score for each of 24 wedge-shaped zones, 15 degrees apart, as shown in figure 2. The operator is alerted to any situation where the composite threat score for a given zone exceeds the alarm threshold, as

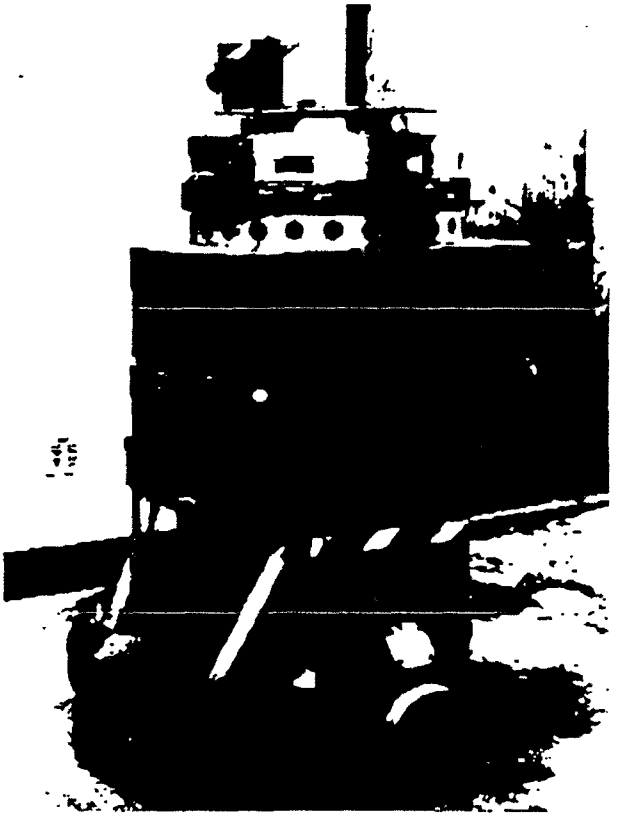


Figure 1. Security Robot

will be discussed in more detail later. A threat assessment value in the range of 0 to 100 is provided as a quantitative indicator of classification confidence, and a threat vector originating from the robot's current position is graphically depicted on the map display.

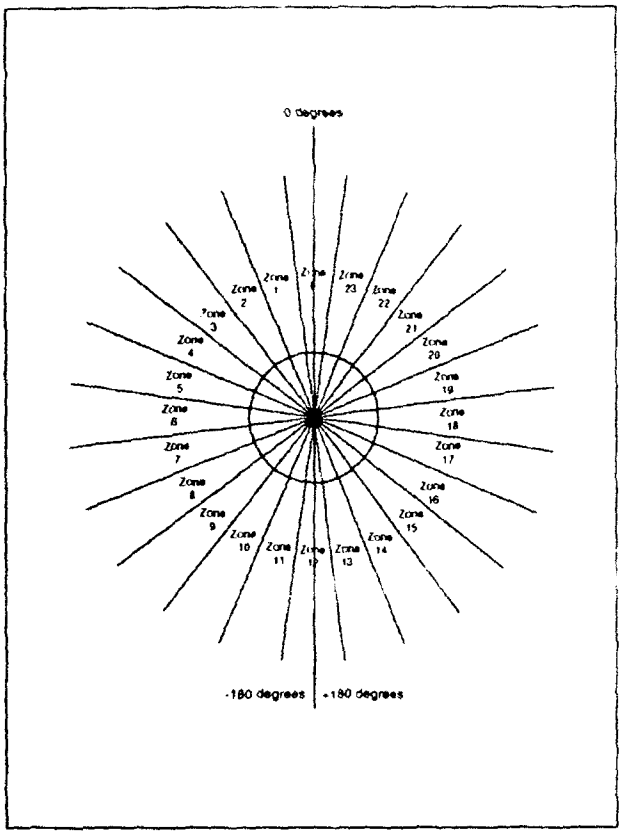


Figure 2. Intrusion Detection System Coverage Zones

Background

One of the earliest perceived applications for autonomous devices was acting as a sentry or security guard. Numerous sensors are readily available to support the detection functions (fire, smoke, intrusion, toxic gas, flooding, radiation, etc.) The ability to maintain an effective security presence under adverse (severe weather, degraded visibility) or even hazardous (nuclear, chemical, and biological) conditions is imperative, and appropriately addressed by mobile robotic systems of this type (Everett, 1988; Zalud, 1992). Success, however, requires the needed research issues of environmental awareness, fixed and mobile sensor fusion, and intelligent security assessment be treated from a systems integration point of view.

