ManageEngine UK Distributor

Summary

Rogue devices can potentially disrupt enterprise wireless networks and can sometimes cause irrevocable damage to the company. Enterprises could unknowingly open up their Intellectual Property (IP) to outsiders and competitors through a poorly configured or unauthorized wireless device. IT managers deploying Wireless LANs should effectively detect and block wireless access points and client stations automatically and in real-time.

This paper explains what rogues are, how they create a business risk, and how to effectively:

- Detect and Block Rogue Access Points
- Detect and Block Rogue Client Stations

Enterprises today, irrespective of their size and business model agree upon the importance of detecting and blocking rogue devices. But no single solution fits them all. Enterprises choose their tool based on numerous factors including their wireless security need, budget, existing tools, future wireless plans etc. This paper also presents a comparison of various rogue detection tools. This compilation would give them the right inputs to decide on the solution that fits them the best.

ManageEngine White Paper:

Wireless Network Rogue Access Point Detection & Blocking

Rogue Types and Associated Risks

With the wide spread adoption of Wireless LANs today, wireless signals are available everywhere. Some cities have complete citywide WiFi coverage enabling mobile users to get connected from anywhere in the city. Multi-tenant apartments are fully covered by wireless service providers. Hospitals and universities run huge wireless deployments spanning hundreds or thousands of access points. Large-scale enterprises too have started adopting Wireless LANs in big way.

All these developments tell us that any wireless deployment today, including yours, is not alone. Your WLAN is just a part of a bigger global phenomenon and in most cases will receive signals that are alien to your organization. Furthermore, visitors to your organization and your own employees carry several wireless devices in and out of your organization daily making round-the-clock wireless device scrutiny a mandatory job.

In such a closely knitted environment it is hard to trust any device fully. A wireless device beaming signals into your premises could be either a harmless neighbour AP or an attacker operated device trying to steal proprietary information from your WLAN. Moreover a poorly configured AP or a client can either open up access to outsiders or get associated with attacker/attacker APs accidentally. Some of the common examples of rogues are illustrated in figure 1.

