Can Wireless LAN Denial of Service Attacks Be Prevented?
Understanding WLAN DoS Vulnerabilities & Practical Countermeasures
Executive Summary

Wireless communications that use a shared Radio Frequency (RF) medium are often vulnerable to Denial of Service (DoS) attacks. Wireless Local Area Networks (WLAN) based on the IEEE 802.11 standard are no exception. In addition to brute force Physical (PHY) layer jamming attacks, WLANs are susceptible to various Media Access Control (MAC) vulnerabilities that can lead to DoS. This paper provides an overview of various WLAN DoS scenarios and available countermeasures to detect and mitigate them.
WLAN Denial of Service Overview

WLANs use the 2.4 and 5 GHz license-free spectrum for communication. This spectrum is shared by other wireless devices and protocols such as cordless phones, microwave ovens, Bluetooth devices, etc. These devices and protocols often do not coexist well together and can create mutual interference when co-located and operating concurrently. WLANs use the IEEE 802.11 protocol to avoid collisions between different devices and allow fair sharing of the medium. WLAN Denial of Service can be intentional (by an attacker in the vicinity) or unintentional (neighboring devices interfering with each other) as illustrated in Figure 1.

Physical Layer Vulnerabilities

WLAN devices sense the RF medium to determine if the channel is free before transmitting their own packets. The protocol is referred to as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). In CSMA, a device wishing to transmit has to first listen to the channel for a predetermined amount of time so as to check for any activity on the channel. If the channel is idle, the device is allowed to transmit. If the channel is busy, the device has to defer its transmission. Collision Avoidance schemes tend to be less “greedy” when it comes to grabbing the channel and back off transmission for random intervals if they sense activity. In essence, WLANs are designed to “play nice” on the shared communication medium.

On the contrary, devices such as microwave ovens simply spew energy in the 2.4 GHz band when they are powered up. Other devices such as wireless video cameras might use a continuous wave modulation scheme where they are always radiating energy on a given RF channel. If these devices are operating in the vicinity of a WLAN, they can effectively shut down all WLAN communication because devices will defer their transmissions until they sense that the medium is idle.
Malicious RF jammers are also freely available on the internet. These devices are illegal and are specifically designed to disrupt wireless communications. Figure 2 shows a handheld, quad-band, cellular and 2.4 GHz band jammer that uses a 6.0V NiMH battery pack with an approximate battery life of one hour. The device has a total output power of 1200 mW (a typical WLAN access point normally operates at 100 mW). Such a device can effectively block WLAN communication within a 30 meter radius. Very high power jammers capable of radiating 200 W of power, effective over a 1 km, are also available in the black market.

MAC Layer Vulnerabilities

The 802.11 MAC is particularly vulnerable to DoS. The current standard protects only data frames and leaves various control and management frames subject to manipulation by an attacker. Since the ratification of the IEEE 802.11i standard in 2004, WLANs have been able to provide strong authentication of wireless devices and encryption of data traffic. The 802.11i standard uses the IEEE 802.1X Extensible Authentication Protocol (EAP) to guarantee that only authorized devices gain access to the wireless network and uses the Advanced Encryption Standard (AES) to guarantee confidentiality and integrity of the data communications between authenticated devices. IEEE 802.11i is the basis for the WPA2 (Wi-Fi Protected Access 2) industry standard. A major limitation in the 802.11i standard is that no protection is available for management or control frames that establish connections and, in general, affect the behavior of WLANs. Tools such as “wlan-jack”, “hunter-killer” and “void11” exploit the lack of management and control frame protection to mount DoS attacks in WLANs.

Management Frame Exploits

One of the most popular WLAN DoS attacks is based on spoofed deauthentication and disassociation frames as depicted in Figure 3. These management frames, like other 802.11 management frames, are not authenticated. As such, an attacker can spoof the MAC address of an AP and send a deauthentication frame to a client, or vice versa. The attacker can periodically scan all channels and transmit spoofed deauthentication messages to valid clients, terminating their connection. Deauthentication is not a request, it is a notification. When the station hears a deauthentication frame, it had no cryptographic mechanism to determine whether the frame actually came from the AP. It terminates its wireless session and may attempt to reauthenticate. The attacker can keep transmitting deauthentication frames preventing any data communication from happening between the AP and station, despite the authentication and encryption that exists for data traffic, resulting in a successful DoS attack. Using the same basic principle, an attacker can spoof the source of other management or control frames that result in DoS.

