Ad Hocs may also prove useful against unauthorized Soft APs, such as IT-managed client settings and WIPS.

7. Misbehaving Clients: Clients that form an unauthorized Wi-Fi connection of any type, whether it may be accidentally or intentionally put themselves and the corporate data at risk. Some enterprises sue a group policy to configure authorized Wi-Fi connections and prevent end-user changes. Others use a host resident agents and or WIPS to monitor Wi-Fi client activity and disconnect high risk connections. However the many businesses still depends on the end user to connect only to known authorized wireless access point.

Given ubiquitous deployment, longer reach, and broader consumer electronics integration, accidental or inappropriate Wi-Fi connections have never been easier. If you haven't already taken steps to stop Wi-Fi client misbehaviour, start now.

8. Endpoint Attacks: In today's world over the air encryption and network edge security have drastically improved, attacker have refocused their attention on the Wi-Fi endpoints. We can find the numerous exploits which have been published to take advantage of buggy Wi-Fi drivers like buffer overflow attack which execute arbitrary commands, automated attacking tools like metasploit can be able to launch Wi-Fi endpoint exploits with an ease.

Although vendors do patch them once they have been discovered, the Wi-Fi updates are not distributed automatically with operation system updates. To protect your workforce, track Wi-Fi endpoint vulnerabilities and keep your Wi-Fi drivers up-to-date.