Toward Better Airport Perimeter Security

Aisthon Ltd., www.aisthon.com, +1(484)858-0505

The Significance of Airport Perimeter Security

Our commercial airports are critical elements of our national infrastructure, our economy, and our way of life. According to the Bureau of Transportation Statistics, in 2016 the US had 531 airports serving air-carrier traffic[1]. They handled 9.7 million flights moving 932 million passengers and 37 billion ton-km of freight. According to Oxford Economics, in 2011, the aviation sector comprised 4.9% of the US economy and provided 9.3 million jobs[2].

Given their critical importance and value, our airports are a key security concern, especially after the terrorist attacks of September 11, 2001. Since then, the US Congress, the FAA, and airport management teams have taken major steps to improve airport security including installation of security fencing and technology-based systems.

Major vulnerabilities still remain, however, as highlighted by a 2016 Associated Press report on perimeter breaches at major US airports[3]. The breaches can range from pedestrians breaching a perimeter for a short-cut to pre-meditated breaches with criminal intent; the latter ranging from minor vandalism to a major terrorist plot. Thankfully, there have not been any major incidents thus far, caused by such breaches other than relatively minor operational disruptions but they have exposed widespread systemic vulnerabilities. These vulnerabilities have the potential to result in major disruptions of air traffic, critical infrastructure damage, loss of life, and loss of public confidence in the safety and security of air travel. According to Barclays Capital, for example, "The events of 9.11…marked a permanent decline in [US] domestic airline demand"[4].

For these reasons many airports strive to establish and maintain the highest security of their facilities and address perimeter security as a major vulnerability.

Challenges in Securing Airport Perimeters

Airport perimeter security faces a number of challenges. Airport perimeters are typically quite long and can range from under 5 to over 30 miles. They are predominantly made up of land-based fence-line with various gate configuration but there are in many cases also natural or man-made water boundaries as well as various walls and buildings that comprise the perimeters. The settings also vary widely from dense urban to sparsely inhabited rural locations. Natural environments range from desert to densely vegetated, from tropical to arctic. This variability requires effective perimeter security systems to be flexible, scalable, and adaptable. They need to simultaneously

[1] https://www.bts.gov/topics/airlines-and-airports

[2] https://www.iata.org/policy/Documents/Benefits-of-Aviation-US-2011.pdf

[3] https://apnews.com/0971b39172ee48d28661aae33724644c/ap-intruders-breach-us-airport-fences-about-every-10-days

[4] http://www.iata.org/pressroom/Documents/impact-9-11-aviation.pdf

maintain high detection capability and very low false alarm rate while operating in mixed and demanding conditions that vary over time.

In addition, there are varying operational considerations such as budget constraints, legacy systems, existing electrical power and data infrastructure, and the specifics of airport operations that put additional constraints on perimeter security systems to be cost-effective, resource-efficient, and easy to integrate.

Perimeter Security Approaches and Limitations

Security management teams have a broad array of options for perimeter security. From perimeter security patrols to sophisticated technological solutions, they provide solution to certain security risks with certain trade-offs. Patrols, for example, offer a straight-forward approach with immediate detection and reaction options but offer only localized detection at any given point in time and can be easily circumvented by a prepared intruder. Camera surveillance can improve the coverage over patrols at the expense of reaction time. Operator surveillance may also be unreliable due to operator fatigue, may require a large number of cameras, and may not be possible in some perimeter areas or times due to the lack of electrical power or visibility. Similarly, many technology-based solutions, while providing better coverage, have high false alarm rates, especially in outdoor environments, making them inefficient and often lead to temporary or permanent disabling of key detection features or capabilities by frustrated operators.

Faced with such trade-offs, many security managers take a very cautious attitude to technological solutions, often delay addressing known vulnerabilities over many years.

Some security teams opt for multi-layered solutions, using a combination of approaches to maximize the probability of intruder detection and minimize the costly false alarms. This can often lead to very complex systems that are both expensive and difficult to manage reliably.

To ensure complete perimeter coverage, it is necessary to have a continuous coverage of the perimeter by a single system without hand-offs that may compromise its continuity. A common approach involves a continuous network of interconnected sensors installed at (on, under, or near) the perimeter (most typically fence-line).