A spoofed disassociation frame also produced the same end result – disassociating the client from the AP. A deauthentication attack is slightly more effective than disassociation since the client has to first re-authenticate and then re-associate, i.e. do more work to re-establish the wireless connection.
Power Save Exploits

Another DoS attack in WLANs exploits the power saving mechanism in the standard. Mobile WLAN clients are allowed to enter a sleep state during which their WLAN radio is disabled to conserve battery life. When an associated client is in a sleep state, the AP buffers any traffic destined for the client. The client wakes up periodically and polls the AP for any buffered traffic, which the AP delivers and subsequently discards. An attacker can send a spoofed power save poll message, while the client is still sleeping, causing the AP to transmit and discard any buffered traffic. It is also possible to trick the client into thinking that there are no buffered frames. Buffered frames at the AP are advertised in a Traffic Indication Map (TIM). An attacker can spoof a TIM, convincing the client that there is no buffered traffic, causing the client to immediately go back to the sleep state, resulting in the frames for the client eventually getting dropped.

Media Access Control Vulnerabilities

The 802.11 MAC is designed for collision avoidance and fair sharing of the RF medium. The fundamental assumption behind fair sharing, of course, is that devices are following the protocol. The basic protocol requires 802.11 devices to contend for the channel during a contention window of time as illustrated in Figure 4. Devices wait for a random backoff period, before sensing the medium and initiating transmission. Once a device has initiated a transmission, other devices wait for the channel to be free before transmitting. A typical MAC frame includes a duration field that tells other devices the length of time (including acknowledgement, ACK) for which the medium will be busy. This facilitates virtual carrier sensing in addition to physical carrier sensing. APs and stations keep track of transmission durations of other devices they hear to determine when the next transmit opportunity will arise.

An attacker can easily circumvent the protocol and monopolize the channel. By initiating transmissions without waiting for the mandated time during the contention window, the attacker can gain repeated access to the channel before a legitimate device does. Further, by spoofing the duration field with very large values, the attacker can convince legitimate stations that the medium is busy and prevent them from gaining access. Several control frames such as Clear to Send (CTS) that are not authenticated can be used with spoofed duration field values to completely block the channel on multiple frequencies with a single radio.
Unintentional DoS

There are several instances when WLANs experience DoS or degraded performance because of neighboring WLAN traffic. Similar to the unintentional interference from non-WLAN sources, this type of interference happens when co-located WLANs are operating on the same channel. For example, a client might be hearing transmission from a neighboring AP and backing off transmissions to avoid collisions. This can lead to reduced throughput and increased transmission latency.

WLAN Denial of Service Countermeasures

A 24x7 Wireless Intrusion Prevention System (WIPS) can be used to effectively detect a DoS attack. However, mitigating DoS attacks, particularly intentional ones initiated by a sophisticated attacker is not possible. An effective overall WLAN DoS mitigation strategy depends being able to (i) Detect an attack accurately in real-time, (ii) Determine the physical location of the attacker and notify appropriate personnel, (iii) Attempt WIPS mitigation and/or physically neutralize the attacker, and (iv) Provide forensic analysis capabilities.

DoS Detection

A WIPS system should be capable of detecting both PHY and MAC layer DoS attacks. Motorola AirDefense Enterprise provides the most comprehensive Layer 1 & Layer 2 WLAN DoS detection capabilities available in the industry. The Motorola AirDefense Enterprise system is capable of detecting 17 different DoS attacks using attack signatures (e.g., wlan-jack, fata-jack, hunter-killer, etc.) as well as protocol anomaly analysis (e.g., EAP floods, CTS floods, deauthentication/disassociation, virtual carrier exploits, etc.). Further, unlike competitive solutions, AirDefense Enterprise is capable of detecting non-WLAN sources of interference that could be causing intentional or accidental DoS. Figure 5 depicts the spectrum analysis capability of AirDefense Enterprise that can be leveraged effectively to detect Layer 1 DoS attacks and classify the type of source.
Location Tracking

Once a DoS attack is detected, it is paramount to determine the physical location of the source or attacker. For example, the attacker could be in the parking lot of an office. By generating an alarm in real-time and pin-pointing the location of the attacker, security guards can be dispatched to neutralize the perpetrator. AirDefense Enterprise can not only detect an attack but also determine the location of the source using signal strength triangulation. Using the highly flexible and configurable notification mechanisms, appropriate personnel present at the site of the attack can be notified in real-time.

DoS Mitigation

Most DoS attacks cannot be mitigated. Unintentional attacks, such as interference from neighboring WLANs or co-located devices such as microwave ovens, can be mitigated by changing the channel plan for the WLAN. The Motorola WLAN includes SmartRF algorithms that can automatically determine the optimum channels based on changing real-time conditions. Motorola AirDefense Enterprise DoS alarms can be leveraged by WLAN management systems to trigger a reconfiguration of the operating channels to minimize interference.