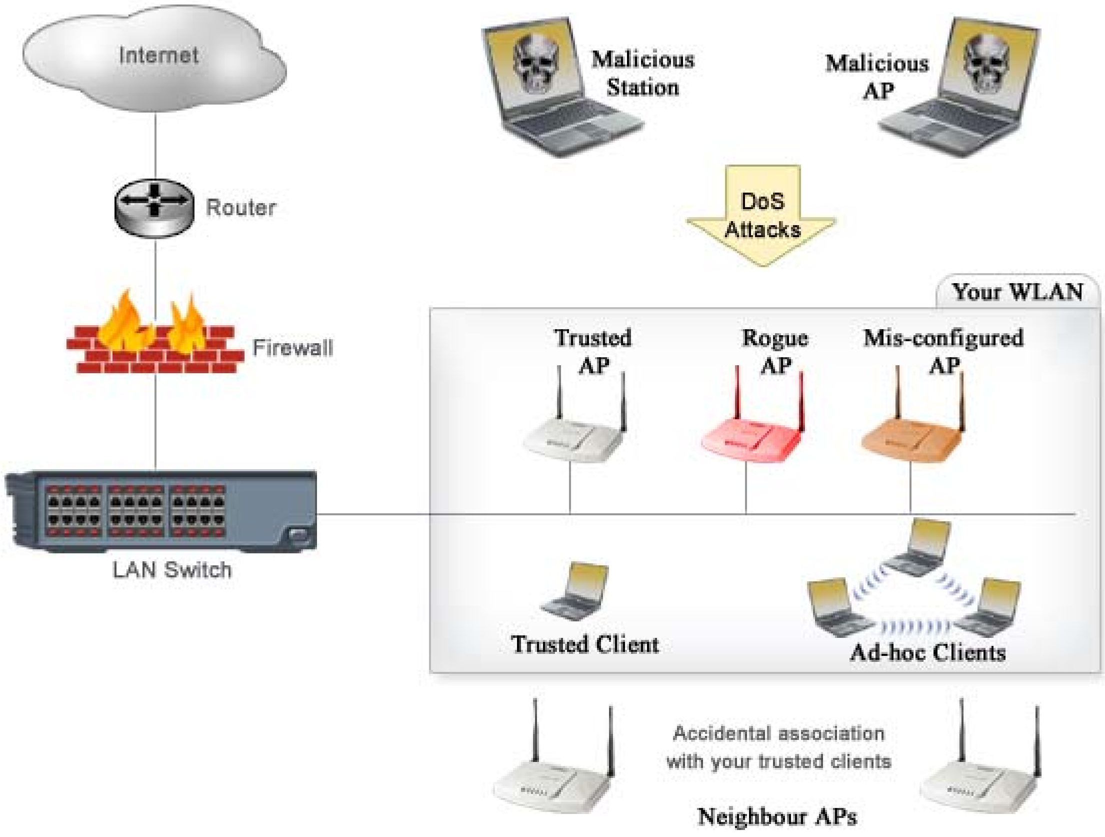


Figure 1: Rogue Devices and Associated Threats

Though the term ‘Rogue’ is often referred to devices that are external to an organization, for clarity, in this paper the term would refer to any unauthorized device irrespective of its real intent. For example:

Employee installed unauthorized Access Points: Driven by the convenience of Wireless home networking some employees plug cheap Small Office Home Office (SOHO) grade access points to corporate LAN. This unintentional act by the novice users punches a big hole on enterprise security exposing critical data to outsiders. The cheap AP may not follow enterprise standard deployment procedures thus compromising security on the wireless and wired network. Visitors inside your building and hackers outside your building can connect to such unauthorized APs to steal bandwidth, send objectionable content to others, retrieve confidential data, attack company assets, or use your network to attack others.

Mis-configured Access Points: Sometimes an authorized access point could suddenly turn into a rogue device due to a minor configuration flaw. Change in Service Set Identifier (SSID), authentication settings, encryption settings etc., should be taken seriously as they could enable unauthorized associations if not configured properly. For example, in open mode authentication any wireless client device in state1 (unauthenticated & unassociated) can send authentication requests to an AP and on successful authentication would move to state2 (authenticated but unassociated). If an AP doesn't validate the client properly due to a configuration flaw, an attacker can send lot of such authentication requests, overflow the AP's client-association-table, and make it reject access to other clients including the legitimate ones.

Attacker Access Points: 802.11 clients automatically choose the best available AP nearby and connect with them. For example, Windows XP connects automatically to the best connection possible in the vicinity. Due to this behaviour, authorized clients of one organization can connect to Access points from the neighbouring organization. Though the neighbours APs have not intentionally lured the client, these associations can expose sensitive data. Ad-hoc devices: Wireless clients can communicate among themselves without requiring a LAN bridging device such as Access Point.

Though such devices can essentially share data among themselves, they pose significant threat to the enterprise as they lack the necessary security measures such as 802.1x user authentication and the dynamic key encryption. As a result, ad-hoc networks risk-exposing data in the air (as data is not encrypted). In addition, weak authentication may allow unauthorized devices to associate. If the ad-hoc mode clients are also connected to the wired network, the entire enterprise wired network is at risk.

Unauthorized Access Points: Enterprises can set polices on what constitutes an authorized AP. The basic one is MAC addressed based filtering. Enterprises can pre-configure the list of authorized devices' MAC and identification of any other device outside the MAC list will signify the presence of a rogue device. Also if an organization standardizes on Cisco Access Points then AP from any other vendor (plugged into the corporate LAN) can be deemed rogue. Similarly enterprises can set various policies including SSID, Radio Media Type, and Channel. Whenever a new access point is discovered in the network that falls outside the pre configured authorized LIST, it can be assumed to be a rogue AP.