Potential security functions assigned to a mobile sentry robot can be categorized into four general areas: (1) detection, (2) verification, (3) assessment, and (4) response (Everett, et al, 1990). Detection is readily addressable by a multitude of commercially available sensors. Verification involves cross checking with other sensors to lessen the chances of a nuisance alarm, and depends heavily upon both the types of detectors employed and the operating environment. The assessment task acts upon the data collected to ascertain the nature of the disturbance, usually to determine if a response is necessary. The response itself must be tailored to the nature of the situation.

Before going into detail about how the robot performs these security functions it is necessary to look at the individual sensors and how they are used in a security environment.

Security Sensor Subsystems

When assessing the possibility of an intruder, the robot receives information from five different types of sensors: a video motion detector (VMD), an acoustic sensor array, a passive infrared (PIR) array, a microwave array, and an ultrasonic (sonar) array. The sensor arrays are independent of one another, and each covers the full 360-degree view surrounding the robot. Each array has its own local processor and is connected to the rest of the system by a power bus and a communications bus. With this *modular* design, each processor can keep track of the state of its sensors and perform any necessary pre-filtering of the data before reporting the information back to the security assessment processor when requested. This modular design approach also allows sensor suites to be modified or upgraded easily when new hardware or improved software algorithms become available (Smurlo, 1991).

Each sensor array continuously updates its sensor information and saves it until requested by the security assessment processor. Once the security assessment processor acquires this information, it uses it to determine the probability that an intruder is present. The functionality of the individual

sensor suites will be discussed below (Everett, 1990).

Video Motion Detector (VMD)

The video motion detector subsystem used on the robot consists of a video camera mounted on a pan and tilt mechanism, which allows the camera to cover the full 360-degree view of the robot. To conserve power, the VMD is only activated when the composite threat is at a warning level, at which time it points in the direction of the perceived disturbance to confirm or discount the threat. The VMD subsystem includes a video line digitizer, an 8-bit microprocessor, an address controller, and video RAM as shown in figure 3. In order to reduce the image processing needs, the VMD only digitizes three select lines from the composite video image. With three lines equally spaced throughout the scene, effective full-screen coverage is achieved without the need to *grab* the entire frame.

