解析超寬頻 (UWB) 運作方式及卓越潛能

■作者：NXP UWB 解決方案產品管理總監 / Rias Al-Kadi
NXP 汽車 UWB 產品行銷經理 / Christoph Zorn 博士

在各種市場 (包含行動、汽車、物聯網 (IoT) 和工業空間) 中，負責開創性應用的開發人員都積極尋覓精準測距的技術，提供準確的室內外定位。幸運的是，UWB（Ultra-wideband) 最近「重獲新生」成為準確、安全和即時的定位技術，優於 Wi-Fi、藍牙和 GPS 等其他無線技術。UWB 提供前所未有的精準度 (公分級；以公分為單位計算)，能夠即時處理情境相關資訊 (例如 UWB 裝置之間的位置、移動及距離) 並在系統加入空間感知能力，將實現無數令人振奮的全新應用。瞭解 UWB 的潛能時，一定要考量 UWB 在測量飛時測距和到達角的獨特特性，並且要特別注意其安全特性。

以 UWB 爲基礎的汽車應用 － 更聰明的智慧型鑰匙

各家車廠在 2019 年下半年計畫推出以 UWB 為基礎的被動無鑰匙進入功能，並探索 UWB 技術實現的各種全新用途，例如車內乘客偵測、自動化代客泊車、免操作自動停車、停車場門禁及得來速付款 (drive-through payment) 等等。其中最受到期待掀起浪潮的 UWB 用途之一，就是透過智慧型手機操作的被動無鑰匙進入 (Passive Keyless Entry;PKE) 功能。

PKE 可解鎖及啓動汽車，無需使用實體鑰匙。您可將遙控鑰匙留在口袋或手提包中，一旦進入解鎖車門的適當範圍，就會由汽車「喚醒」遙控鑰匙，並於進入車內時偵測遙控鑰匙，啓動點火系統的發動按鈕。

PKE 遙控鑰匙十分方便，成為顧客高度期待的功能，受到汽車製造商歡迎。此外有了這項功能，方向盤柱就不必配備笨重的鎖心柱，不但減輕汽車重量，也能降低車輛撞擊時膝蓋受傷的風險。消費者也相當喜愛 PKE 功能，因為這樣就不需要四處尋找實體鑰匙開鎖、發動或上鎖車輛，讓生活更加便利。可惜現今的遙控鑰匙也受到竊賊喜愛，他們可以輕鬆取得各種便宜的駭客裝置偵測車輛的喚醒訊號，將其引導至鑰匙加以喚醒，強制發出開門訊號。這就是所謂的遞接式攻擊 (relay attack)。

由於現今有部分遙控鑰匙是使用訊號強度而非時間戳記，偵測車主是否進入車輛兩公尺範圍內，讓遞接式攻擊能夠得逞。這種攻擊通常是由兩人進行，一個人在您的鑰匙附近，另一個人則在您的車子附近。例如您外出前往購物中心、咖啡廳或餐廳時，或是在家但將車鑰匙留在車道或窗戶附近，第

圖 1：遞接式攻擊複製訊號用於開鎖

(資料來源：NXP 恩智浦)

一位竊賊會在與鑰匙距離夠近的位置，傳送與汽車偵測鑰匙時傳送的相同詢問訊號。如果您的鑰匙回應詢問訊號，就代表鑰匙位在範圍內，這樣第一位竊賊就會攔截回應訊號，然後將其傳送 (或遞接) 至車旁的第二位竊賊，由第二位竊賊使用前述攔截的回應訊號誘騙車子解鎖及發動 (圖 1)。

在 PKE 遙控鑰匙加入 UWB 技術，並使用智慧型手機存取後，飛時測距 (Time of Flight ;ToF) 計算可有效對抗遞接式攻擊。竊賊攔截的任何訊號都會標示時間戳記，代表訊號是在範圍之外產生。這樣訊號抵達車輛且計算行進時間後，就會顯示訊號產生的地點太遠，無法開啓車門。這就像是持有電影日場門票的觀眾，由於票券時間錯誤且超過時間，無法入場觀看夜場電影；竊賊竊取的 UWB 訊號無法用於進入車輛，因為訊號顯示的時間錯誤，而且基本上已經逾時。