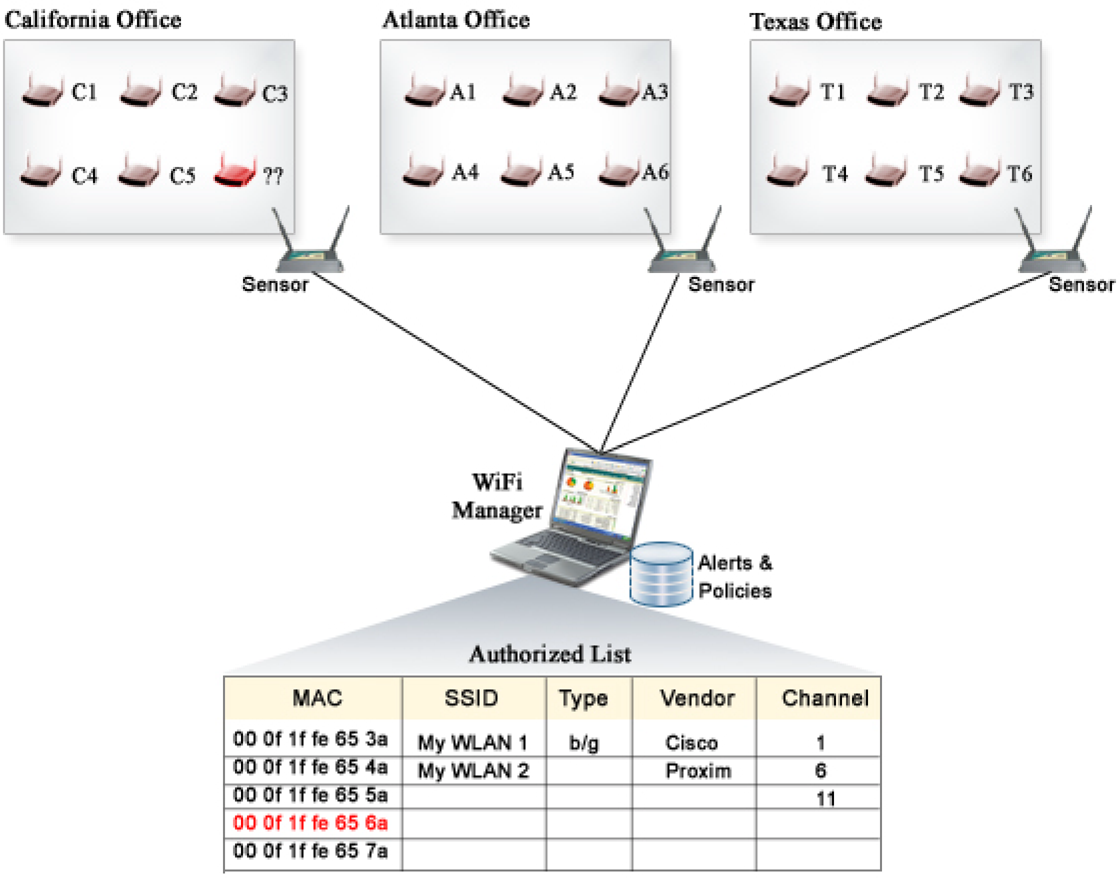
Attacker operated Access Points: Wireless LANs are prone to numerous attacks. Furthermore, freely available open-source attack tools ease the job of attackers. Attackers can install Access Points with the same ESSID as the authorized AP. Clients receiving stronger signal from the attacker operated AP would then attract legitimate clients to associate with it. The AP can then launch a man-in-the-middle attack. Attacker operated clients: Using a wireless enabled laptop and couple of tools an attacker can successfully disrupt wireless service in networks few feat away. Most such denial-of-service attacks aim at exhausting AP resources such as the client-association-table.

In short, a rogue device is any untrusted or unknown device running in your WLAN. Detecting these devices is the first step to efficiently defend your WLAN from rogues.

Rogue Detection and Blocking

Rogue detection and blocking is a continuous process involving at least three components:

- A dedicated piece of hardware probe/sensor to monitor the air and identify network behaviour
- A central IDS engine that gathers inputs from many such probes/sensors and helps in pinpointing a device as rogue.
- A network management software that can talk to the wired network, identify the switch port to which the rogue AP is connected and shutdown the port.



MAC	SSID	Type	Vendor	Channel
00 0f 1f fe 65 3a	My WLAN 1	b/g	Cisco	1
00 0f 1f fe 65 4a	My WLAN 2		Proxim	6
00 0f 1f fe 65 5a				11
00 0f 1f fe 65 6a				
00 0f 1f fe 65 7a				

Figure 2: Multi-site remote network management using distributed RF sensors and centralized IDS/network management server

Each component in the above diagram performs different WLAN functions but work in unison to detect/ analyse and block rogue devices.

Rogue AP detection

Rogue detection is a two step process starting with discovering the presence of an Access Point in the network and then proceeding to identify whether it is a rogue or not. Some of the very commonly used techniques for AP discovery are:

- RF scanning
- AP scanning
- Using wired side inputs

RF scanning: Most WLAN IDS vendors follow this technique. Re-purposed access points that do only packet capture and analysis (a.k.a RF sensors) will be plugged all over the wired network. These sensors will be quick to detect any wireless device operating in the area and can alert the WLAN administrator. But the draw back of these sensors is the possibility of dead zones, which are not covered by the sensors. If a rogue Access Point finds its place in any of these dead zones, it might go unnoticed till more sensors are added.

AP Scanning: Few Access Point vendors have this functionality of detecting neighbouring Access Points. If you deploy such Access Points in your WLAN it will automatically discover APs operating in the nearby area and expose the data through its web interface as well as its MIBs. Though it is a very useful the ability of the AP to scan neighbouring devices is limited to a very short range. Rogue APs operating outside this coverage area will go unnoticed. Moreover this works only for those who deploy APs with such functionality.

