April 2023

Device Identification and Authentication with Radar and UWB Ranging

Xiating Zou

Cheng-Jung (CJ) Lee

Device Identification and Authentication with Radar and UWB Ranging

ABSTRACT

Devices such as tablets and smart displays can be automatically unlocked when a user carrying a compatible wearable device approaches. With user permission, the event of the user being in close proximity is detected, and the user is authenticated by communicating with the wearable device using ultra-wideband (UWB) radio. However, UWB ranging can suffer from front-back ambiguity such that the detection of the presence of a user that is behind the device can unlock the device, which can lead to security and/or privacy risk. This disclosure discloses a two-pronged approach to user identification, user authentication, and front-back disambiguation during automatic unlocking of a device using UWB radio. UWB radio is used to achieve handshaking and user-profile identification. Radar is used to provide front/back information. False positives are avoided by authenticating the user when a difference between the distances reported by radar and by UWB are within a threshold.

KEYWORDS

- Automatic unlock
- Front-back ambiguity
- Field-of-view (FoV)
- Ultra-wideband (UWB)
- Proximity detection
- Radar
- User authentication
- Device handshake

BACKGROUND

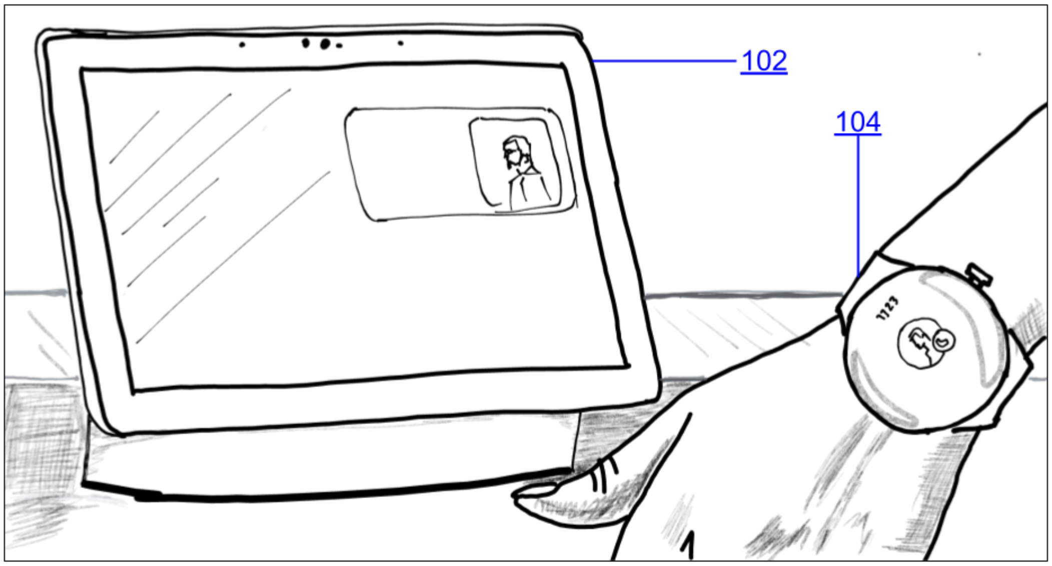

Fig. 1: Unlocking a tablet or smart display based on detecting an approaching user

Many devices such as tablets, laptops, smart displays, smart-home devices, etc. (102) feature an automatic unlock function, which unlocks the screen (and optionally, automatically displays relevant information and applications) when a user with a compatible wearable device (104) approaches. Determining that a user is in close proximity can be based on communicating with a wearable device of the user over a short-range wireless protocol such as ultra-wideband (UWB) radio, Bluetooth, etc.