UWB 緣起及現況

UWB 最初是在 1960 年代開發供雷達應用，之後經調整作為正交頻分多工 (orthogonal frequency-division multiplexing, OFDM) 技術，並於 IEEE.15.3 標準化成為超高資料速率傳輸技術，最高可達 480Mbps。UWB 以這種規模的容量與 WiFi 直接競爭，但其資料傳輸功能很快就敗下陣來，成為傳輸用途的局外人。UWB 的下個角色為脈衝無線電技術，遠比之前更加成功。這項技術獲得 IEEE 802.15.4a 指定，使用 2ns 脈衝測量飛時測距和到達角。不久之後其安全功能擴大應用範圍，延伸方案獲 IEEE 802.15.4z 指定 (PHY/RF 層級)，使其成為獨特且安全的精確測距與感測技術。

使用智慧型手機作為智慧型鑰匙進入及發動車輛的概念非常具有吸引力，因此主要的汽車及智慧型手機業者，都積極參與在 802.15.4z 標準定義安全機制。UWB 如何以這樣的精準度，掌握如此重要的用途？以下將探討 UWB 的背景及來龍去脈。

UWB 爲何能成爲不同的無線技術

有別於大部分無線技術，超寬頻 (UWB) 技術是透過脈衝無線電運作，在寬廣的頻帶範圍內使用一系列脈衝，因此有時也稱為 IR-UWB 或脈衝無線電 UWB。相較之下，衛星、Wi-Fi 及藍牙在狹窄頻率使用調變正弦波傳輸資訊。

UWB 脈衝具有多項重要特性。首先 UWB 脈衝陡峭狹窄，即使在充滿雜訊的頻道環境中，也能產生易於識別的尖峰。此外對 ToF 測距測量而言，UWB 脈衝比 WiFi 或 BLE 等其他技術更適合用於密集的多重路徑環境。經由一條以上路徑抵達接收器的無線電訊號，由於受到主訊號路徑附近物體的反射或中斷，可利用 IR-UWB 輕鬆區別，但使用窄頻系統則需耗費大量時間，而且能力有限。

UWB 於不同區段的無線電頻譜運作，遠離 2.4 GHz 周圍繁忙的 ISM 頻帶。用於定位及測距的 USB 脈衝，是在 6.5 及 8 GHz 之間的頻率範圍運作，不會干擾頻譜其他區段的無線傳輸。這代表 UWB 能與現今最熱門的無線形式共存，例如衛星導航、Wi-Fi 及藍牙。

如果在一般功率水準下運作，距離最長可達 10 公尺，不過如果使用更高功率的脈衝，UWB 甚至可達到 200 公尺的範圍。UWB 通訊也能輸送資料，其中 UWB 封包的酬載部分，能以約 7 Mbps 的速率傳送資料，並可大幅擴充達到 32Mbps。

UWB 目前使用時間非常短的 2ns 調變脈衝列，脈衝間距可能為統一或非統一，脈衝重複頻率 (PRF) 範圍可由每秒數十萬到數十億脈衝。一般支援的 PRF 為 62.4MHz 及 / 或 124.8MHz，通常分別稱為 PRF64 及 PRF128。UWB 的調變技術包括脈衝位置調變及二元相移鍵控。

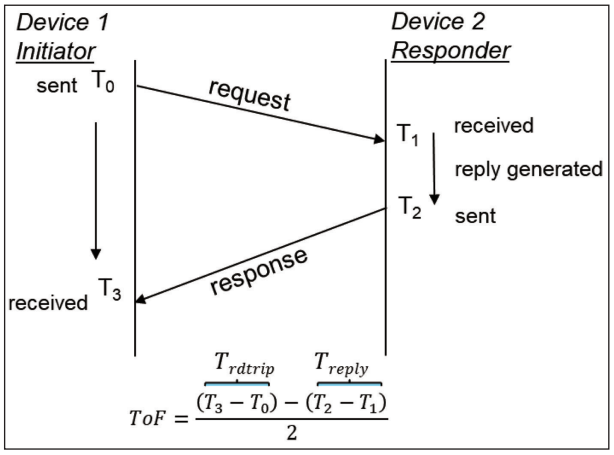
定義脈衝重複頻率

- ■脈衝發射器以開啓關閉的方式，在特定速率 (PRT 或 PRF) 提供峰值功率 (Ppeak)。
- ■最大範圍與發射器輸出功率直接相關，系統發射越多能量，目標偵測範圍就越大。