Wired Side Inputs: Most network management software use this technique to discover Access Points. This software use multiple protocols to detect devices connected in the LAN, including SNMP, Telnet, CDP (Cisco Discovery Protocol – specific to Cisco devices) etc. This approach is very reliable and proven as it can detect an AP anywhere in the LAN irrespective of its physical location. Moreover, wireless NMSs can not only discover the AP but also constantly monitor it for health and availability.

The bandwidth utilization of the AP over a period of time can be obtained and plotted in a graphical format. For ease of troubleshooting the operator can set thresholds on various AP parameters to get notified prior to the occurrence of a fault. The limitation with this method is that any AP that doesn't support SNMP/Telnet etc. will go unnoticed by the network management software.

AP Discovery Method	WLAN IDS Systems	WLAN NMS
RF Scan	✓	✗
AP Scan	✗	✓
Wired Inputs	✗	✓

Once an AP is discovered, the next step is to identify whether it is a rogue or not. One way to do this is to use pre-configured authorized list of APs. Any newly detected AP that falls outside the authorized list would be tagged rogue. Some of the different ways in which IT managers can populate the authorized list are:

- Authorized MAC
- Authorized SSID
- Authorized Vendor
- Authorized Media Type
- Authorized Channel

Authorized MAC: IT administrators can import ACL settings to WiFi Manager or type in the MAC address of authorized Access Points in the network. This enables the rogue detection tool to alert WLAN administrators whenever AP with a different MAC is detected.

Authorized SSIDs: Enterprises would in most cases standardize on the authorized SSIDs that needs to be used. These SSIDs can be fed to the rogue detection tool so that it alerts WLAN administrators whenever an AP with a different SSID is detected.

Authorized Vendor: Many enterprises standardize their WLAN gear and prefer to add only those vendor devices as they grow. This enables the rogue detection tool to alert WLAN administrators whenever AP from a vendor other than the one standardized is detected.

Authorized Radio Media Type: Enterprises sometimes standardize on 802.11 a,b,g, or bg Access Points. This enables the rogue detection tool to alert WLAN administrators whenever AP with different radio media type is detected.

Authorized Channel: Sometimes enterprises may want their APs to operate on select channels. This enables the rogue detection tool to alert WLAN administrators whenever AP operating in a different channel is detected.

Rogue AP blocking

Once a rogue AP is discovered the next immediate step is to block the AP from the network so that the authorized clients don't associate with it. There are two ways of blocking the rogue APs.

1. Tit for Tat: Launch a Denial-of-service (DoS) attack on the rogue AP and make it deny wireless service to any new client.
2. Pull it out of the network: Either the WLAN administrator can manually locate the AP and pull it physically off the LAN OR block the switch port to which the AP is connected.

Launching a DoS attack on the rogue

AP Most Wireless IDS vendors follow this practice. This is kind of using offence for defence. Once a rogue AP is detected the WLAN administrator can use the sensor to launch a DoS attack on it by sending numerous disassociation packets.

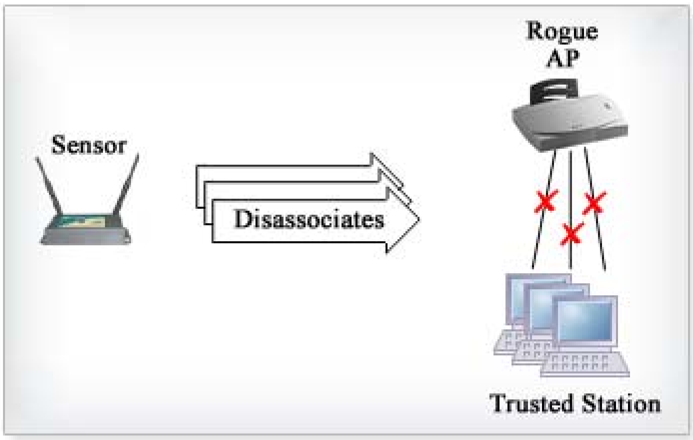


Figure3: Rogue blocking by sending disassociation packets

How disassociation attack works?

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and APs implement such a state machine (refer illustration below) based on the IEEE standard. A successfully associated client station stays in State 3 in order to continue wireless communication. A client station in State 1 and State 2 cannot participate in the WLAN data communication process until it is authenticated and associated. IEEE 802.11 also defines two authentication services: Open System Authentication and Shared Key Authentication. Wireless clients go through one of the two-authentication process to associate with an AP.