Such systems are based on detecting acoustic or mechanical disturbances at the perimeter and processing the sensor signals to infer intrusion attempts. A common approach is to use fiber-optic, electronic, or electro-mechanical sensors to detect mechanical vibrations on the perimeter. Since the majority of systems employ continuous sensing media and have limited pinpoint accuracy, they are often sectioned into “zones” that are often 500-1000 feet long.

There are several issues that arise from this strategy. The relatively large zones often require manual video investigation of alarms in order to identify the source and can lead to frequent unnecessary security force deployment. In addition, the use of vibration sensing, has several major disadvantages:

- Common intrusion scenarios, where a heavy object (ladder, mattress, etc.) is placed against the fence, mechanical vibrations are heavily dampened and are often not detected.
- The system can be disabled carefully removing the cable ties and lowering the sensor cable slowly to the ground without producing detectable vibrations.
- Common environmental factors, i.e. wind, rain, traffic, jet exhaust, etc. trigger vibrations comparable to intrusions and produce false intrusion alarms.

Clearly, this leads to a system with major detection and reliability weaknesses that is also susceptible to a very high false alarm rate. To manage false alarms, a common "solution" is to reduce the sensitivity or even turn off detection during adverse weather conditions, leaving the facility unprotected.

Next-Generation Perimeter Security

Designed originally for the needs of major airports, the next-generation fiber-optic perimeter intrusion detection system (NG-PIDS) was developed specifically to address the shortcomings of prior PIDS solutions while meeting the most demanding requirements. Most notably, the system is designed to alleviate the debilitating trade-off between intrusion detection capability and false alarm rate affecting the vast majority of offered systems.

The system is based on a proven and mature fiber-optic sensing technology called Fiber Bragg Grating (FBG)[5]. FBG sensors are point sensors manufactured in optical fibers that are used commonly for structural integrity and condition monitoring in civil engineering, transportation, and the energy industry.

FBGs are passive sensors and require no electrical power or electronics in the field to operate. They are immune to EMI, RFI, and are immune to lightning strikes, hence require no grounding. They are intrinsically safe and require virtually no maintenance.

Compared to other fiber-optic sensing methods, FBG sensors provide high-speed, high-precision mechanical strain measurements with pinpoint location accuracy. The point nature of the sensors also allows the system to adapt to local variations in environmental conditions without sacrificing detection effectiveness. Unlike other sensor system that can detect only intrusions that result in mechanical vibrations, FBG-based systems can very reliably detect common breach scenarios with no significant fence vibrations, such as intruders using ladders or other large items placed on the fence.

A typical NG-PIDS system has hundreds to thousands of sensors. Given their high sensitivity, individual sensors are naturally affected by environmental noise and cannot be reliably used to detect intrusions. The array of data from all sensors, however, analyzed over space and time using advanced signal processing algorithms allows the system to differentiate human-caused fence disturbances from environmental disturbances and random noise.

[5] https://en.wikipedia.org/wiki/Fiber_Bragg_grating

NG-PIDS is a modular system, allowing to be modified, expanded or re-configured while maintaining the operation of the parts of the perimeter that are not changed. This means that the security of the perimeter can be maintained during repairs, maintenance, or upgrades to the fence, expansion of the perimeter or other changes to the site.

With its effectiveness and reliability demonstrated in multiple comparative field trials, the NG-PIDS is a critical component for any integrated perimeter security design. Optimal implementations use the system as the reliable early warning indication in conjunction with complementary technologies, such as video or radar, to verify intrusions and track perpetrators around and within the security perimeter. This ensures an overall system with no single point of failure and shortens the detection-to-apprehension time.

The NG-PIDS system has received awards for outstanding engineering and innovation and its outstanding performance in field trials and deployments has been recognized by security organizations worldwide[6][7][8].

[6] http://www.airportsinternational.com/2012/01/changi-airport-in-fibre-fencing-first-2/8534

[7] http://www.researchsea.com/html/article.php/aid/7958/cid/2/research/a_star_and_industry_partners_clinch_asean_outstanding_engineering_achievement_awards.html

[8] http://www.securitynewsdesk.com/perimeter-intrusion-detection-system-approved-uk-government-use/