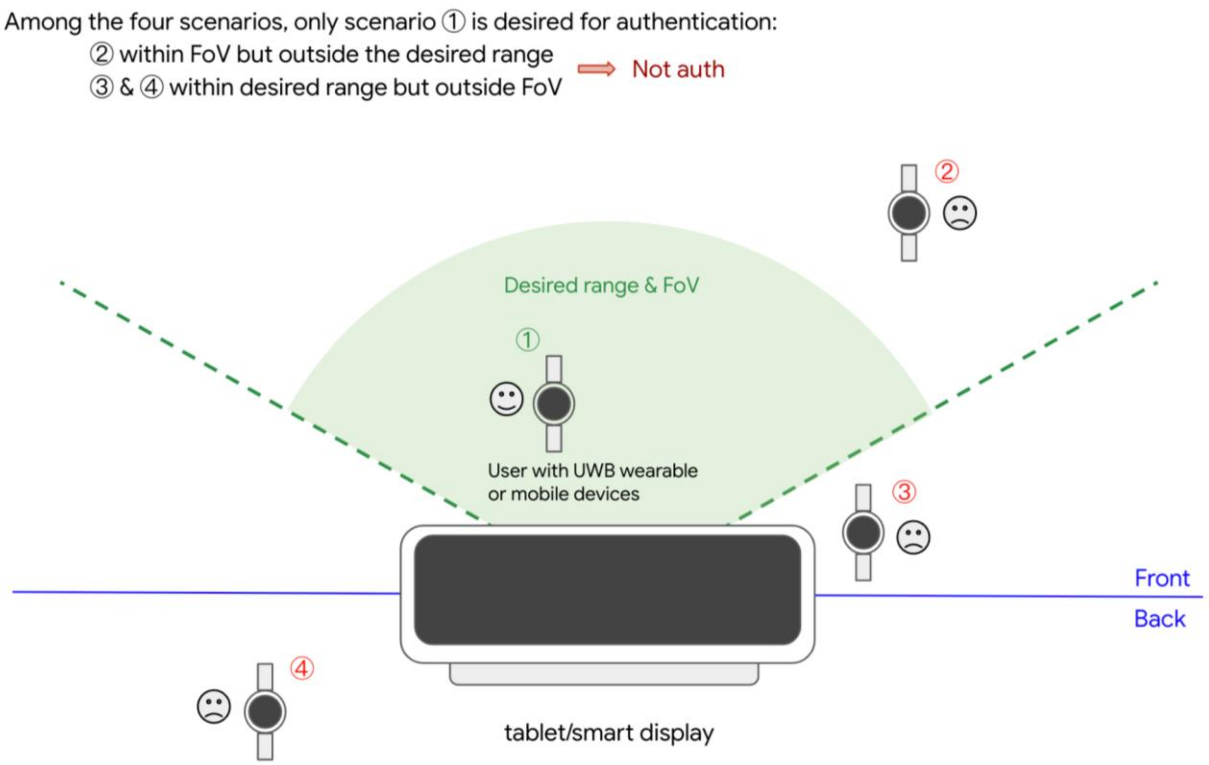
Among the four scenarios, only scenario ① is desired for authentication:
② within FoV but outside the desired range
③ & ④ within desired range but outside FoV
Not auth
②
Desired range & FoV
①
User with UWB wearable or mobile devices
③
Front
Back
④
tablet/smart display

Fig. 2: Automatic unlock requires the user to be within range and inside the field-of-view

As illustrated in Fig. 2, the automatic unlock feature requires not only the distance between the user and the smart display (or other device) but also information relating to whether the user is in the front or at the back of the device, or more specifically, whether the user is inside or outside the field-of-view of the device. This can help avoid unintentional authentication and resultant erroneous unlocking of the device. Specifically, automatic unlock requires the user to be within range and inside the field-of-view to achieve accurate identification and authentication of the user.