However, a determined attacker can always disrupt a WLAN. Some WIPS vendors misleadingly assert that they can “prevent” DoS attacks. One vendor in particular claims that they can use their sensors to effectively prevent the attacker from gaining access to the channel, while allowing authorized devices to communicate, by using a mechanism similar to that described in Figure 4. The vendor claims that they can spoof duration fields in their transmissions and reserve the channel for authorized devices while denying them to the attacker. It is based on the flawed assumption that the attacker is playing in accordance with the 802.11 rules and will listen to them! The attacker can simply ignore the channel reservation attempted by spoofed frames from the WIPS sensor and continue to transmit numerous deauthentication frames. The authorized devices need to hear just one to end the wireless session. Further, the attacker can always mount a physical layer attack that is totally immune to the proposed technique. By attempting to orchestrate transmit opportunities for valid devices in a proprietary manner, the vendor’s system will result in significant
performance degradation when traffic load increases with virtually no real DoS mitigation benefits. The IEEE 802.11 community has recently ratified the 802.11w standard that will provide authentication and encryption protection to several 802.11 management frames. Motorola WLAN infrastructure supports 802.11w. The primary advantage of 802.11w is that it can prevent DoS attacks that exploit spoofing of management frames. An 802.11w compliant station will be able to distinguish whether the deauthentication frame in Figure 3 came from the AP it is connected to (if the AP also supports 802.11w) or was spoofed by the attacker masquerading as the AP. It will ignore the spoofed deauthentication frame and prevent the DoS attack from being successful. Similarly, the authenticity and integrity of other commonly spoofed management frames is provided by the 802.11w standard. The fundamental mechanism that Layer 2 DoS attacks exploit in WLANs is the lack of authentication of management and control frames. Unfortunately, while the 802.11w standard offers protection from DoS attacks that exploit spoofed management frames (such as deauthentication or disassociation), it offers no protection from similar attacks that use spoofed control frames, media access blocking or RF jamming methods.

The only guaranteed mechanism to neutralize an intentional DoS attack is to find and eliminate the attacker. For that, the WIPS needs to be able to accurately detect both Layer 1 and Layer 2 DoS, locate the source as well as provide flexible notification mechanisms that integrate with the enterprise’s physical security infrastructure to capture and neutralize the attacker.

Forensic Analysis
Real-time DoS attack detection is important. However, the ability to analyze minute-by-minute wireless behavior with a historical perspective is indispensable for detecting sophisticated and persistent WLAN attacks. AirDefense Enterprise allows organizations to trace any suspicious device by rewinding and reviewing minute-by-minute records of connectivity and communication with the WLAN, thereby facilitating forensic investigations. Wireless activity is logged and data is stored in a tamper-proof way to ensure a full audit trail is maintained. AirDefense Enterprise maintains 325 different statistics for every wireless device, every minute, and is capable of storing this data for months. By analyzing patterns over a period of time, even subtle DoS scenarios can be unearthed. Sophisticated capabilities such as historical location tracking can be utilized to determine the physical whereabouts of the attacker, over time, and can be vital in nabbing the culprit.

Figure 6: Advanced Forensics for investigating WLAN DoS attacks
Conclusions

Wireless DoS attacks can be initiated at the physical or MAC layer and can cripple a WLAN. While intentional DoS attacks cause the most damage, unintentional interference can also be deleterious. Physical layer DoS attacks are caused by RF jammers that prevent WLAN devices from communicating. MAC layer DoS attacks exploit the lack of management and control frame protection, along with media access vulnerabilities in the 802.11 protocol. Management frame protection has been recently incorporated into the standard through the 802.11w-2009 amendment. However, control frame protection and RF jamming attacks are not addressed by the revision. Some vendors inaccurately claim to be able to “prevent” DoS attacks. These claims are dubious since RF jamming attacks as well as MAC based attacks initiated by a determined attacker cannot truly be prevented. A successful mitigation strategy involves being able to accurately detect, locate and physically neutralize the attacker. Granular historical forensic data is extremely useful in detecting and locating sophisticated attacks. AirDefense Enterprise provides the most comprehensive DoS detection and mitigation capabilities for WLAN deployments.
About Motorola AirDefense Solutions

Motorola offers a comprehensive portfolio of wireless LAN (WLAN) infrastructure solutions designed to enable the truly wireless enterprise, regardless of the size of your business — from large enterprises with locations all over the world to branch offices and small businesses. Delivering Internet protocol (IP) coverage to virtually all spaces both indoors and outdoors, Motorola's innovative wireless enterprise portfolio includes fixed broadband, mesh, enterprise WLAN and Motorola AirDefense wireless security solutions. With time-proven resiliency, security and performance equal to or greater than that of a wired network, Motorola's solutions substantially reduce network deployment and maintenance costs, and ensure the availability of cost-effective wireless connectivity in every corner of the enterprise. The result is the truly wireless enterprise — offering full mobility at a fraction of the cost of a traditional wired network.

For more information visit us on the web at www.motorola.com/airdefense or www.motorola.com/enterprise