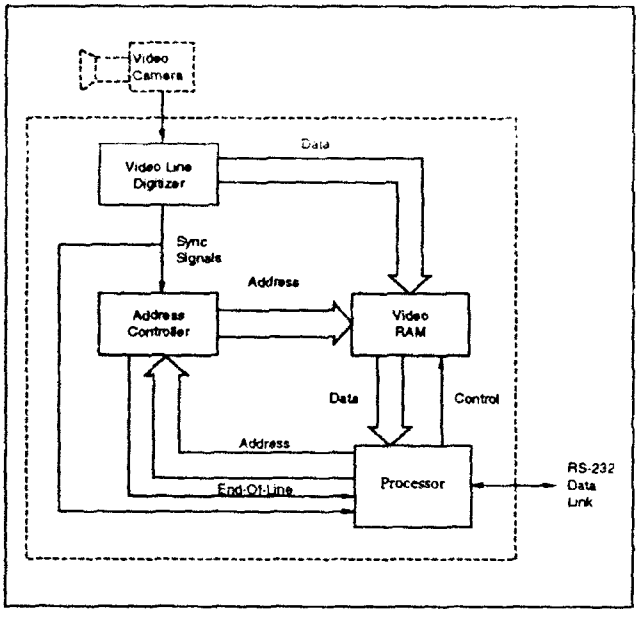


Figure 3. Video Motion Detector Block Diagram

The vision processor commences data transfer and analysis when the *line grabber* has completed an acquisition operation. The most simplistic motion detection scheme, and the one employed here, involves subtracting the current intensity array from a previously acquired array, and reacting to any significant discrepancies between the two, which are indicative of a change in the scene under observation. In reality, some software filtering is required to eliminate noise and reduce the occurrence of nuisance alarms, but this is easily accomplished on a 512-element linear data array in the time available.

Assuming full 512-pixel coverage, only 2K bytes of RAM are sufficient to support the microcomputer operating system and to save three select lines of video data. When motion is detected in any of the three lines, three new lines are selected for the next motion analysis operation. If these lines are chosen in such a fashion around the vicinity of the initially detected disturbance, it is possible over successive frames to converge on and effectively bound the area perturbed by the intrusion. In this fashion, the system can detect and output information describing the geometric area involved so as to provide servo-control inputs for camera positioning or robot motion algorithms.

Acoustic Sensor Array

A passive acoustic sensor array (ASA) has been developed to provide bearing information to the source of detected noise. The array consists of three omnidirectional microphones symmetrically oriented 120 degrees apart, and separated by a distance *d*. The prototype version of the ASA is shown in figure 4 mounted on ROBART II, with the three transducers individually supported by coil springs. The springs provide some degree of acoustical isolation, while raising the transducers so as to yield a clear path for wavefront propagation without any blockage by the video camera.

The ASA will calculate a bearing to an acoustical disturbance when the sound travels across the array and triggers all three detection elements in a specific sequence, the exact order of course being dependent on the relative position of the source. Because of the symmetrical orientation discussed above, the direction of the disturbance can be classified as being in one of six sectors by examining the *firing* sequence of the comparators associated with each of the three detectors. The relative bearing to the perceived source is then calculated using conventional triangulation techniques and converted to an absolute bearing depending on the sector involved.

Passive Infrared (PIR) Array

Passive infrared sensors detect changes in the energy spectrum at the 10 micrometer wavelength, which is generated by a potential intruder in the form of body heat. This type of pyroelectric sensor has quickly shown application on mobile robots due to the small size, low power consumption, and excellent performance and reliability characteristics.

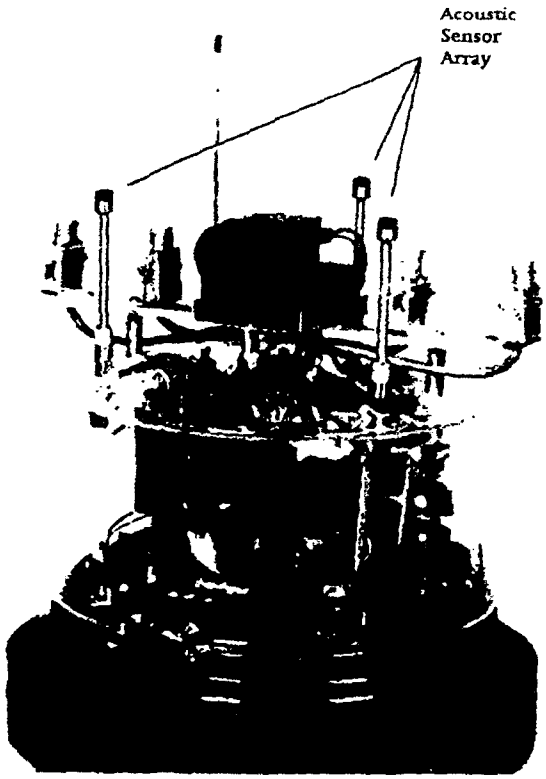


Figure 4. Acoustic Sensor Array mounted on ROBART II

The PIR array employed on this security robot consists of 48 individual sensors arranged in a symmetrical fashion (figure 1). Each sensor covers a non-overlapping, cone-shaped detection field. After a brief settling period upon power-up, the circuit adjusts itself to ambient conditions, and any subsequent deviations from that setpoint will result in an alarm output. This type of sensor exhibits a low nuisance alarm rate in an indoor environment, and therefore is weighted more heavily when calculating the possibility of an intruder.

