Automatic Device Wake and Authentication Based On Ultrasound

N/A
Automatic Device Wake and Authentication Based On Ultrasound

ABSTRACT

Wireless communication between devices requires the devices to be active at the same time. Wireless pairing and authenticating of devices (e.g., via Bluetooth) currently requires each device to be in a sharing mode or to be connected to the same network, which can consume device battery and requires specific user action. This disclosure describes techniques that, with user permission, automatically wake a device to communicate with another device based on ultrasound signals received from the other device. The received signal can also be interpreted as an intent for an action, if permitted by the user. The described techniques are suitable even when target devices are unknown, can limit communication to a physical ranger, and are suitable even in situations where the devices that communicate do not have a network connection.

KEYWORDS

- Ultrasound wake
- Device wake
- Device pairing
- Device authentication
- Device activation

BACKGROUND

Wireless communication between devices requires the devices to be active at the same time. Also, wireless pairing and authenticating of devices (e.g., via Bluetooth) is not a frictionless process. For example, a user has to typically proactively put their device into a sharing mode to pair with another device.
Another approach for pairing devices is to use a push notification to devices that are on a shared network, e.g., on the same WiFi network. Network pairing and authentication processes, however, present challenges in particular situations. For example, network pairing does not work where the target devices are unknown (e.g., guests in a house) and is not a solution when there is no network connection available (e.g., emergency scenarios).

DESCRIPTION

This disclosure describes techniques that, with user permission, automatically wake a device to communicate with another device based on ultrasound signals received from the other device. The ultrasound signals are detected by a device microphone (e.g., an always-on microphone that detects audio signals such as a wake word) on the target device. The two devices can then exchange information. The received signal can also be interpreted as an intent for an action, e.g., automatically open a camera application and prompt the user to take a photo.

Fig. 1: Automatic device wake and authentication based on ultrasound
Fig. 1 illustrates an example of the techniques of this disclosure for automatically waking a device - smart glasses 104 - using ultrasound signals. As illustrated in Fig. 1, a second device in this example, a display screen (102) transmits an ultrasound signal to nearby devices in range that are suitable for pairing. The ultrasound signal, upon detection by a microphone (107) of the smart glasses, automatically wakes and authenticates the smart glasses worn by a user (106) without the user having to put the smart glasses in a sharing or detection mode. For example, the ultrasound signal may encode a request from the display screen for access to the user’s account in order to configure the display. A user interface (108) may be displayed to the user (e.g., on the smart glasses or via audio) that the display screen is requesting confirmation of the user’s account.

Additional examples of use are listed below:

**Example 1**

A user’s personal computer emits ultrasound signals. The user comes nearby to their personal computer while carrying another mobile device (e.g., a smartphone, wearable, smart glasses, tablet, etc.), that includes a microphone. The microphone receives the ultrasound signals and based on prior registration, automatically wakes up and pairs the mobile device and personal computer. With this automatic process, data transfer between the computer and mobile device is enabled. In this case, a specific device (the user’s mobile device) can be woken up by including in the ultrasound signals signature authentication that identifies the specific device.

**Example 2**

As shown in Fig. 1, the display screen may be newly acquired by the user and need to be configured for use. Upon detection of the ultrasound signal emitted by the display screen, the
user receives a prompt via their smart glasses to complete the setup process for the display screen. In this case, the identity of the emitting device may not be known to the receiving device.

**Example 3**

The infotainment system in a car can enable sharing a current audio playlist to multiple mobile devices that are present in the same vehicle by utilizing the described techniques, e.g., by transmitting ultrasound locally within a short range that covers the car. In this manner, distribution of the playlist is restricted based on proximity.

The described techniques are suitable even when target devices are unknown (e.g., newly purchased devices, guests in a hose, etc.), can limit communication to a physical ranger (e.g., nearby only), and are suitable even in situations where the devices that communicate do not have a network connection. By eliminating the need to put a device in a pairing mode, the techniques conserve battery and simplify connection to other devices, without requiring specific user input.

While the foregoing discussion refers to use of ultrasound signals, alternate wakeup signals can be used as permitted by the user. For example, if the receiving device includes a camera, the transmitting device may display a code that can be detected by the camera, when in visual range. Alternatively, the information may be encoded in infrared signals that can be detected and used to initiate communication between devices.

The user is provided with options to configure their device to enable or disable automatic detection of ultrasound signals transmitted by other devices. For example, the user can restrict automatic detection to specific other devices that can perform signature authentication via ultrasound. A user can also select how the received ultrasound signals are processed, e.g., enable or disable automatic actions (e.g., capturing an image) in response to receiving the ultrasound signal. No detection is performed if the user does not enable ultrasound communication.
CONCLUSION

This disclosure describes techniques that, with user permission, automatically wake a device to communicate with another device based on ultrasound signals received from the other device. The received signal can also be interpreted as an intent for an action, if permitted by the user. The described techniques are suitable even when target devices are unknown, can limit communication to a physical range, and are suitable even in situations where the devices that communicate do not have a network connection.