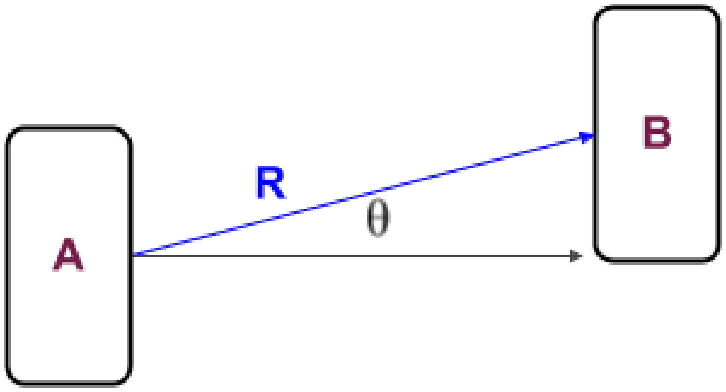

Fig. 3: Ultra-wideband (UWB) radio for device localization

As illustrated in Fig. 3, ultra-wideband radio (UWB) radio can be used for device localization. In Fig. 3, device A uses UWB to determine the distance R between itself and device B, and also the angle θ between itself and device B. The angle θ is also known as angle of arrival (AoA) because it is the angle at which ranging signals arrive from device B to device A. However, UWB ranging suffers from front-back ambiguity, as described below.

Typically, direction-finding UWB techniques report not directly the angle θ but the sine (or cosine) of the angle θ. Because the map between sinθ and θ is not one-one, there can be ambiguity in the determined angle of arrival.

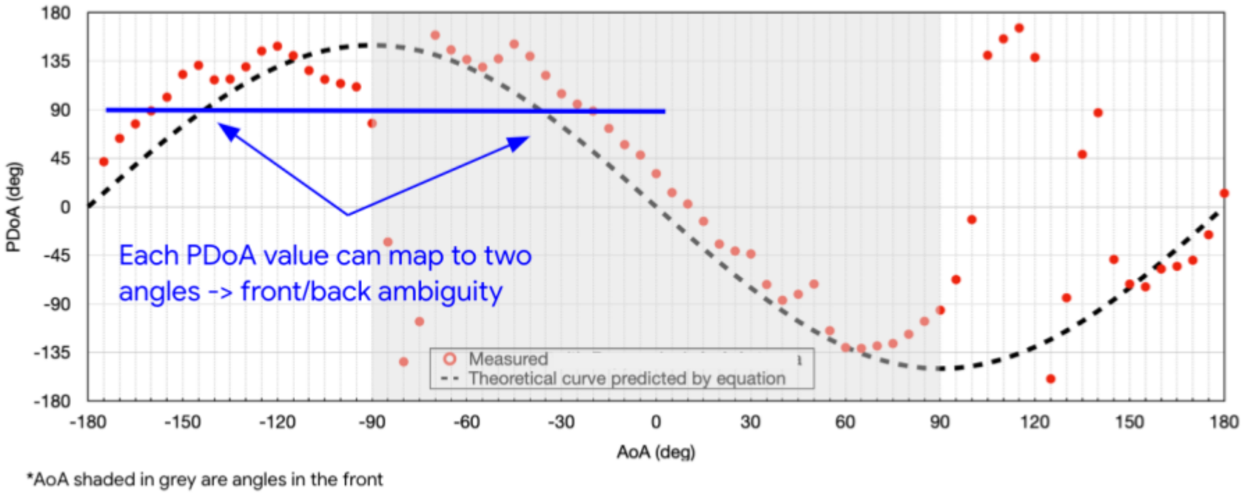

Fig. 4: Front/back ambiguity arising from the one-to-many nature of the sinθ→θ map

Fig. 4 illustrates that front-back ambiguity can arise from the one-to-many nature of the sinθ→θ map. The direction-finding technique reports the value of $2\pi(d/\lambda) \sin\theta$ (referred to as phase difference of arrival, PDoA), where d is an antenna dimension (e.g., inter-element spacing) and λ is the wavelength of the radio waves used for ranging. The red dots represent experimentally observed values of PDoA versus the physical AoA θ, while the black, dashed curve represents a theoretical curve. An observed value of the PDoA $2\pi(d/\lambda) \sin\theta$ (the horizontal blue line) maps to at least two values for the physical angle of arrival θ. One value for θ can correspond to the user being in front of the device to be unlocked, while the other value of θ can correspond to the user being behind the device. Currently, there is no solution that provides simultaneously both the front/back (inside FoV/outside FoV) information and device (user) identity.