Microwave Array

Microwave motion detectors are active devices which operate at radio frequencies and rely on the Doppler shift introduced by a moving target to sense the relative motion of an intruder. Six microwave sensors are equally spaced in an array to provide full 360-degree coverage around the robot. Since microwave energy is known to reflect off walls, each sensor tends to flood the room and when an intruder is present, several sensors may activate simultaneously. Due to this phenomenon, the directional information from these sensors has been weighted less heavily.

Ultrasonic (sonar) Array

The sonar array consists of an ultrasonic ranging module multiplexed to 24 Polaroid electrostatic transducers. The ranging module is an active time-of-flight device developed for automatic camera focusing, and determines the range to a target by measuring the elapsed time between the transmission of a *chirp* of pulses and the detected echo.

Upon activation in the security scenario, the 24 sensors are fired to get initial range readings with no intruder present. The sonar sensors then fire at a periodic rate and compare the new range readings to those obtained from the initial readings. Any deviation in the two sets of readings are interpreted as an intruder being present. Both range and bearing to the intruder can be determined in this fashion.

Data Acquisition

On each pass through the main program's security assessment loop (figure 5) the state of each sensor, as represented in a blackboard data structure, is monitored. If a sensor state has changed, its new state and the time are stored in the *current information* field of the blackboard. The data that was previously in the *current information* field is placed at the front of the *history list* in the same data structure. In this way, a detailed history of the state of each sensor is kept for a finite period of time, typically five minutes. Also in the data structure is a *baseline weight* for each sensor which determines how much each sensor contributes to the overall composite threat. The baseline weighting values are taken from an array which

bases the initial weight on the demonstrated reliability of the individual sensor.

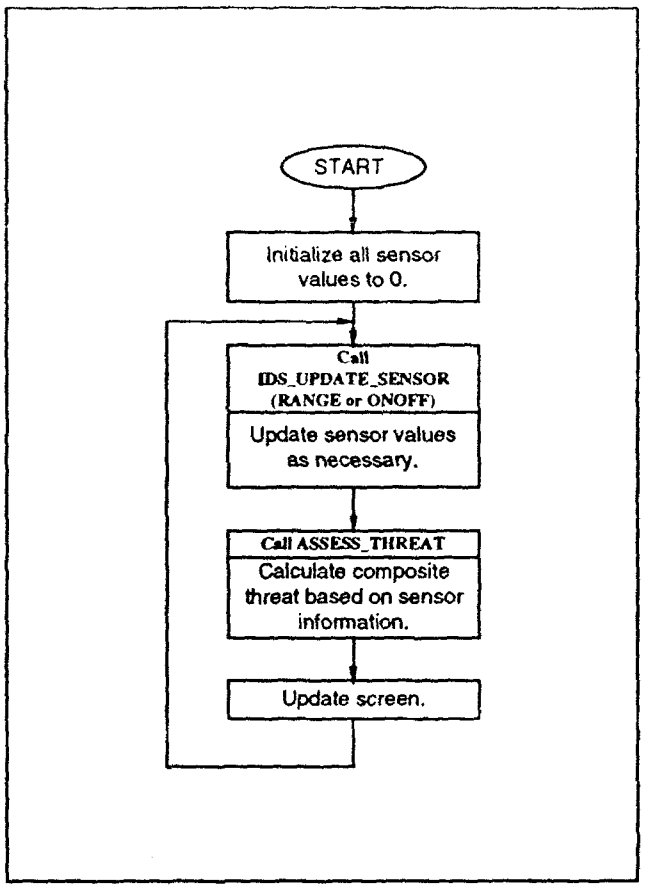


Figure 5. Intrusion Detection System Main Program Flow

After new data has been read in, the *threat assessment* function is called. This function adjusts the sensor weights when purposeful motion is detected or when sensors of different types correlate with each other. The *threat assessment* function (figure 6) then calculates the composite threat based on the adjusted weights. The weight adjustment and composite threat calculation algorithms are discussed below.

