



**US Army Corps
of Engineers**
Engineer Research and
Development Center

Environmental Effects on Intrusion Detection Systems

Description ERDC has developed methods for determining the effects of weather and terrain on exterior intrusion detection systems (IDSs) to improve their effectiveness and accuracy. Diurnal and seasonal variations in site conditions, the less predictable changes caused by storms, and the sensor-specific impacts of winter conditions all affect IDS reliability.

Capabilities ERDC provides guidance to federal agencies and departments in the selection and operation of IDSs for specific site conditions, such as terrain, geographic location, season, and weather. Understanding the interaction of an IDS with its environment is necessary to assess and improve upon its reliability. ERDC's expertise can be applied to system development, trade-off studies, and performance testing, as well as to the selection, installation, and operation of commercially available IDSs.

Supporting Technology

The Weather Vulnerability Assessment Tool (WVAT) is a stand-alone software application that corrects for the influence of weather on IDS performance data and predicts detection capability under other weather conditions. WVAT alerts operators to specific situations (weather events, daytime/nighttime scenarios) in which the likelihood of detecting an intruder falls below a chosen allowable probability of detection. It also indicates the likelihood of nuisance alarms as a function of weather and time of day.

Exterior IDS testing takes place under realistic, natural conditions at the IDS facility at the Cold Regions Research and Engineering Laboratory in Hanover, N.H.

Benefits

Sensor system performance is optimized when environmental effects are accounted for during security planning and IDS installation, ensuring that the investment in infrastructure produces the required return in security level.

Security personnel who are aware of detection limitations due to weather and terrain effects understand that the probabilities of detection and nuisance alarm rates are a function of an IDS's operating environment.

If variations in site conditions exceed an IDS's alarm threshold, numerous nuisance alarms may occur, causing security personnel to lose confidence in the sensor system and perhaps even fail to respond appropriately. Transitional periods can be particularly troublesome because of the frequency of change in a sensor's operating environment.



Success Stories

To expand the range of technologies available to the federal government, ERDC experts are evaluating commercial security products under Cooperative Research and Development Agreements (CRADAs), with particular applications to basecamp security and monitoring access at training lands.

IDS field tests have included training exercises for U.S. Army Special Forces soldiers, who participated as high-threat intruders.

A model has been developed that compares an intruder's thermal signature (ITS) with SWOE data on the thermal background to predict if the contrast is adequate for detection.



Performance verification test procedures, describing actions specific to a given type of IDS, have been developed and are now included in field manuals.

Point of Contact

Contact Dr. Lindamae Peck at (603) 646-4261/Fax: (603) 646-4397, or by email at lpeck@crrel.usace.army.mil.