

A Configuration Protocol for Embedded Networked Devices on Secure Wireless Networks

Larry M. Sanders, Joseph B. Evans
Information & Telecommunication Technology Center
University of Kansas
Lawrence, KS 66045
{lsanders, evans}@ittc.ku.edu

Benjamin J. Ewy
Ambient Computing, Inc.
Lawrence, KS 66045
bewy@ambientcomputing.com

Abstract

With the rise of wireless networking products based on the IEEE 802.11 standard, traditional embedded networked devices are shedding their cables. As the cost and size of Wi-Fi chipsets continues to decrease and the number of deployed Wi-Fi networks increases, we are likely to see an explosion in Wi-Fi enabled embedded networked devices. Applications for traditional embedded networked devices span such areas as physical security systems, environmental monitoring and control, Internet applications, personal digital assistants, industrial monitoring and control, and health monitoring systems.

Devices wishing to join a wired network, such as Ethernet, typically need only be plugged into a hub or switch to gain network connectivity. The device may then utilize higher-level configuration protocols such as DHCP or it can be configured via a SNMP configuration utility or browser accessing a built-in web server. Wireless devices do not have that luxury and require configuration at the data link level. In the common case of a Wi-Fi enabled laptop joining a wireless network, the user generally enters the SSID (network name) and optionally the WEP keys, and then uses higher-level configuration protocols. The SSID and WEP configuration parameters require embedded devices with limited or no input capabilities (e.g., keyboard) to implement additional user interfaces, such as a USB connection or wired Ethernet, to facilitate initial network configuration – which adds cost and complexity to the embedded devices. In this paper, we present a new protocol that allows a wireless embedded networked device to be easily configured for use on a WEP enabled Wi-Fi network.

Background

Wi-Fi is easily the most commercially successful LAN technology since Ethernet. The most common topology for Wi-Fi networks is Infrastructure mode. This is created when an Access Point (AP) bridges traffic from the distribution system (typically Ethernet) to wireless stations within range of the AP, generating a Basic Service Set (BSS). An Extended Service Set (ESS) is created when multiple APs are linked via the wired Ethernet backbone to provide for seamless Wi-Fi coverage across an entire building or campus. Wi-Fi, sometimes called wireless Ethernet, differs from Ethernet in many ways.

In particular, multiple Wi-Fi networks may need to use the same RF spectrum and physical area. Separate networks can coexist in this scenario and are distinguished by a parameter called the Service Set Identifier (SSID) or network name. It is also more difficult to secure physical access to the Wi-Fi network than wired Ethernet because wireless can often propagate outside the intended coverage area. For this reason, the existing 802.11 standard specifies a data confidentiality service called Wired Equivalent Privacy (WEP), which utilizes RC4, a shared key stream cipher. While newer versions of WEP are being standardized to solve insecurities, replacements also require some type of configuration data on the client side. Both the SSID and WEP keys are configuration parameters that need to be programmed into a device that is attempting to join a particular Wi-Fi network.

Protocol Overview

Wi-Fi-Co is a protocol and suite of tools to facilitate the initial configuration of network parameters to an embedded networked device within a Wi-Fi network. Wi-Fi-Co enables a configuring host, such as a

desktop computer on the wired portion of an ESS network, to send network parameters to a Wi-Fi enabled embedded device within range of the encrypted wireless network.

Wi-Fi enabled devices can easily capture wireless traffic in promiscuous mode, provided they are within range of an Access Point in an ESS. However, if WEP is enabled, the data portions of the bridged traffic will be encrypted, and without the shared keys, the Wi-Fi node will be unable to decrypt the packet. Wi-Fi-Co is able to send data across this wired, unencrypted network to wireless, encrypted network boundary by utilizing fields within the 802.11 MAC header. In infrastructure mode, an AP will bridge traffic from the distribution system (wired Ethernet network) to the wireless network by encapsulating the packet in the 802.11 frame format. A simplified description of this process is summarized below.

The 48-bit Ethernet destination and source MAC addresses are copied to the address 1 and address 3 fields of the 802.11 MAC header, respectively. Address 2 will contain the MAC address of the AP and address 4 is not used. The data portion of the Ethernet frame will be 802.2 LLC encapsulated and copied to the data portion of the 802.11 frame (see figure 1). Finally, if WEP is enabled, the data portion is encrypted, and the frame is transmitted to the Wi-Fi station.

Since the 802.11 header is transmitted in plaintext, the source address field enables six bytes of data to be sent from the Ethernet portion to a Wi-Fi station within range of an AP. Configuration data can be fragmented and embedded in the source MAC field. The destination MAC field specifies the broadcast address, guaranteeing that the AP will broadcast the frame on the Wi-Fi BSS (see figure 2). The target embedded device can then capture and reassemble the network parameters enabling the device to join the Wi-Fi network.

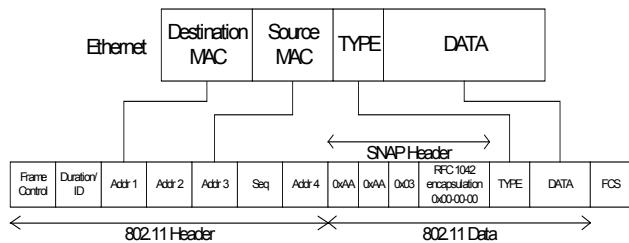


Figure 1: 802.11 Encapsulation

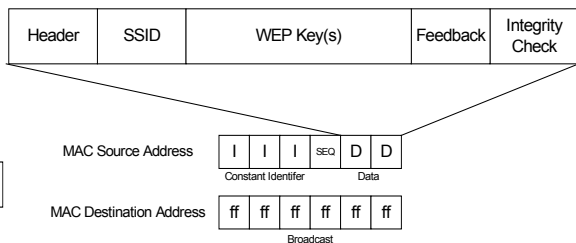


Figure 2: Wi-Fi-Co Fragmentation

Since Wi-Fi-Co utilizes broadcast communication, a method to protect the shared secret WEP keys is needed. One solution is for the embedded device’s firmware to contain a unique key that can be used when configuring the device. A certificate with a secret key might ship with the device, and the user could enter the key on the configuration host. Then the Wi-Fi-Co configuration buffer could be encrypted with this key, protecting the network from other malicious hosts that may be monitoring wireless traffic. This extra user input on the configuration side is acceptable because it is assumed that input to the configuration software (desktop computer) is much easier than input to the embedded device.

Wi-Fi-Co has been implemented and evaluated on devices including laptops, PDAs, and special-purpose embedded wireless controllers/sensors. Configuration times typically range from tens of milliseconds up to a few seconds depending on network traffic and processor capabilities.

Summary

Wi-Fi-Co provides an inexpensive, simple solution that allows a wireless embedded networked device to be configured on a WEP enabled Wi-Fi network. Networked devices that only provide user interfaces at the network level cannot utilize the network until programmed with link level Wi-Fi configuration parameters, which typically means implementing an additional interface just to facilitate initial configuration. This is an expensive solution for simple applications such as wireless sensors, video surveillance devices, environmental control devices, and other network-centric devices. Wi-Fi-Co can eliminate expensive interfaces and reduce complexity of embedded devices based on wireless LAN technologies.