Detecting Purposeful Motion

The information stored in the history file is analyzed for signs of purposeful motion, and the weights for affected sensors are adjusted accordingly and stored as the updated current information as follows:

- The algorithm identifies the first active sensor of a given group.
- If a sensor to the right or left of the active sensor is also currently active, the active sensors weight is increased by a factor K_0.
- Data stored in the history file is then examined to determine if adjacent sensors of the same group on either side of the active sensor had previously been active within some prespecified period of time.
- If history of such activity is present, the weight of the active sensor is increased by an increment equal to its initial weight times some scalar S_1.
- In the event an adjacent sensor is found to have been active, the history file is again examined to see if the next sensor in the array also had previously detected motion.
- If previous motion is again indicated, the weight of the active sensor is further increased by a second increment equal to its initial weight times some scalar S_2.
- This process is then repeated for all other active sensors of the given type, after which the remaining groups of motion detection sensors are similarly examined.

In this fashion, if a temporal history of lateral motion across the field of view of the sensor array is present such that adjacent sensors are activated in a distinct sequence, the resulting signature is classified as purposeful as opposed to random motion, and the active sensor weight is significantly increased.

Most of the motion detector arrays (microwave, PIR, acoustical, video) are capable of angular resolution only, and provide no range information. An exception is the ultrasonic motion detection array which identifies a potential intrusion through changes in measured target distances as seen by one or more sensors in the 24-element array. This feature provides for an additional level of analysis to be performed on sonar data accumulated in the history file. Purposeful motion of an intruder should result in a somewhat continuous target path profile, with no significant discontinuities or jumps in target position. When properly exploited, this analysis can become an important tool which is especially helpful in filtering out bad sonar data. (Ultrasonic ranging systems operating in air are

particularly susceptible to errors arising from beam interaction at the target surface (Everett, 1985)).