DESCRIPTION

This disclosure discloses a two-pronged approach to user identification/authentication and front-back disambiguation. With user permission, UWB ranging is used to achieve handshaking and user profile identification. Radar, e.g., miniature radar, is used to provide front/back information (or inside/outside FoV). Examples of applicable radar technologies include UWB radar, 24 GHz radar, 60 GHz radar, etc.

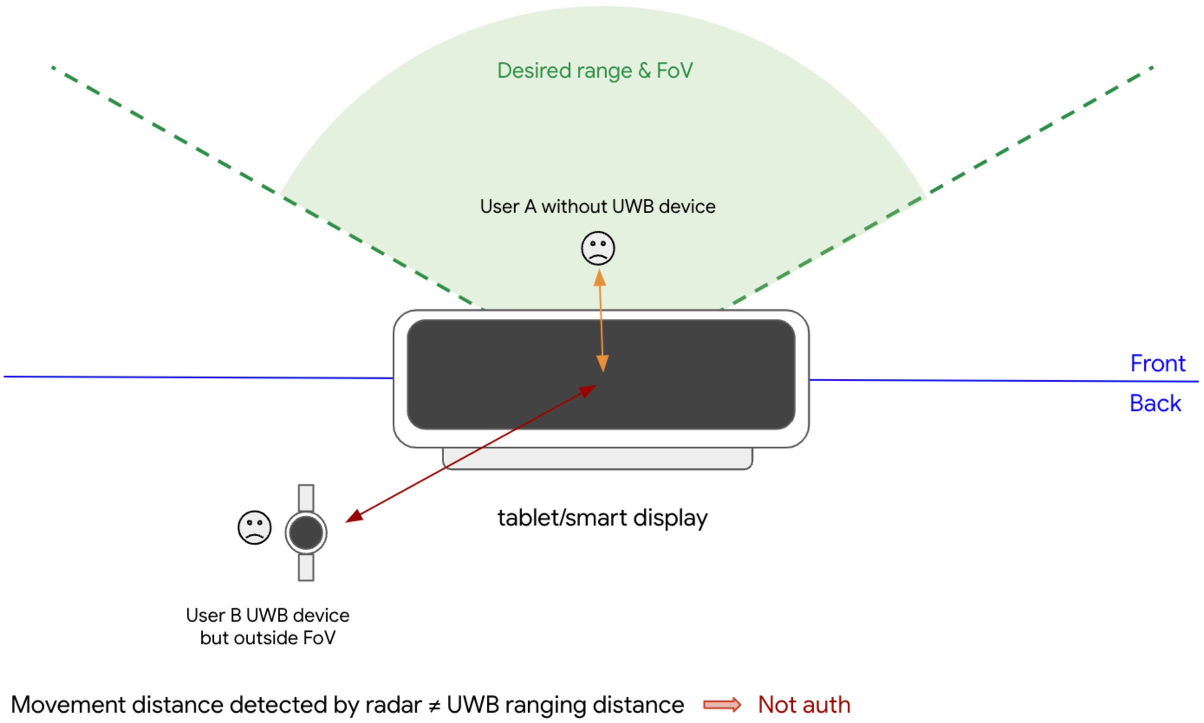

Fig. 5: A false positive scenario

An issue with simultaneous identification and front/back disambiguation using radar and UWB is the possibility of a false positive, which is illustrated in Fig. 5. Lacking a wearable UWB device, User A cannot be identified by or to connect to the smart display. User A is nevertheless detected by radar, and the smart display determines that some user, albeit an unknown one, is at its front. User B, who has UWB and is within range, successfully connects to the smart display. Because User B is behind the smart display, radar cannot detect their presence. Due to the front/back ambiguity inherent in UWB, no conclusive determination can be made that User B is in fact behind the device. Synthesizing the available observations, an incorrect conclusion is reached that the unknown user at the front of the device is User B, since radar reports a user in the front, no user profile information is available via radar while the available profile information, obtained via UWB, is that of User B. This can result in the device incorrectly authenticating the user in the front (User A) as User B. With such erroneous authentication, erroneous display of information relevant to User B may occur while user A is proximate to the device. This poses a security and privacy risk.

