

Effective WLAN Management With Distributed RF Sensors: A White paper

Monitor your RF spectrum 24x7 for intrusions and other potential threats using distributed RF sensors.

This paper examines the importance and benefits of distributed RF sensors in managing wireless networks and describes the critical role these sensors play in WLAN management software.

Dev Anand
devanand@adventnet.com
Analyst - Wireless Solutions
AdventNet, Inc.

Table of contents

RF is inherently very dynamic	3
Securing RF needs right set of tools	3
Common approach to RF management.....	3
AirTight security with distributed RF sensors	5
Commonly available sensors	7
Role of sensors in WLAN management	7

RF is inherently very dynamic

RF technology is very dynamic in nature as it changes in response to the real-world conditions. Noise, interference, and increased traffic load, signal attenuation – these are some of the factors that can cause RF topology to change from one moment to the next. For most network managers RF technology has remained something that is always *in the air*.

Securing RF needs right set of tools

When network traffic is broadcast over an open medium, such as air, the challenge of securing the critical corporate data increases by many folds. Network managers are constantly trying to secure corporate wireless networks from unauthorized activity such as unauthorized rogue access points and intrusions, denial of service attacks, and RF jamming attacks. Monitoring the RF requires special set of tools that have the ability to sniff the air and pull out the information from those wireless packets.

Common approach to RF management

The three common ways in which RF can be monitored are:

- Using mobile users' laptops and/or access points as background sensors
- Using dedicated comp as sensor
- Using distributed dedicated hardware RF sensors

Mobile laptops as background sensors



In this model either the mobile users' laptops or the access points themselves can be used as RF sensors to sniff the air packets and forward the packets to the central management software. Though this is a cost effective solution, as it uses the existing devices to do the job, this often does not derive the desired results. For the very basic reason that the RF sensing is not a dedicated activity and is done only as a background activity, meaning when the user does not utilize them.

Dedicated comp as sensor



In this model a dedicated system is used as a dedicated sensor. Though this model is slightly costlier than the earlier one, as it involves some investment being tied down permanently, it works better than the earlier model for one reason that its location, and thus the covering area, is fixed.

Dedicated and distributed RF sensors:



In this model hardware RF sensors are deployed over the corporate premise offering 24x7 monitoring. This model offers the most desired results in terms of the security as it covers the whole enterprise with a 24x7 dedicated sensing. Moreover the first two models, background sensors and comp, have a dependency on the type of PCMCIA card and driver used. Some incompatibility issues with these cards/drives with the management software may result in deteriorated quality.

Pick your choice: Low cost or high security

Model	Cost	Security
Background sensors	Very Low	Low
Dedicated PCs	Low	Medium

Dedicated RF sensors	High	High
----------------------	------	------

Advantages/ Disadvantages of the three models

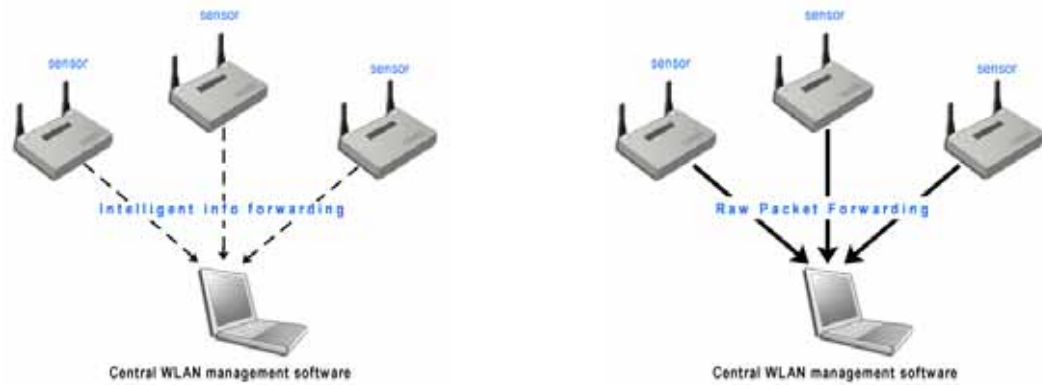
Model	Advantages	Disadvantages
Background sensors	Very low cost	Sensing is done only when the device idle. Card/Driver dependency.
Dedicated PCs	Low cost	Card/Driver dependency.
Dedicated RF sensors	24x7 monitoring High coverage High security	High cost

AirTight security with distributed RF sensors

In spite of being costly, RF sensors are now being widely accepted by enterprises for their capacity to offer highest levels of security. Clubbed with smart WLAN management software these RF sensors can offer literally AirTight Security to corporate wireless networks.

