

---

**Dedicated Distributed Sensing – The  
Right Approach to Wireless  
Intrusion Prevention**

## Dedicated Distributed Sensing – The Right Approach to Wireless Intrusion Prevention

*Wireless technology is growing in popularity. Businesses are not only migrating to wireless networking, they are steadily integrating wireless technology and associated components into their wired infrastructure. The demand for wireless access to Local Area Networks (LANs) is fueled by the growth of mobile computing devices, such as laptops and personal digital assistants, and a desire by users for continual connections to the network without having to “plug in.”*

*“Wireless LANs are the major wireless security problem facing businesses through 2008.”*

**Gartner, 2004**

Like most innovative technologies, using Wireless LANs (WLANs) poses both opportunities and risks. The wireless explosion has given momentum to a new generation of hackers who specialize in inventing and deploying innovative methods of hijacking wireless communications, and in using the wireless network to breach the wired infrastructure. The reader is referred to the AirDefense white paper “Wireless LANs: Is My Enterprise at Risk?” for more details on the risks associated with wireless networks.

### ***WIPS Architectures***

The ease with which WLANs can be compromised has fueled the need for WIPS. The WIPS monitors airwaves, looking for attack signatures, protocol/policy violations and behavioral anomalies. It reports these events and could also take corrective measures, if required. Fundamentally, two WIPS architectures have evolved.

### ***The AirDefense Solution***

The AirDefense solution is based on a ***Distributed Collaborative Intelligence Architecture*** (DCIA), pioneered by AirDefense, to provide the most comprehensive wireless intrusion protection. DCIA uses a ***dedicated*** network of sensors and embedded client based agents that continuously monitor the airwaves and wireless activity for attacks and policy violations. This architecture has the following salient features:

1. APs with special firmware allowing promiscuous mode are used as dedicated sensors. Promiscuous mode allows sensors to listen to all packets picked up by the antenna. In addition, the sensors use an intelligent channel scanning algorithm to detect traffic across the RF spectrum. The sensors locally analyze all the received packets, collect several statistics and events of interest and use a very efficient Application Programming Interface (API) to communicate selected events and statistics over a secure link to a centralized server.

2. Lightweight software agents are installed on laptops and other wireless devices. These agents monitor wireless activity and enforce pre-determined security policies even when the device is not within the monitored enterprise perimeter.
3. The centralized server correlates events and statistics from all the sensors and agents and runs a multi-dimensional engine that integrates several detection technologies. Security policies are centrally managed and monitored from the server.

### **Infrastructure Integrated Solutions**

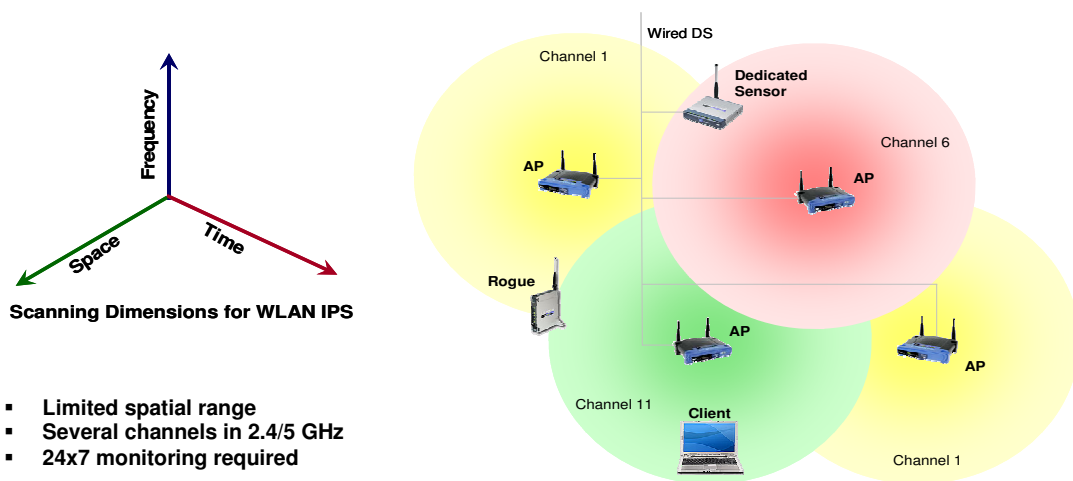
As the market demand for WIPS increased, WLAN infrastructure vendors that originally provided wireless Access Points (APs), switches and controllers have tried to roll-in basic WIPS features and sell an integrated ‘check-box’ solution. In this architecture, some APs provide time multiplexed functionality serving as regular APs and part-time sensors. When the APs are providing data services, they are locked on a given channel and cannot hear traffic on other channels. When the APs are serving as sensors, regular wireless clients could have their link disrupted. The sensors may act independently or aggregate their information into a switch or controller.

