**FIGURE 14.8** Sensor placement

If an integrated WIDS/WIPS solution is deployed, all access points are deployed as part-time sensors. Once again, it is strongly recommended to deploy some full-time sensors with an integrated solution. When WLAN security monitoring is an extremely high priority and cost is not an issue, the more sensor devices the better. WIDS/WIPS deployments at military bases often follow a ratio of one sensor for every two APs or may even deploy sensors with a 1:1 ratio.

**Proprietary WIPS**

As you have already learned, most WIDS vendors prefer to call their products a wireless intrusion prevention system (WIPS). The reason that they refer to their products as prevention systems is that they are all capable of mitigating attacks from rogue access points and rogue clients. Currently, the main attack mitigated by a WIPS is rogue devices. In the future, other wireless attacks might be mitigated as well. In the meantime, several WIPS vendors are using proprietary methods to mitigate some WLAN attacks.
As attacks become more sophisticated and the number of client devices explodes due to bring your own device (BYOD) networks and the Internet of Things (IoT), intrusion detection and prevention as we have known it must change.

How can we deal with these new threats? One new vendor has an unique approach to this growing security problem. They are 802Secure. Using 802Secure’s secure wireless risk management, SWARM, Intelligence, administrators and security professionals for the first time can view active wireless attacks on a benign network, while protecting the brand and production network. 802Secure meets the needs of recording and analyzing new advanced attack techniques being implemented by hackers. Their answer is the Wireless Risk Audit Tool (WRAT) which is an end-to-end, proactive, and secure solution that helps defend organizations from all manners of wireless attacks (Wi-Fi, Bluetooth, ZigBee, RFID, NFC, and licensed band). See Figure 14.9 for a look at the innovative hardware.

**Figure 14.9** WRAT hardware

Unlike, traditional Intrusion Detection Systems (IDS) which try to map attacks against known attacks or performance signatures, which have a limited set of signatures for the new wave of IoT attacks and fall short of detecting new attack vectors created by IoT, i.e., infiltration via 2.4Ghz, exfiltration via 900Mhz, the 802Secure Cloud Service leverages Big Data Analytics to automatically cross-reference prerecorded attacks, giving valuable insight and resources to stop new attacks from penetrating your network. The WRAT consists of low-cost on premises hardware connected to a cloud-based analytics and reporting platform. The WRAT reports out of band to the analytics and reporting platform over an LTE connection. More impressive than the out of band reporting is how 802Secure deals with threats. For example, their Deceptive Networking monitors the 802.11 RF spectrum including a/b/g/n/ac. If a breach of policy occurs or a wireless vulnerability is being exploited AirDecoy™ can divert suspicious traffic to a virtual decoy network in the 802Secure cloud for further wireless threat intelligence gathering. Each deceptive network or decoy environment deployed will be unique to the each customer. The key to the
deception technology used by 802Secure is a diverse ecosystem of tools that prevent adversaries from being able to map out an attack. This provides visibility into advanced Wi-Fi and IoT attacks. 802Secure’s DITCH cloud service (Distributed Intelligence Threat Cloud Heuristics) automatically cross-references prerecorded attacks giving valuable insight and resources to stop new attacks from penetrating networks. The system learns the methods used by an attacker. If they move to another location, spoof their MAC address or change the devices they have been using, the system will still recognize their style and let you know that the same attacker(s) are now in another location. The Incident Audit Analysis or the Who, What, Where, When, and How data is collected by the AirDecoys and presented within the 802Secure DITCH cloud, which provides full drill down capabilities with historical trending within an easy to use GUI interface (see Figure 14.10). As the landscape of attacks keeps growing and changing, security professionals must increase the size of and improve the tools within their detection and mitigation arsenal.

**FIGURE 14.10**  802Secure Command Center

---

**Device Classification**

Although the upper-layer payload of 802.11 data frames is usually encrypted, the Layer 2 information remains exposed to allow for MAC layer communications to occur. All Layer 2 information is captured and analyzed by WIDS/WIPS solutions. Any 802.11-based