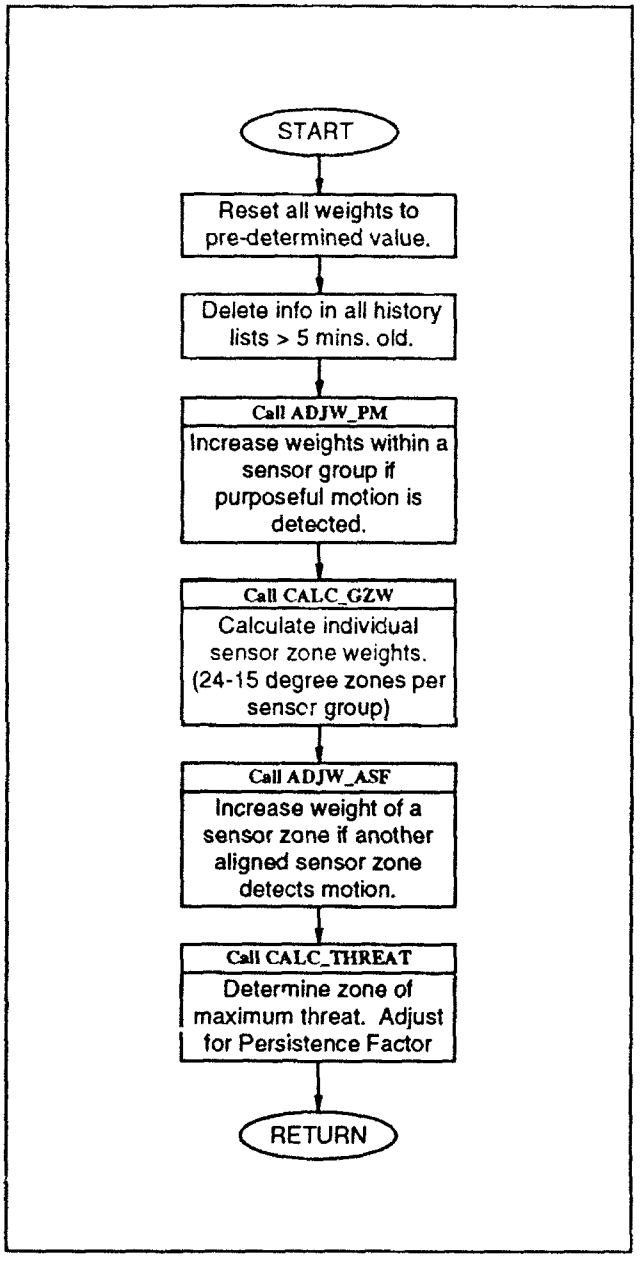


Figure 6. Intrusion Detection System Threat Assessment Flow

To further minimize nuisance alarms resulting from the inherent poor repeatability in range measurements, information from the PIR sensors is fused with that from the ultrasonic motion detection array. Only those changes in sonar range which are validated by a corresponding PIR hit are considered significant. This technique is referred to as *cross correlation*, or *angular sensor fusion*, and will be discussed in some detail below.

Cross Correlation

The next step in the assessment routine involves converting the individual sensor weights to zone weights for each sensor group. This is done by first determining for each sensor in a given zone the probability that the potential intruder is in that zone, given that the sensor is active. For example, if an active sensor lies on the boundary of two zones, there is a 50-percent probability that the intruder is in either zone. The calculated probability is multiplied by the sensor's weight, and the values are summed for each sensor in the zone. The zone weights of each sensor group are then checked for correlation and increased or decreased accordingly, thus minimizing the occurrence of nuisance alarms. This is accomplished as follows:

- Convert individual sensor weights of each group into 24 zones of 15 degrees each (save them as intermediate zone weights).
- Compare the zones of each sensor group with corresponding zones of other sensor groups.
- If two corresponding zones have non-zero weights, increase their zone weights as follows:

$$ZW_N(i) = ZW_O(i) + K_1(ZW_I(i) + ZW_I(j))$$

where:
$ZW_N(i)$ = New Zone Weight (sensor i)
$ZW_O(i)$ = Old Zone Weight (sensor i)
ZW_I = Intermediate Zone Weight
K_1 = Scalar Constant

Note that the adjusted weight values of the confirming sensors are used as the old zone weight in the above calculation. This becomes important when the zone weights from more than two sensor groups correlate. In this fashion, the increase in weighting is proportional to the confidence factor of the confirming sensor. This process is then repeated for all zones of each sensor group.

Composite Threat Calculation

Once the various weight contributions have been generated for the individual sensors of each type, the *threat calculation* function is called to sum the individual sensor group zone weights to generate a single composite threat value for each of the 24 zones. The maximum composite threat of the 24 individual zones is then used as the current composite threat. To smooth out the actual composite threat displayed on the screen, this current composite threat is compared to those values calculated in the last 4 seconds. The maximum of these values becomes the new composite threat.

Persistence Factor

The threat magnitude is then further adjusted by a *persistence factor* (PF), which provides an additional predefined contribution to the composite threat score. The PF is indicative of and proportional to the magnitude and duration of prior activity in the area under surveillance. The PF serves to increase system sensitivity for scenarios where some activity was previously detected, though this activity was in itself insufficient to generate an alarm condition.

$$PF = \int F(t)\, M(t)\, dt$$

Where F(t) represents some time-dependent weighting function, and M(t) similarly represents the magnitude of the observed composite threat as a function of time. These can be piecewise approximated over N arbitrary time increments as:

$$PF = \sum_{i=1}^{n} F_i M_i$$

$$= F_1M_1 + F_2M_2 + \ldots + F_nM_n$$

F(t) can be represented as a linear function which varies from 0 at T_0 to 1 at T_f, with the time between T_0 and T_f broken up into *n* sample periods. For example, if n = 10, then $T_1 = 0.1$, $T_2 = 0.2$, $T_3 = 0.3$, etc. up to $T_{10} = 1.0$.