飛時測距 (ToF) 計算

在科學及軍事應用中，判定兩點 (或裝置) 之間水平距離的程序稱為測距。飛時測距 (ToF) 是一種測距形式，使用訊號行進時間計算距離。圖 2 提供基本說明，協助瞭解 ToF 計算在兩個配備 UWB 功能的裝置之間如何運作。

圖 2：適用於 UWB 的飛時測距計算，其中裝置 1 為控制者，裝置 2 為受控者



(資料來源：NXP 恩智浦)

計算飛時測距 (ToF) 時，需要測量訊號從抵達點行進前往點 B 的時間。我們取得訊息來回時間的來回讀數，其中包括裝置 2 的處理時間，然後從中減去處理時間並除以 2，就可得到 ToF。為了判定行進期間所涵蓋的範圍大小，因此將 ToF 乘以光速。

由於 UWB 具備高頻寬 (500MHz)，因此脈衝是以奈秒寬為單位，可提升精準度。使用窄頻收發器的 WiFi 及 BLE 技術，其 ToF 及測距準確度有限，約為 +/-1m 至 +/-5m，但 UWB 可達到 +/-10cm 之內。

由於 UWB 訊號獨特且易於讀取，因此即使在多重路徑環境中，也能在脈衝抵達和離開時輕鬆識別，並達到高度確定性。UWB 能以出色的高傳輸速率精準追蹤脈衝，以短脈衝串傳送大量脈衝，因此即使在非常靠近的範圍內，也能提供精細的 ToF 計算。

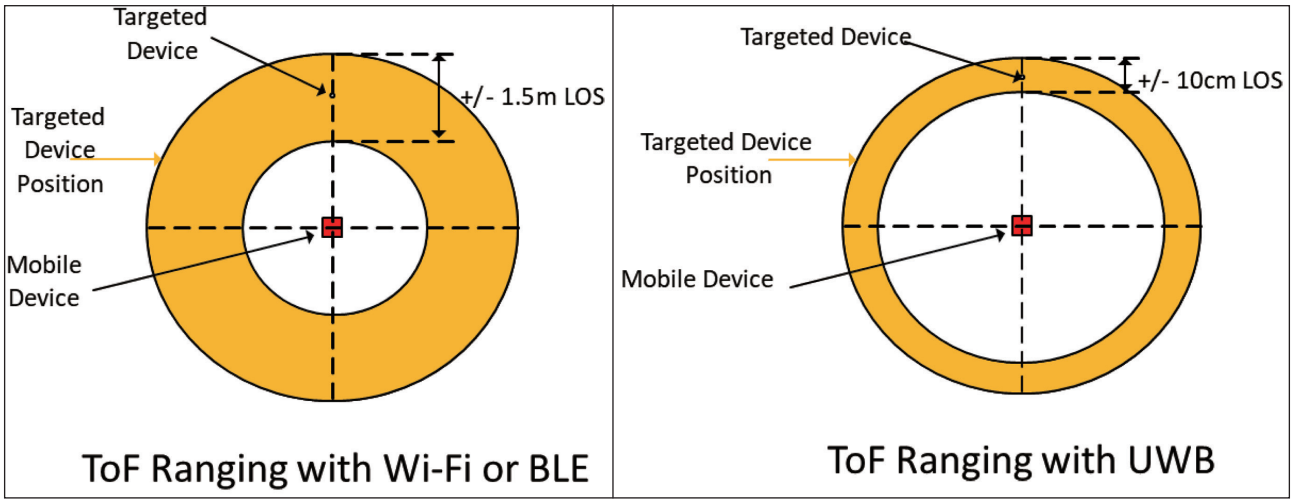
調變正弦波的多重路徑分量，是在使用 Wi-Fi 或藍牙技術定位時產生，只能透過複雜方式加以區別。這正是 Wi-Fi 及藍牙測量結果準確度難以低於 1 公尺的原因之一。