### **Myths of Integrated WIPS Solutions**

This section debunks some of the myths associated with integrated ‘check-box’ solutions available from infrastructure vendors.

### **Myth #1 – Part-Time Scanning Is Good Enough**

Figure 1 shows a typical WLAN deployment in the 2.4 GHz band. APs on non-overlapping frequencies are placed adjacent to each other so that devices can concurrently communicate in adjacent cells. If an AirDefense solution is employed, a dedicated sensor is placed for every few APs. In the infrastructure integrated solutions, the APs themselves have to double up as scanners.



**Figure 1:** WLAN deployments and multi-dimensional WIPS scanning requirement

Let us look at the complexity of the WIPS scanning requirement. An intrusion can happen anywhere in the wireless deployment area, it can happen at anytime and worse it can happen at any frequency. Dedicated sensors have significantly better visibility along the frequency and time dimensions. In the FCC domain there are 13 channels in the 2.4 GHz band and 23 channels in the 5 GHz band. WLAN devices usually support various other country specific channels. Wireless clients constantly scan channels looking for a strong signal to connect to. Part-time scanning solutions claim that they have the ability to go off-line and scan other channels with fine time granularity. While this approach might somewhat work for static rogue devices that are on the network for extended periods of time, it will not be effective against transient attacks. As network load increases, APs doubling up as sensors will find it increasingly hard to go offline to scan other channels. Further, latency sensitive traffic such as voice will make AP offline scanning virtually impossible without disruption in call quality. Simply put, part-time scanning solutions offer the least protection when the wireless network is being used the most.

To quantify the effect of network load on part-time scanning efficiency we performed a simple simulation. Regular traffic was generated on one channel and unauthorized traffic was generated on a different channel. Frames of different sizes characteristic of 802.11 were used with frame arrival characterized by a Poisson process. AP channel utilization was increased by increasing the regular traffic load. We assumed an oracle AP that knows when packets are arriving on its operating channel and misses none of them. The perfect AP scans for unauthorized packets when there is no traffic on its operating channel. Figure 2 shows simulated results. Even with a low channel utilization of 20%, the perfect AP is only capable of detecting about 60% of unauthorized frames on a different channel; at 50% utilization the unauthorized frame detection capability is down to 15% and at 90% utilization it is less than 1%. In reality, an AP scanning on a different channel will occasionally miss regular data frames on its operating channel. Depending on the QoS that the AP wants to guarantee, it will be forced to scan pessimistically reducing the unauthorized frame detection rate even further.

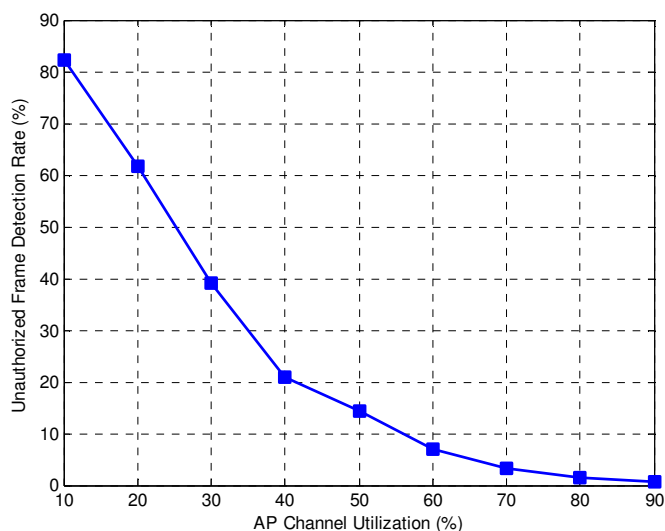


Figure 2: Best case rogue frame detection rate as a function of AP channel utilization