Disassociation Flood Attack is a form of denial of service attacks that forces a client to the unassociated/authenticated state (State 2) by spoofing disassociation frames from the AP to a client. Typically, client stations would re-associate to regain service until the attacker sends another disassociation frame. An attacker would repeatedly spoof the disassociation frames to keep the client out of service.

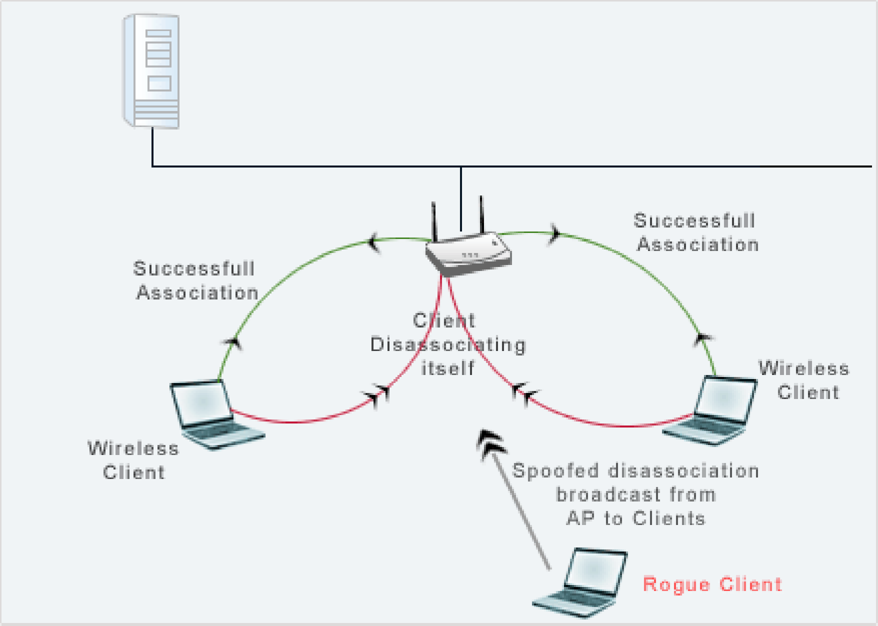


Figure 4: Disassociation Attack Model Diagram

Pulling an AP off the LAN

This is manual work. The administrator can walk up to the rogue AP and pull it off the LAN. In many cases it would be an over enthusiastic employee who has installed the AP for wireless communication.

Blocking the switch port

Wireless network management software offers this functionality. Once the rogue AP is detected the software will look for the rogue AP’s MAC address in all the switches connected in the LAN. The port at which the MAC is connected can then be blocked for any LAN traffic. This would automatically prevent the clients connected to the AP from dropping the connection and get associated to the nearest AP. This is a very effective technique.