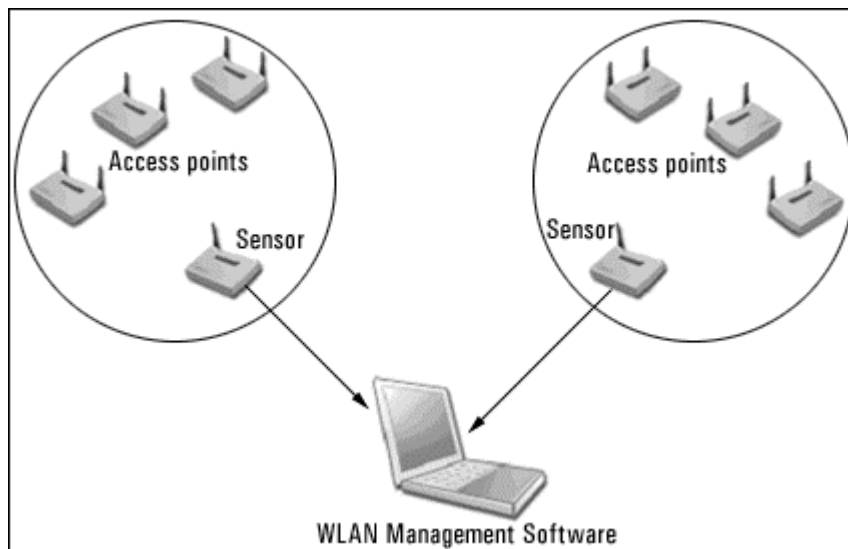
Most sensors in the market have the capability to operate in two modes – dumb packet capture and forwarding and intelligent correlation and information forwarding. The basic difference between the two modes is the amount of data that is dumped onto your network.

In the first mode, dumb forwarding, the entire RF data that is on the air is put into your wired network as it is forwarded to the central management software. This is undesirable in most enterprise scenario as it threatens to choke the network. In the second mode, intelligent forwarding, the sensor parses the packets and passes only the key information such as signal strength, signal to noise ratio, operating channel etc.



The decision on which mode to operate the sensor depends on whether it is enough to get the key info or is something else is required. The answer varies from enterprise to enterprise depending on the software they choose. Some software have additional algorithms built into an intermittent component called aggregator (or software sensor in some cases) which collects the raw packets, parses them, applies the algorithms and finds few more details which are not available in the sensor as such. In such cases the enterprises are advised to hookup the aggregators and the sensors through a dedicated hub so that the main network is not overloaded.

Distributed RF sensor architecture:



Commonly available sensors

Today, there are quite a good number of players offering hardware RF sensors. Some of the known names in the market include AirMagnet, AirDefence, Network Chemistry, and WildPackets. These hardware sensors form the foundation for most of their higher applications such as WLAN analyzers and management applications.

Company	Hardware Sensor
AirMagnet	AirMagnet Hardware Sensor
AirDefense	AirDefense Sensor
Wild Packets	RFGrabber
Network Chemistry	RFProtect Sensor

Role of sensors in WLAN management

WLAN management without sniffing the air is a false claim. It is impossible to manage WLANs by depending purely on the wired side information. RF sensors bring in the following functionality to the management software:

- Intrusion detection
- Denial-of-service attack detection
- Vulnerability assessment

Intrusion detection

The term rogue is probably more popular than any other buzzword in the WLAN lexicon. RF sensors primarily help in detecting these rogues and pass on that information to the WLAN management software. On receipt of such information, the software would alert the operator using alarms or using notification mechanisms such as e-mail or SMS.

DoS attack detection

Attacks are more common in Wireless LANs than in the wired world. The flexibility that you can stay away from the network but still be able to lock it down motivates (!) people to discover newer attacks. RF sensors can help in detecting such attacks and can pass on such critical information to the software. Some of the common DoS attacks are RF jamming attack, FataJack attack, Duration attack, Authentication storm, De-authentication storm, Association storm, Disassociation storm etc.

Vulnerability assessment

Prevention is better than cure, especially when the cure is too costly as in case of WLAN networks. A small vulnerability in your access point can punch a BIG hole in your corporate security. RF sensors help in identifying these tiny vulnerabilities. Some of the common vulnerabilities in access points are AP broadcasting the SSID, Default SSID is in use, Adhoc network in operation, Weak WEP IVs in use, Net Bios traffic detected etc.

Wireless monitoring

Few RF sensors have the capability to monitor key network parameters such as signal strengths, errors, associations, and traffic details. The WLAN management software can then graphically represent these data.