Even in a low channel utilization scenario, a determined hacker can easily generate traffic to lock an AP that is working on a given channel while simultaneously lure a probing station on a different channel with a stronger signal. Another example where part-time scanning will not work is with stealth rogue devices. Such devices are becoming increasingly popular with the hacking community. A stealth rogue device lies dormant until it hears a secret knock. The knock could be generated using a special sequence of benign looking frames that triggers the rogue device to start actively transmitting for a pre-determined amount of time. Again, it is easy to engage part-time AP/scanners on different channels while stealth rogue communication is occurring.

As we have seen, part-time scanning definitely presents significant frequency holes in the WIPS architecture. A popular misconception is that part-time AP/scanners can at least listen to all the traffic that is being exchanged on the channel they are working on. A fundamental problem with this argument is that an AP that is transmitting cannot listen to any other packets on the same channel. WLAN transceivers are half duplex. In addition, typical WLAN traffic patterns are asymmetric, i.e., more data gets downloaded from an AP than uploaded to it. It is not unusual for an AP to have 80% of its frames being transmitted and only 20% being received. In a fully loaded network, this implies that an AP suppose to be providing sensing functionality, at least on it's operating channel, will not be able to listen to any traffic 80% of the time.

Another argument that is used by 'check-box' infrastructure solutions is that since APs typically outnumber dedicated sensors – they have better spatial coverage. This argument ignores the fact that AP deployments are very dense to ensure uniform coverage at the highest data rates. Management frames typically get exchanged at the lower data rates. Lower data rates have much more transmission range than higher data rates. In a dense deployment scenario, as shown in Figure 1, a single dedicated sensor will be able to monitor WIPS critical management frames that get exchanged at lower data rates. If more sensors are required, they can always be added. The notion that the associated cost will be extremely high is not true (see Myth #3 below).

*“The AirDefense platform with 24x7 monitoring has the right approach to WLAN security.”*

**Jeff McConocha, President, NCS Datacom**

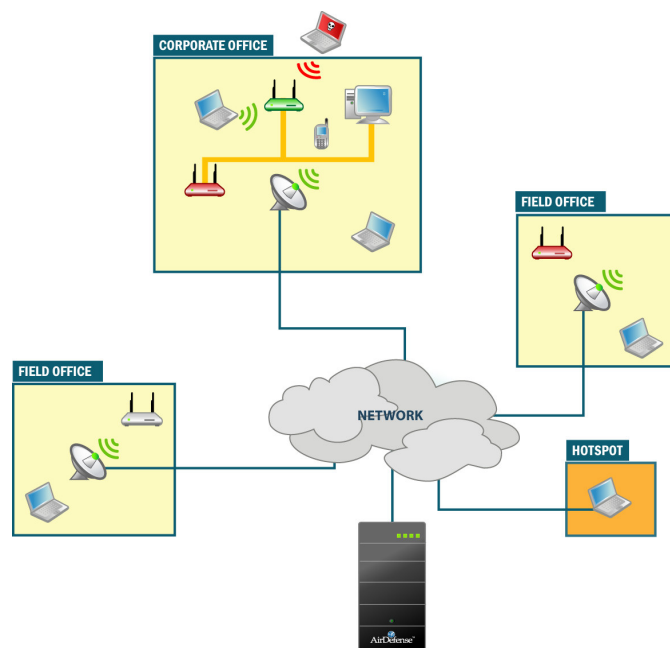
**Conclusion:** Part-time scanning solutions present significant frequency and time holes in a WIPS that can easily be exploited.