圖 3 顯示 UWB ToF 計算結果與 Wi-Fi 和藍牙計算結果的比較情形。

選用的到達角 (AoA) 計算

有一點很重要，就是 ToF 計算判定的是徑向距離，並不是判定方向。也就是說 ToF 計算可讓裝置 1 瞭解裝置 2 距離多遠，但並不知道方向，無法瞭解是在前後左右還是東南西北。因此 ToF 圖為圓形：如果 ToF 計算顯示裝置 2 與裝置 1 距離 15 公分，則裝置 2 的可能位置，就在以裝置 1 為圓心向每個方向測量 15 公分的圓形範圍內。其中可能需要額外

圖 3：使用 Wi-Fi 和 BLE 對比 UWB 的 ToF 測距結果

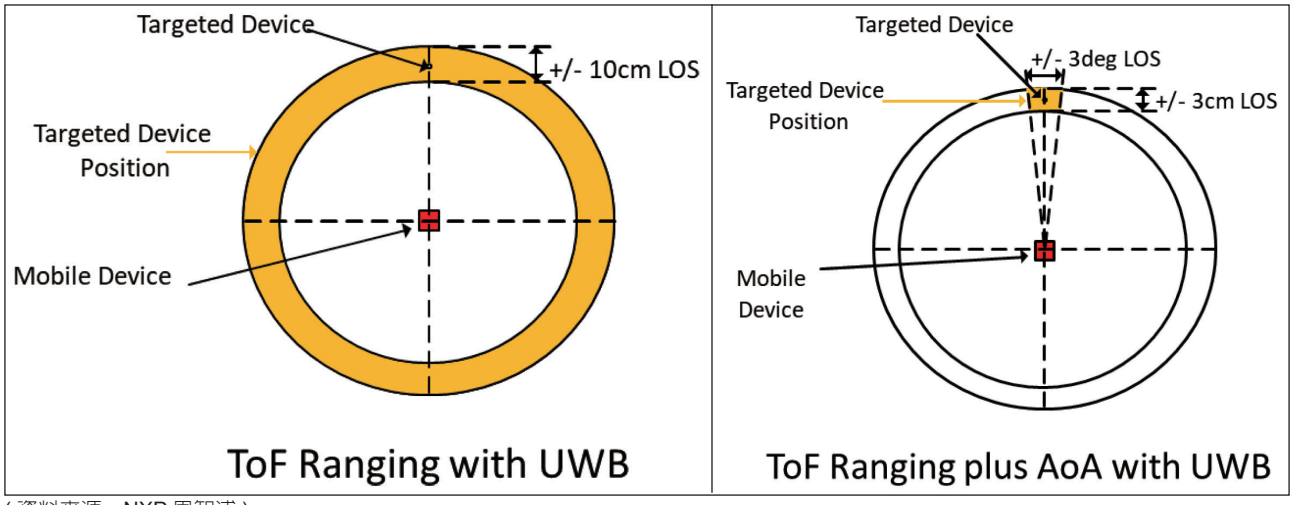


(資料來源：NXP 恩智浦)

裝置，利用兩個距離圓圈的相交部分，透過第二次測量的方式判定位置。

因此為了讓 UWB 技術的討論內容更齊全，我們應考量目前非汽車應用的一項重要層面：到達角 (AoA)。這項資訊有助於判定裝置 2 在圓圈之中的位置。如欲計算 AoA，裝置 1 必須配備一組精心定位

