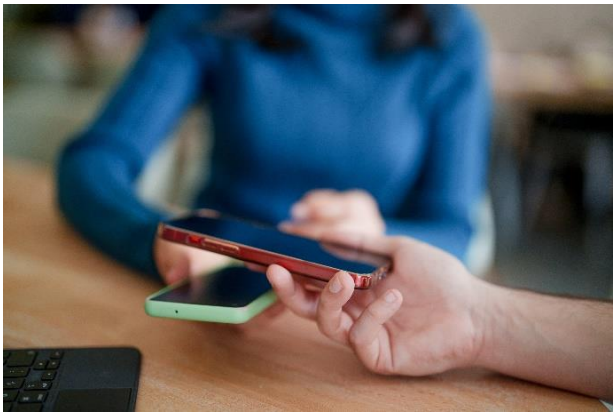
Proximity Detection Highlights

Proximity Detection: Convenient, secure location services

Proximity Detection technology allows a Wi-Fi® device to detect a second Wi-Fi device and connect to it upon reaching a certain distance between them (called "ranging"). This connection can trigger automatic actions that fulfill a desired functionality. Many use cases and applications, including device finder and automatic device unlock, must ensure that ranging can only occur between devices that have a trust relationship and that ranging measurements have high integrity. This verifies the validity of any automatic actions between trusted peer devices triggered by detection. Proximity Detection provides additional Physical Layer (PHY) security to enable a variety of use cases, complementing the high-accuracy, low-latency distance measurements and Medium Access Control (MAC) layer security provided by Wi-Fi Location™.



How Proximity Detection works

To establish trust between participating devices, Proximity Detection leverages Protected Management Frames to utilize a shared encryption key. This encryption key ensures the contents of encrypted packets cannot be overheard or tampered with by an attacker. Encrypting certain fields at the PHY level of the protocol helps achieve distance integrity. Some of these fields include:

- The packet long training field (LTF) used for Orthogonal Frequency-Division Multiplexing (OFDM) symbol-level encoding, which determines the precise time a packet arrives at the receiving client device
- A protected training field, which prevents modification of a receive timestamp

With a shared key and a trust relationship between participating devices, bad actors cannot intercept and modify the ranging protocol for their own purposes. Users can expect Proximity Detection to safeguard information, protect personal property, and provide a valid indication of distance for triggering automatic actions.

Applications using Proximity Detection

Automatic device unlock

User problem: An IT professional frequently uses a company-owned computer that needs to be unlocked before use and locks automatically after a short period of inactivity to prevent unauthorized access. The manual unlocking process results in unproductive user time and a poor user experience.

Proximity Detection solution: Using Proximity Detection, the computer detects a second device (such as a smartphone), triggering an automatic action to unlock the computer without the user manually entering login credentials. Furthermore, if they work at the computer without typing for several minutes, the computer will not automatically lock them out as long as the smartphone is nearby. However, if they leave the room with their smartphone, the computer will correctly lock itself.

The result is an entirely positive user experience, increasing productivity and reducing frustration while maintaining security.

Device finder

User problem: It is easy to lose a mobile device, and often the lost device is nearby — for example, under a cushion or behind a piece of furniture.

Proximity Detection solution: Proximity Detection allows a second device to detect the lost device, providing an accurate distance measurement that can guide a user toward the lost device. A shared key ensures that only devices with the required credentials can locate each other, providing security for the device owner.

Proximity media transfer: Tap-to-cast

User problem: Users will often stream music on their smartphones and listen to it on wireless earbuds. However, if a user moves close to a smart speaker, they may prefer to transfer the stream to the speaker for better sound quality. Ordinarily, this requires setting up a new network connection, which can be cumbersome.

Proximity Detection solution: The streaming music can automatically transfer from the earbuds to the speaker when the smartphone detects the speaker at a specific distance, such as a few centimeters, allowing the user to "tap-to-cast" without manually connecting the devices. Proximity Detection guarantees that only users with the correct credentials can cast a media stream to their devices.

Wi-Fi® is the best choice for location use cases

Proximity Detection utilizes Wi-Fi's widespread coverage, consumer market penetration, and sub-meter-level accuracy to enable a variety of applications and services. To ensure a safe connectivity experience, Proximity Detection includes security at the MAC and PHY levels, which supports the integrity of the information used by the protocol and prevents timing attacks that use inaccurate range estimates to access locked devices and secure areas. Proximity Detection complements Wi-Fi Location, which supports indoor navigation, asset tracking, and AP-to-AP ranging use cases including simplified deployment and 6 GHz AFC location.

About Wi-Fi Alliance®

Wi-Fi Alliance® is the worldwide network of companies that brings you Wi-Fi®. Members of our collaboration forum come together from across the Wi-Fi ecosystem with the shared vision to connect everyone and everything, everywhere, while providing the best possible user experience. Since 2000, Wi-Fi Alliance has completed more than 80,000 Wi-Fi certifications. The Wi-Fi CERTIFIED® seal of approval designates products with proven interoperability, backward compatibility, and the highest industry-standard security protections in place. Today, Wi-Fi carries more than half of the internet's traffic in an ever-expanding variety of applications. Wi-Fi Alliance continues to drive the adoption and evolution of Wi-Fi, which billions of people rely on every day.

© 2025 Wi-Fi Alliance. All rights reserved. Wi-Fi®, Wi-Fi CERTIFIED®, Wi-Fi Alliance®, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, and other marks are trademarks of Wi-Fi Alliance.