## **Myth #2 – Regular Access Points Can Always Be Made Into Full-Time Scanners**

Some infrastructure 'check-box' solutions have recognized that full-time scanning is essential for true WIPS. They have recanted their original argument by saying that if full-time scanning is required, it is easy to convert an AP into a dedicated sensor, on the fly. While this may seem straightforward, there are several practical issues that arise. WLAN infrastructure solutions come in different flavors. Most of the architectural variations lie in the functional split between the actual AP and the switch/controller to which the AP connects to. 'Thin AP' architectures implement most of the MAC functionality at the switch leaving only timing critical functions for the AP. 'Thick AP' architectures implement almost all of the functions within the AP itself. Several intermediate flavors exist between the true 'thin' and 'thick' AP architectures. Depending on the infrastructure vendor, putting a regular AP in a dedicated sensor-only mode may or may not provide full promiscuous mode visibility at the

switch. In other words, special firmware might still be required to make the AP report all the packets back to the switch.

A very important function that a dedicated sensor provides is the ability to analyze events and frames locally and then encapsulate only the relevant alarms and events into an efficient data stream that can be sent back to the central WIPS server. This makes the AirDefense WIPS architecture extremely scalable across distributed locations. Figure 3 illustrates a classic requirement that arises in enterprise WIPS deployments using a healthcare provider as an example. The healthcare provider might have a main hospital, a medical office building and several smaller Doctor's offices where WIPS is required. Smaller offices might have limited internet connectivity – resorting to a 56K dialup connection in several instances. The AirDefense system seamlessly scales into this geographically distributed heterogeneous deployment. Dedicated sensors locally analyze and defend the remote offices and only need less than 3 kbps to communicate with the central server.



**Figure 3:** AirDefense's distributed collaborative intelligence architecture

Even if infrastructure providers had the ability to turn on full promiscuous mode scanning in their 'thin' APs, the bandwidth required to communicate all the packets to the central switch would not be available. Adding a switch/controller in every office location would be cost prohibitive and would defeat the purpose of centralized management that the infrastructure solutions often tout.

Another major drawback of APs behaving as sensors is that under normal mode of operation the APs are forced to expose their identity through regular 802.11 frames that they transmit. Hackers looking at AP transmissions can detect obvious information such as MAC addresses or more subtle characteristics such as vendor, chipset, firmware version, etc. This information can be leveraged for more directed attacks – potentially against the WIPS itself. AirDefense's dedicated sensors work in stealth mode, never revealing their identity on the wireless side. AirDefense sensors are also available in camouflaged form factors looking like smoke detectors blended into the ceiling tiles.

*“The company has only a small Cisco WLAN, but it uses AirDefense to monitor WLAN activity. (AirDefense Enterprise) Version 6.0 lets network managers immediately and remotely disable a rogue device with a single keystroke”*

**Frederick Nwokobia, Senior Engineer, Lehman Brothers Inc.**

WLAN chipset vendors have started offering proprietary extensions for extended range and higher throughput using physical layer modifications. These extensions are readily available in commoditized WLAN hardware. For example, widely available Atheros based APs and client cards offer extended range capabilities at non-standard rates. Extended range is a valuable feature for hackers offering the ability to gain access into a network from a distance. An infrastructure provider that uses a different chipset (e.g., from Broadcom, Conexant, etc.) in its part-time AP/sensors will not be able to decode this traffic.

Finally, third party validation of an infrastructure is always a good practice, especially when it comes to security. Several vulnerabilities in WLAN infrastructure components such as switches and APs have been exposed<sup>1</sup>. The fundamental question to ask is: Can I trust WLAN infrastructure to audit itself for security?

**Conclusion:** Infrastructure APs and sensors are different in their functional requirements. Switching an infrastructure AP to receive only mode does not make it an effective WIPS sensor.

### **Myth #3 – Dedicated WIPS Costs More**

A popular argument used against dedicated sensing solutions for WIPS is that the cost associated with an overlay network of sensors is significantly more. It is important to realize that the Total Cost of Ownership (TCO) of a WIPS system has three basic components – the initial installation cost, the recurring management cost and the periodic maintenance costs. Amortized over the product life cycle, the initial installation cost is a small fraction of the TCO equation. WIPS management costs can be a substantial component of the TCO. The alarms that a WIPS generates have to be monitored and acted upon. An often ignored aspect is the management cost associated with false positives. Many ‘check-box’ WIPS solutions offer simplistic signature based alarms that are prone to false positives. Redundant and context-unaware alarms can add significant management costs that are usually hidden upfront. The AirDefense system uses sophisticated threat index based alarm generation using several detection technologies to minimize false positives and irrelevant alarms.