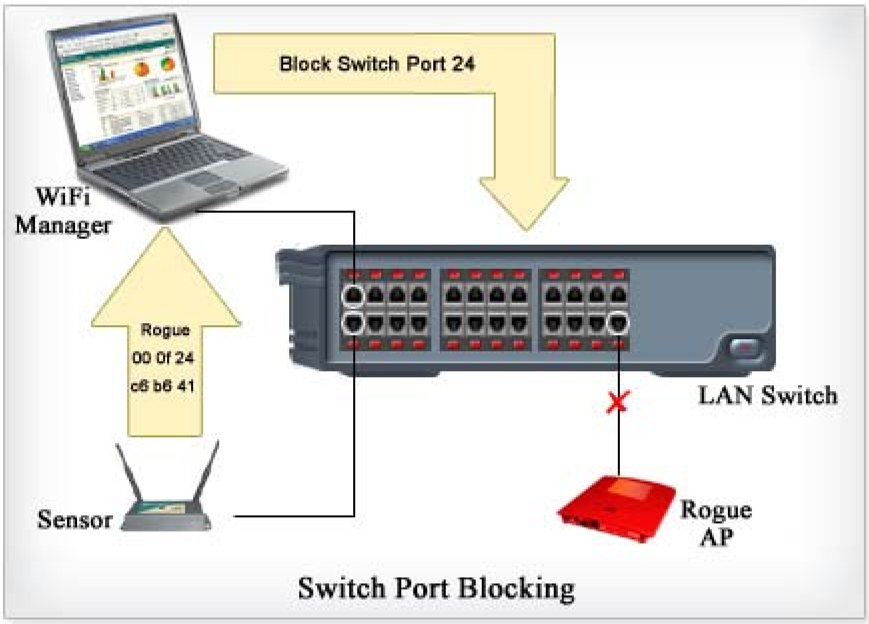


Figure 5: Switch Port Blocking

Rogue client detection

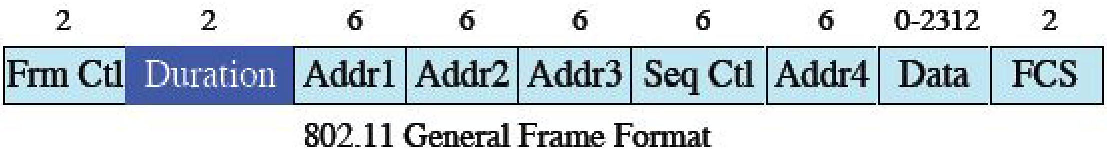
Rogue clients are malicious wireless client devices that either try to gain illegitimate access to your WLAN or try to disrupt normal wireless service by launching attacks. There are numerous ready-to-launch wireless attack tools freely available on the net. Many of them are open sourced and work pretty well with most Wireless client cards. This turns any curious mind to professional hacker in minutes. Many do it simply for the pleasure of being able to disturb someone remotely. All these developments force WLAN administrators to give a second look at any wireless client that is misbehaving. Some of the behaviours that could potentially spell danger are:

Client sending frames with prolonged duration

When a client sends frames with prolonged duration, other clients in the network have to wait till the specified duration to use the RF medium. If the client continuously sends frames with such high duration, then it can prevent other clients from using RF medium and remain unassociated forever.

How duration attack works?

WLAN devices perform virtual carrier sensing prior to using the RF medium. Carrier sense minimizes the likelihood of two devices transmitting simultaneously. Wireless nodes reserve the right to use the radio channel for the duration specified in the frame. A general 802.11 frame format would look similar to what is shown below.



2	2	6	6	6	6	6	0-2312	2
Frm Ctl	Duration	Addr1	Addr2	Addr3	Seq Ctl	Addr4	Data	FCS

802.11 General Frame Format

Figure 6: General format of 802.11 packet

The duration value in the frame indicates the duration in milliseconds for which the channel is reserved. The Network Allocation Vector (NAV) stores this duration information and is traced for every node. The basic rule is that any node can transmit only if the NAV reaches zero or in other words no one has reserved the channel at that time. Attackers take advantage of the NAV. An attacker can send frames with huge duration values. This would force other nodes in the range to wait till the value reaches zero. If the attacker is successful in sending continuous packets with huge durations, then it prevents other nodes from operating for a long time and thereby denying service.

