May 18, 2018

WAKE UP RADIO PROTECTION FROM DENIAL OF SERVICE ATTACK BASED ON BASEBAND MONITORING

Matt Silverman

Santosh Pandey

WAKE UP RADIO PROTECTION FROM DENIAL OF SERVICE ATTACK BASED ON BASEBAND MONITORING

AUTHORS:
Matt Silverman
Santosh Pandey

ABSTRACT

A malicious attacker can drain the batteries of Internet of Things (IoT) devices by sending many wake up radio (WUR) transmissions. Accordingly, techniques are provided herein to enable an Access Point (AP) to detect any malicious WUR requests. The AP may intelligently mitigate the attack with the help of the stations (STAs).

DETAILED DESCRIPTION

802.11ba seeks to increase battery life span for Wi-Fi® based Internet of Things (IoT) devices by allowing the primary device to enter a sleep mode with a low-power wake up radio (WUR) listening for wake up transmissions. A malicious attacker can drain batteries by sending many of these WUR transmissions.

There are currently no adequate security procedures to protect against WUR replay attacks. For example, the station (STA) may be re-keyed to a new Identifier (ID), if the AP detects that the STA is under attack. This is an unsustainable model if the attacker is replaying all of the AP's Wakeup Requests, as there will be too many re-key attempts and all the STAs are attempting to communicate traffic to the AP.

The mechanism described herein uses dedicated monitor radios on APs that scan for 802.11ba wake up transmissions (WUTs) and attempt to detect malicious behavior. Malicious behavior may be detected using the monitor mode radio on the AP to detect whether the AP's packets are being replayed. The AP may also search for an unsolicited response from the STA's primary radio. In another example, the AP may search for instances where the WUT misrepresents itself as an AP on the network. This may involve tracking baseband characteristics of the WUT frame and comparing to those of known APs for mismatches.

If a malicious WUT device is identified, the network AP with a monitor radio may mitigate the attack by interfering with the WUT. For example, when a WUT from the

malicious device is initially detected, the monitor radio may insert an On/Off key transmission that will be synchronized with the destination Media Access Control (MAC) address field of the WUT frame to modify the destination MAC to an unused dummy MAC (e.g., timely jamming) to cause the victim IoT device to ignore the WUT frame. This may involve estimating the transmission level required to match the receiver level at the victim device, the WUT frame from the attacker based on the WUT preamble, and the time synchronization to the WUT.

Since the unwanted device has been previously identified, a positive ID using the preamble may be obtained. The following metrics may be used: (1) Angle of Arrival (AoA) at the AP based on a cross-correlation of the preamble across a switched antenna array or across a simple multiple antenna AP; (2) Carrier Frequency Offset (CFO) based on an estimate provided by the preamble; (3) channel matrix based on the preamble after CFO correction; and (4) ripple in the Broadband (BB) filter across subcarriers (i.e., the locations of the nulls and peaks).

Furthermore, the AP may indicate to the STA that there is a malicious WUT in the vicinity. The STA can then learn which WUTs are from real APs as opposed to malicious attackers over time by learning the PHY parameters. This may include monitoring the Received Signal Strength Indicator (RSSI) of the WUR request from the AP, the carrier offset of the WUR request from the AP, and the start-of-packet parameters involving the SYNC field.

The learning may involve a very simple classification using maximum likelihood or other basic techniques. For complicated attacks where higher resources are available at the STA, additional factors and techniques may be used.

The AP may search for the malicious WUT and determine whether to trigger STAs to perform additional processing, if necessary. There may be situations where the AP chooses to ignore the attack, or selectively notify only some STAs to begin monitoring. The AP may choose the STAs based on factors such as which STAs are experiencing the most false positives for primary radio wake up. If STAs are very resource constrained, the APs may choose not to let the STA perform additional mitigation processing.

A WUT frame replay may be detected even if the WUT frame does not contain a sequence ID. Since the WUT frame is transmitted by the AP, the AP may maintain the state

and easily detect a replay. One example is to identify a WUT having the transmit address of the AP, but which the AP has not sent.

It may be determined that a WUT misrepresented itself as an AP on the network based on an excessive frequency. The excessive frequency can be determined by monitoring a successful WUT. For example, consider a STA that receives a WUT, wakes up the primary radio, and then realizes that there are no packets queued at the AP for the STA. Every time such a state is reached, the STA may increment a counter X. If such a state is reached multiple times frequently (e.g., greater than X times in a second), the STA may determine that this is excessive.

Radio Frequency (RF) technology is local and varies with many parameters (e.g., multipath, etc.). However, overall the transmission from a well behaved AP usually follows a Gaussian distribution with a 7dB standard deviation for indoor applications. Also, APs tend to send certain packets at a fixed data rate and hence transmit power. This is practically true for packets such as beacons, probe responses, Ready to Send (RTS) packets, Clear to Send (CTS) packets, etc. Therefore, a malicious attacker would have to transmit a WUT with an exact power so as to emulate the Gaussian distribution. This is not the only way to detect a WUT attack, and may be used in conjunction with other techniques provided herein (e.g., carrier offset, etc.). For example, STAs in 802.11ba are IoT STAs and most likely have some kind of motion detection sensors to further build confidence in these techniques and make sure they have not moved.

In summary, a malicious attacker can drain the batteries of IoT devices by sending many WUR transmissions. Accordingly, techniques are provided herein to enable an AP to detect any malicious WUR requests. The AP may intelligently mitigate the attack with the help of the STAs.