*“As a large customer of Cisco wireless infrastructure and AirDefense wireless IDS, we saw a significant benefit in bringing together the two products to build a more secure wireless network. The integration of these two major solutions should lower costs and improve security by enabling flexible deployment of IDS capability and will reduce the cost of deployment and on-going management as well as increase the level of security.”*

**JD Fluckiger, Computer Protection Program Manager, Pacific Northwest National Laboratory**

Initial installation cost comparisons between infrastructure integrated and dedicated WIPS can also be misleading. A normalized price to performance metric is required for fair comparison. Metrics

---

<sup>1</sup> [http://www.cisco.com/en/US/products/products\\_security\\_advisories\\_listing.html#advisory](http://www.cisco.com/en/US/products/products_security_advisories_listing.html#advisory)  
<http://www.arubanetworks.com/support/wsirt/alerts/>

such as cost per unique alarm per unit area will clearly show that even with an overlay sensing network the AirDefense dedicated WIPS solution has lower initial cost. The AirDefense system offers over 200 unique alarms compared to 30 offered by the leading infrastructure integrated solution.

Finally, cable installation costs usually exceed the sensor or AP hardware cost. AirDefense offers innovative, standards compliant, completely passive, power and data sharing solutions that allow a single Ethernet cable to service both an AP as well as a dedicated sensor. This patent pending technique can virtually eliminate the overhead cost of running extra cables for each sensor. All things being equal, if an infrastructure WIPS uses dedicated APs for every dedicated sensor that the AirDefense system provides, even the absolute initial installation cost is lower for AirDefense's dedicated WIPS.

**Conclusion:** A well designed dedicated WIPS can have lower TCO than an integrated solution.

## **Myth #4 – WIPS Is All About Static Rogue Wireless Devices On My Wired Network**

While rogue devices are a significant vulnerability in wireless networks, several transient and very dangerous new threats have emerged. Static rogue devices are a passive vulnerability in the network that could potentially get exploited. These devices are usually on all the time and easy to detect. Active attacks, on the contrary, happen quickly and are not restricted to the confines of an enterprise wireless deployment. A classic example of easy and potentially lethal attacks that can happen outside the infrastructure perimeter is Wi-Phishing and Evil Twins. An Evil Twin is an AP offering a wireless connection to the internet pretending to be a trusted wireless network. The unsuspecting user sees the Evil Twin hotspot which looks identical to a legitimate public network that the user logs on to every day. An Evil Twin attack could be used to steal confidential information such as passwords or, more deleteriously, inject Trojans and viruses that can further propagate into the enterprise network through the compromised laptop. The reader is referred to the AirDefense white paper "Wi-Phishing and Evil Twins at Hotspots" for more details.

Mobile worker protection is therefore an integral and indispensable function that the WIPS must offer. AirDefense protects mobile laptops using AirDefense Personal and AirDefense BlueWatch. These client based agents continuously monitor wireless services and activity and enforce policy based alarms and responses.

**Conclusion:** Static rogue devices are a fraction of the wireless threats prevalent today. The WIPS must be able to defend against threats and attacks that are transient and beyond the infrastructure perimeter as well.

## **Myth #5 – Sensing Aside, Both WIPS Architectures Are Created Equal**

When comparing the two WIPS architectures, a popular myth is that the only difference between the systems is dedicated versus time multiplexed scanning. Scanning only provides the eyes and ears into the wireless network. Effectively analyzing these data feeds is what differentiates a true WIPS from 'check-box' solutions. AirDefense uses multiple patent pending technologies such as advanced signature matching, threat index assessment, historical filtering, behavioral correlation, stateful

protocol analysis and policy compliance to provide the brains behind the eyes and ears. Most 'check-box' solutions use simple signature matching which is prone to false positives, redundant alarms and oblivious to day zero attacks.