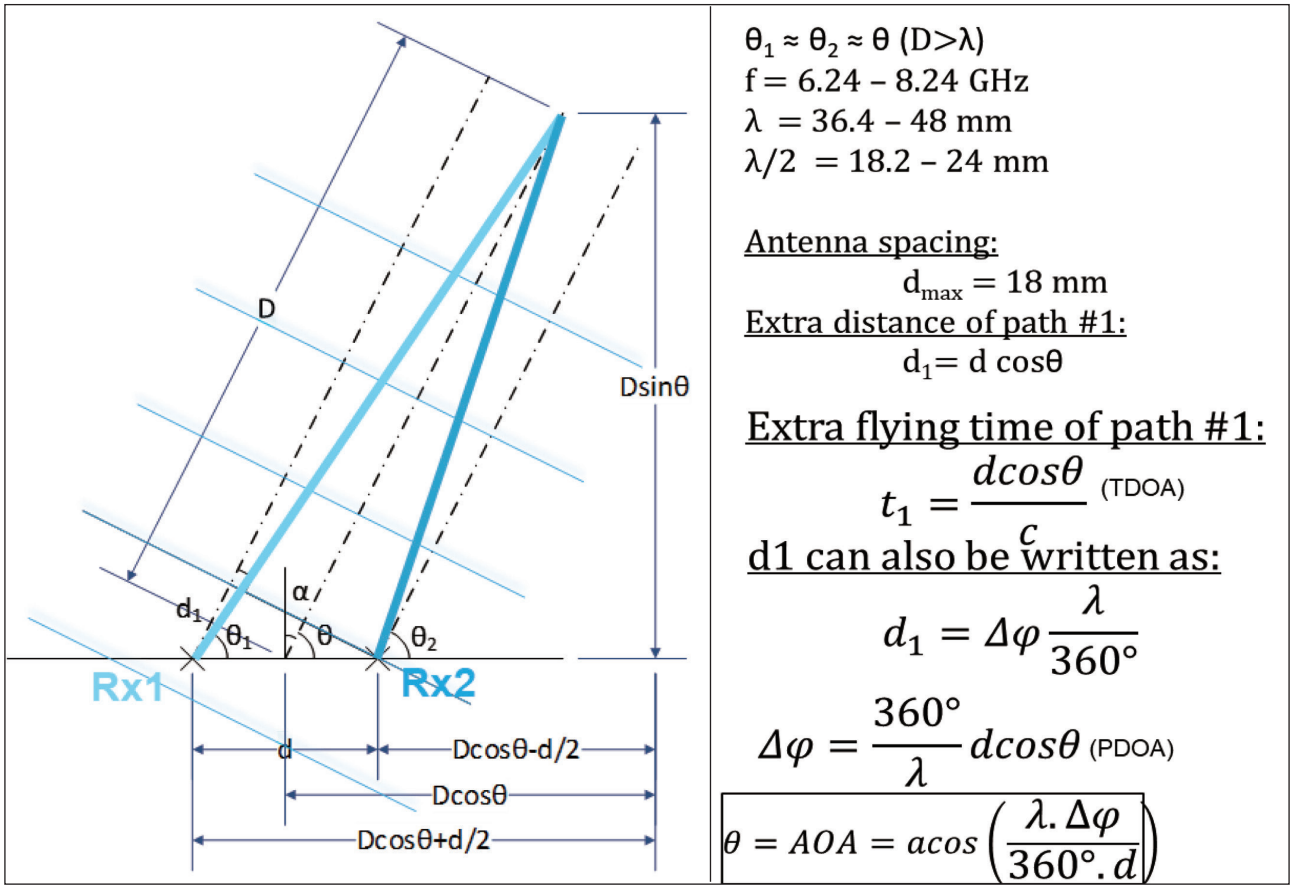
圖 4：ToF 測距搭配 AoA 可產生高準確度結果



(資料來源：NXP 恩智浦)

圖 5(左)：裝置 1 配備兩個 AoA 天線 Rx1 及 Rx2 的範例

圖 5(右)：AoA 計算使用抵達時間和天線間距判定各個傳入訊號角度



(資料來源：NXP 恩智浦)

(資料來源：NXP 恩智浦)