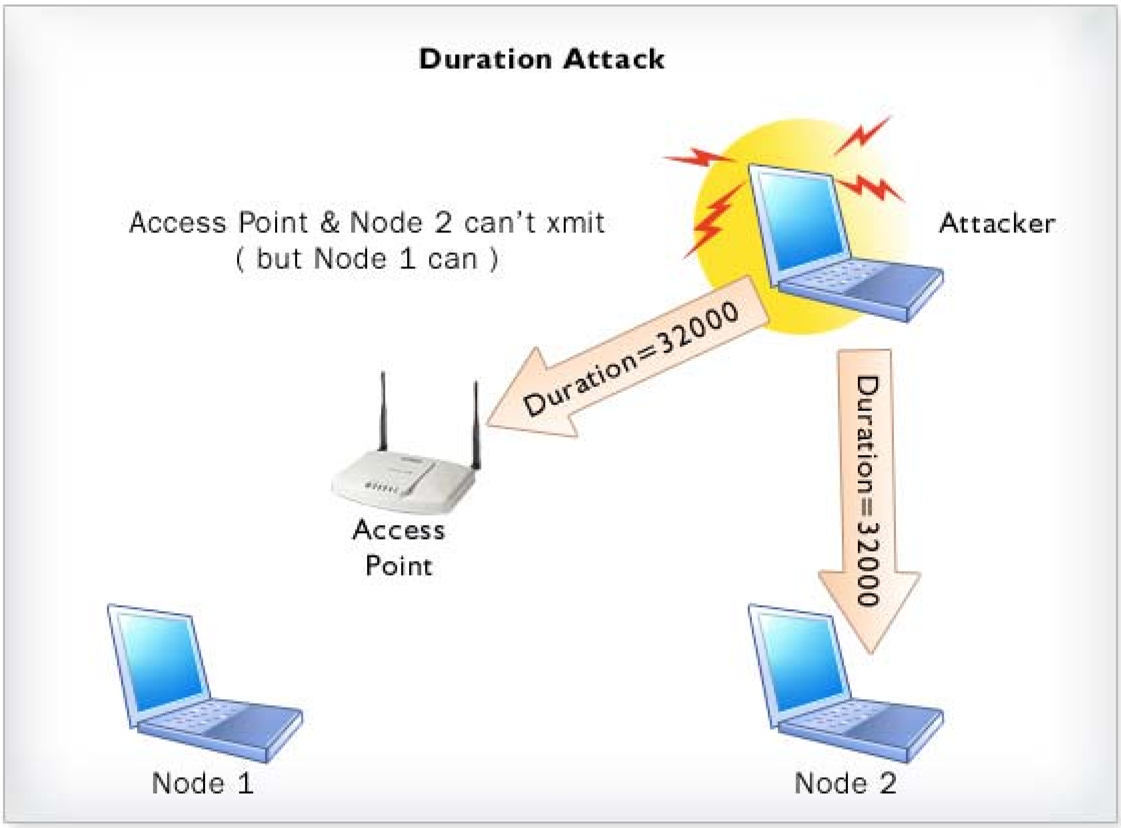


Figure 7: Rogue client launching a duration attack on WLAN

Unassociated client sending packets

A client can decide not to connect to the Access Point but still send out wireless packets (mostly broadcasts, associations/authentication requests). Typically, this behaviour can be attributed to malicious clients or attackers who want to gain knowledge on your wireless network. When normal authentication procedures deny access to such attackers, they choose to inject forged packets into the wireless network by staying unconnected.

Device probing for 'any' SSID

Access points if not configured properly allow clients to connect with 'any' SSID. This is a vulnerability, which the WLAN administrator should identify and stop beforehand. If a client tries to connect using 'any' SSID it would most probably be a rogue client.

Unauthorized clients

Rogue clients can also be detected by pre-configuring the authorized list of clients in the network. Some of the different ways in which IT managers can populate this authorized list are:

Authorized MAC: WLAN administrators can import the list of authorized clients' MAC address into WiFi Manager. This enables WiFi Manager to trigger an alarm whenever it sees a client with a different MAC address.

Authorized vendor: If an enterprise standardizes on vendor for client adaptor, then WLAN administrators can configure WiFi Manger to trigger alarm if it sees adapters from a different vendor.

Rogue client blocking

Once a rogue client is detected, WLAN administrator should shut down the client from the network. Most common method of keeping rogue clients away is by configuring their MAC address in the Access Point's Access Control List (ACL). ACL determines whether to deny or allow a client to connect to the Access Point. WLAN administrators can specify the rogue client's MAC address in the ACL of all authorized Access Points to keep the rogue client off the network for ever.

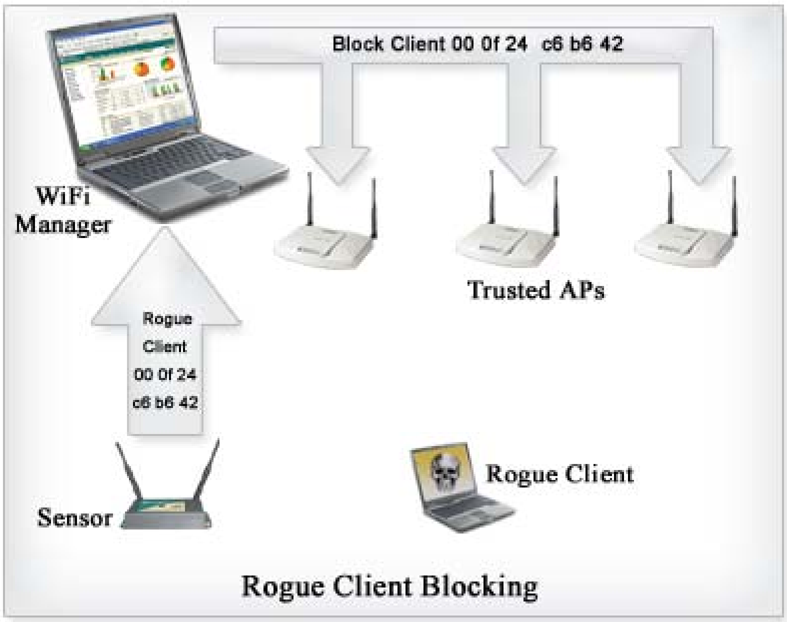


Figure 8: Detecting and blocking rogue client using WiFi Manager

How WiFi Manager can help

WiFi Manager is a combined WLAN security and management software for 802.11 a/b/g networks. It presents a Web-based view of all wireless networks operating in your building, access points available inside each network, status of those access points, channel at which they operate, mobile clients connected to them and their signal strength/ noise values, and association history. You can configure/ upgrade firmware of access points using this software. And once integrated with RF sensors, WiFi Manager becomes a full-fledged wireless IDS system detecting more than 120 different types of intrusions, denial-of-service attacks, and vulnerabilities in the WLAN.