*“With this (AirDefense Personal) technology, customers can control not only what they have in their own environment, but also what they are doing when they take their laptops out into the world. From an enterprise perspective, that's a technology I think just about every customer would want to have.”*

**John Sieg, Business Security Executive, International Systems Marketing**

In addition to rogue device management, the WIPS system should also provide mobile worker protection, proactive vulnerability assessment, policy monitoring and compliance management, operations troubleshooting along with forensic and incident analysis capabilities. Only AirDefense's dedicated WIPS architecture offers all these functional vectors. As an example, consider the ability to do forensic or incident analysis. An infrastructure integrated solution might run its WIPS on the switch that offers little or no mass storage. Forensic analysis of an incident is difficult if not impossible without a detailed activity log for every device. AirDefense's IntelliCenter provides digitally signed activity and statistical records for all devices in the WLAN on a minute-by-minute basis with the ability to aggregate the data over several years. The reader is referred to the AirDefense Products brochure for additional information on the capabilities that define a true WIPS.

**Conclusion:** Scanning is just one component of the WIPS. The true value of the system lies in its analysis engine.

## **Summary**

WLAN infrastructure vendors are offering integrated WIPS. These solutions provide only 'check-box' functionality. Part-time scanning, typically used by these systems, has significant frequency and time holes. APs and sensors have different functional requirements and integrated solutions that try to use APs as sensors will have several limitations. While it may seem that integrated solutions have lower cost, in fact, the normalized cost as well as the TCO is lower for AirDefense's dedicated WIPS. Finally, WIPS is not just about rogue device management, it also encompasses everything from mobile worker protection to forensic analysis capabilities. AirDefense's dedicated distributed collaborative intelligence based WIPS offers the most comprehensive solution with the highest return on investment.

*“AirDefense is a clear leader in wireless surveillance and offers the best available solution on the market.”*

**Rene Hinsch, Managing Director, AirWire**

**AirDefense**, the market leader in anywhere, anytime wireless security and monitoring, is trusted by more Fortune 500 companies, healthcare organizations and high-security government agencies for enterprise wireless protection than any other wireless security provider. Ranked among *Red Herring's* Top 100 Private Companies in North America, AirDefense products provide the most advanced solutions for rogue wireless detection, policy enforcement and intrusion prevention, both inside and outside an organization's physical locations and wired networks. Common Criteria-certified, AirDefense enterprise-class products scale to support single offices as well as organizations with hundreds of locations around the globe.

**AirDefense Enterprise**, the flagship product, is a wireless intrusion prevention system that monitors the airwaves 24x7 and provides the most advanced solution for rogue detection and mitigation, intrusion detection, policy monitoring and compliance, automated protection, forensic and incident analysis and remote troubleshooting. As a key layer of security, AirDefense Enterprise complements wireless VPNs, encryption and authentication. Using a monitoring architecture of distributed smart sensors and a secure server appliance, the AirDefense Enterprise system provides the most comprehensive detection of all threats and intrusions. Unlike any other solution on the market, AirDefense Enterprise analyzes existing and day zero threats in real time against historical data to more accurately detect threats and anomalous behavior originating inside or outside the organization. The system automatically responds to threats according to appropriate business process and compliance requirements on both wireless and wired networks, making AirDefense Enterprise the industry's most secure and cost-effective wireless intrusion prevention and troubleshooting solution.

**AirDefense Personal**, the industry's first end-point security solution, provides uninterrupted protection for all mobile employees and their enterprise wireless assets, regardless of location – at work, home, airports or other wireless hotspots. Policy profiles are defined centrally on AirDefense Enterprise and automatically downloaded to each mobile user. If threats are discovered, AirDefense Personal notifies the user and sends the alerts to AirDefense Enterprise for central reporting and notification. This unique solution allows the network administrator to enforce corporate policies and provide complete protection for the mobile workforce, regardless of location.

The **AirDefense InSite Suite** is a collection of powerful tools available today for network architects to design, install, maintain and troubleshoot wireless networks. Tools included in the suite are: **AirDefense Mobile**, complementary to AirDefense Enterprise allows administrators to perform wireless assessments, security audits, locate and manage rogues. **AirDefense Architect** provides complete design and 3D RF simulation of wireless LANs based on building-specific environments. **AirDefense Survey** provides real-time, in-the-field measurements of Wi-Fi RF environments for site-specific surveys.

For more information or feedback on this white paper, please contact [info@airdefense.net](mailto:info@airdefense.net) or call us at 770.663.8115. **All trademarks are the property of their respective owners.**