的專屬天線，專門用於 AoA 測量。並非所有 UWB 解決方案都包含額外天線，不過如果設置額外天線，就可大幅提升準確度達到數公分的範圍 (圖 4)。

AoA 計算為獨立進行，與 ToF 計算不同，但兩者的類似之處在於：以脈衝計時開始進行。AoA 陣列每個天線所接收的每個訊號，在抵達時間及相位方面都有微小但可識別的差異。每個訊號的抵達時間及相位將記錄用於類似三角測量法的幾何計算，協助判定訊號來源。

圖 5 左圖顯示裝置 1 配備 Rx1 及 Rx2 兩個 AoA 天線的範例。訊號從裝置 2 到達 Rx1 的時間比 Rx2 長，代表 Rx1、Rx2 及訊號來源形成的三角形偏向右側，亦即訊號來自裝置 1 的東北方。

訊號由裝置 2 前往裝置 1 時，到達 Rx1 的時間比 Rx2 長。圖 5 右圖所示的 AoA 計算，利用抵達時間及天線間距判定各個傳入訊號的角度，並以 Rx1、Rx2 及裝置 2 繪製三角形。此範例的三角形在 Rx1 部分的邊較長，並且指向右側，代表裝置 2 位於裝置 1 右側。

UWB 如何管理安全性

UWB 最重要的附加功能之一，就是定義成為未來 802.15.4z 規格的一部分，成為實體層 (PHY) 傳送及接收資料封包的額外部分。這項新功能是由恩智浦開發及推薦的技術為基礎，稱為混碼時間戳記序列 (Scrambled Timestamp Sequence) 或 STS。其中加入密碼、隨機數產生及其他技術，讓外部攻擊者更難以存取或操控 UWB 通訊。

保護 ToF 計算

飛時測距計算很容易受到遠距操控。如果您可以干擾計算的時間戳記或其他層面，就可以讓計算所得距離看起來比實際上更靠近。這對特定應用是一項嚴重問題，例如安全門禁系統；如果系統受騙認為有權進入的使用者接近，但其實並非如此，就可能觸發開啓不該打開的鎖。

用於測距的原始 UWB 標準 802.15.4a，是在十多年前發佈，其中並未依據現今標準重視安全問題。在測試 4a 標準時，研究人員發現外部攻擊者能夠縮短高達 140 公尺的測量距離，機率超過 99%。各界對這項特定漏洞感到憂慮，成為推動修訂提出 4z 標準的原因之一。

其中的概念在於讓 ToF 相關資料無法存取或預測，在實體層封包加入加密金鑰及隨機數字。這有助於對抗各種外部攻擊，包括 Cicada 攻擊、前序編碼注入攻擊，以及早期偵測 / 後期連線 (Early Detect/Late Connect，EDLC) 攻擊，其中使用原始 UWB 實體層的決定性及可預測特性操控距離讀數。更新後的測量方法提供最佳保護，對抗以操控距離測量為目標的暴力攻擊法。 CTA

微軟 Office 2010 將在 2020 年 10 月 13 日終止支援服務

繼 Windows 7 之後，微軟宣布 Office 2010 將於 2020 年 10 月 13 日終止支援服務，一旦終止支援後，企業將不再接受到微軟提供的安全性更新服務和線上支援等多項服務協助。此外，Windows 10 最新更新 (版本 2004)，將於今年五月正式發布，帶來多項功能更新，讓使用者體驗再升級。

Office 2010 支援服務將於 2020 年 10 月 13 日終止，Office 2010 應用程式仍然可繼續運作，但將不會再接收到微軟提供的安全更新、修補程式等延伸安全性更新服務。

微軟將不再為 Office 2010 用戶提供報告或發現的弱點技術支援、錯誤修正或安全性修正，且不再提供可協助保護 Office 2010 用戶電腦不受病毒、間諜軟體和其他惡意軟體威脅的安全性更新服務

微軟未來將不再提供 Office 2010 用戶大部分的線上協助內容，用戶將不再獲得電話或對談提供技術支援，不再收到 Microsoft Update 提供的 Office 2010 軟體更新，更無法再從 Microsoft 網站下載 Office 2010 。