This false positive scenario can be countered by comparing the distance reported by UWB ranging with the distance reported by radar. Distance comparison between radar and UWB can reject a substantial proportion of false positives, since both UWB ranging and radar can achieve a ranging accuracy of a few centimeters. Specifically, a user is authenticated when the two distance values as reported by radar and by UWB ranging are close enough. In the example of Fig. 5, if radar reports that the unknown user A in front is at a distance of 15 cm and UWB reports that the user B is at a distance of 30 cm, authentication is halted (since the reported distance values are widely unequal), and the false positive is forestalled.

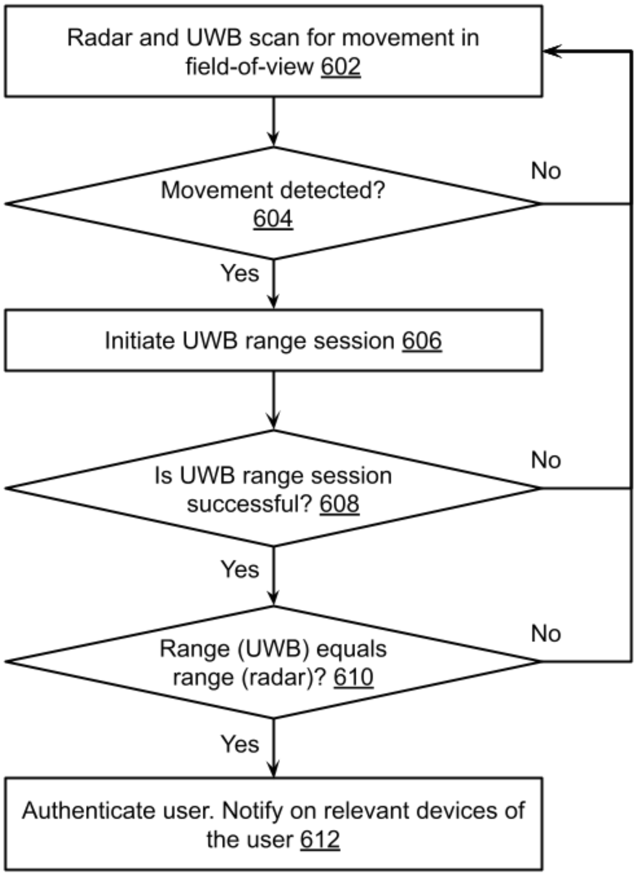
Radar and UWB scan for movement in field-of-view 602
Movement detected? 604
No
Yes
Initiate UWB range session 606
Is UWB range session successful? 608
No
Yes
Range (UWB) equals range (radar)? 610
No
Yes
Authenticate user. Notify on relevant devices of the user 612

Fig. 6: Distance comparison between radar and UWB ranging to forestall false positives

Fig. 6 illustrates the prevention of false positives by comparing range estimates between radar and UWB. Both radar and UWB scan for movement in the field of view (602). If movement is detected (604), UWB initiates a range session (606). If the range session is successful (608), the range as determined by UWB is compared to the range as determined by radar (610). If the two range estimates are equal or close to each other (610) - the absolute value of the difference is less than a certain threshold - the user is authenticated (612). The authentication event, if any, is reported on relevant devices of the user, e.g., wearable (smartwatch) devices, smart display, smartphone, tablet, etc.

CONCLUSION

This disclosure discloses a two-pronged approach to user identification, user authentication, and front-back disambiguation during automatic unlocking of a device using UWB radio. UWB radio is used to achieve handshaking and user-profile identification. Radar is used to provide front/back information. False positives are avoided by authenticating the user when a difference between the distances reported by radar and by UWB are within a threshold.