M(t) meanwhile can be piecewise implemented as the maximum observed composite threat over any given time increment or sample period. In keeping with the above example which assumed 10 sample periods, the equation would appear as follows:

$$PF = S\,[0.1\, M_1 + 0.2\, M_2 + \ldots + M_{10}]$$

where M_1 through M_{10} are the maximum composite threat values observed during sample periods 1 through 10, respectively, and S is a scalar.

The PF should have some maximum upward bound, such as 10, and would be added to the current composite threat as follows:

Final Composite Threat =
Initial Composite Threat + PF

The final adjusted composite threat is then compared to a predetermined alarm threshold value. If the composite threat exceeds this threshold it is assumed to be in an alarmed condition. The axis of the active (alarmed) zone is then used to graphically plot a threat vector on the map display.

Situations Which Cause an Alarm

The initial weight values of each sensor and the multipliers such as S and K_0 have been chosen such that the following situations cause the robot to go into an alarm condition. Though these are not the only situations that cause an alarm, they are the most common.

1. A PIR sensor detecting purposeful motion is just below the alarm threshold. Any of the following minimum conditions must also occur to cause the composite threat to increase above the threshold:
   a) An adjacent PIR active.
   b) Any microwave sensor also active.
   c) Any other sensor group cross correlating.

2. Cross correlation of a sonar and PIR sensor is just below the alarm threshold. Any of the following conditions will cause the composite threat to increase above the threshold:
   a) An adjacent PIR active.
   b) Any microwave sensor active.
   c) A correlating video or acoustic sensor.

3. Cross correlation of a PIR and microwave sensor is just below the alarm threshold. Any of the following conditions will cause the composite threat to increase above the threshold:
   a) An adjacent PIR active.
   b) Three other microwave sensors active.
   c) A correlating video, acoustic, sonar, or PIR sensor.

4. The video motion detector alone is below the alarm threshold. Any of the following conditions will cause the composite threat to increase above the threshold:
   a) Cross correlation with an acoustic, sonar, or PIR sensor.
   b) A microwave at the same angle or two microwaves not at the same angle.

5. The acoustic sensor array active along with any of the following conditions will cause the composite to increase above the threshold:
   a) Cross correlation with video or PIR.
   b) Cross correlation with microwave AND sonar.
   c) Three microwaves, but must include the one at the same angle.

6. The following are examples of other less likely situations that will cause an alarm:
   a) Three adjacent sonars all on and the middle one detecting purposeful motion.
   b) Sonar sensor detecting purposeful motion AND one adjacent sensor of another type cross correlating.

Conclusion

The realtime security assessment algorithm discussed above has been shown to effectively fuse information from various types of sensors, interpret that information, and return a useful assessment of its surroundings to a remotely located user. The algorithm has been extensively tested with a demonstrated high probability of detection in an indoor environment. Furthermore, it has shown a significant improvement in differentiating between real and nuisance alarms as compared to a system which does not correlate information obtained from its individual sensors.

References

Everett, H.R., "A Multi-Element Ultrasonic Ranging Array," *Robotics Age*, July 1985.

Everett, H.R., "Security and Sentry Robots", *International Encyclopedia of Robotics Applications and Automation*, John Wiley, NY, March 1988.

Everett, H.R., Gilbreath, G.A., Tran, T.T., *Modeling the Environment of a Mobile Security Robot*, NOSC Technical Document 1835, Naval Ocean Systems Center, San Diego, CA, August 1990.

Smurlo, R., Laird, R.T., "A Modular Robotic Architecture," Mobile Robots V, Chun, Wolfe, Editors, Proc. SPIE 1388, pp. 566-577, 1991.

Zalud, B., "Robot Revival," *Security* , June 1992.