Figure 9: WiFi Manager Screenshot

AP discovery using WiFi Manager

WiFi Manager has the unique advantage of using all methods of AP discovery, making the AP discovery process really foolproof.

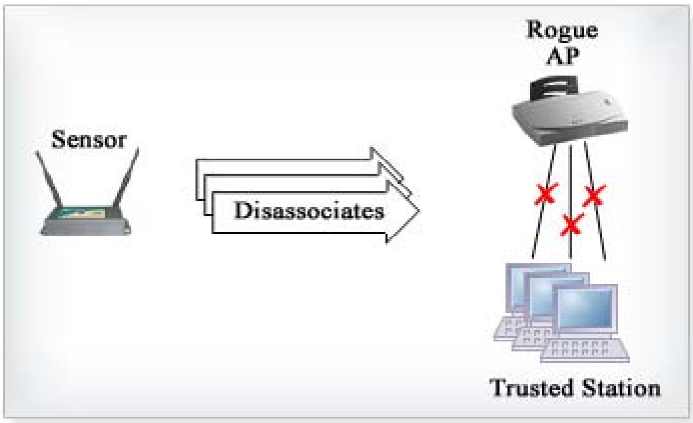
AP Discovery Method	WLAN IDS Systems	WLAN NMS	WiFi Manager
RF Scan	✓	✗	✓
AP Scan	✗	✓	✓
Wired Inputs	✗	✓	✓

Rogue AP detection using WiFi Manager

WiFi Manager uses multiple rogue detection techniques including the use of authorized lists. WLAN administrators can pre configure the authorized lists or can make use of the ‘Mark As Trusted’ option in WiFi Manager to add APs to the authorized list.

Rogue AP blocking using WiFi Manager

If the AP is found to be rogue, then it can be blocked from the network using the Switch Port Blocking option in WiFi Manager. Higher versions of the RF sensor support launching dissociation attack on the APs.



Rogue Detection and Blocking Tools - a Comparison

There are about a bunch of them offering the rogue detection and blocking capability to enterprises. Tools are available at all price points with some very useful but limited functionality open source contributions. All these can be clubbed into different categories as give below.

- Opensource WLAN Discovery Tools
- Wireless IDS Systems
- Wireless Network Management Software
- Integrated WLAN Security and Management Software

Open source WLAN discovery tools

Tools that are worth mentioning are Wellenreiter, netstumbler, and Kismet. They have been around for quite some time and can do a decent job of detecting all Wireless Access Points in the network. Can be a good starting point to detecting rogues. But they lack rogue detection algorithms and/or the ability to block rogue APs.

Wireless IDS systems

Leading wireless IDS systems include AirMagnet enterprise and AirDefense enterprise. Both solutions use distributed RF sensors for AP discovery and rogue detection. Help blocking the rogue Access Points by sending out disassociation packets. Switch port blocking can be done using third party NMS systems.

Wireless Network Management Software

Available options include Wavelink Mobile Manager and Airwave Management Platform (AMP). Both solutions depend purely on wired side inputs for AP detection and both support IDS sensors from AirMagnet. Wavelink requires proprietary agents (software) to be distributed all over the network for data collection whereas AMP doesn’t require such agents.

Integrated Security and Management Software

WiFi Manager is an integrated Wireless IDS and Wireless Network Management software. It clubs the best of Wireless IDS tools and the Wireless Network Management tools.

Comparison matrix

The comparison is intended only for informational purposes. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, AdventNet makes no claim, promise or guarantee about the completeness, accuracy or adequacy of information and expressly disclaims liability for errors or omissions in the contents.

	Wireless IDS	Wireless NMS	WiFi Manager
RF Scan	✓	✗	✓
AP Scan	✗	✓	✓
Wired inputs	✗	✓	✓
Rogue annihilation using disassociation attack	✓	✗	✓
Switch port blocking	✗	✓	✓
AP Configuration	✗	✓	✓
AP Firmware upgrade	✗	✓	✓

Summary

For more details on ManageEngine WiFi Manager and how it can help your wireless network security, please contact

Networks Unlimited on +44 (0)1798 873001 at sales@manageengine.co.uk or our website www.manageengine.co.uk