摘要

在支援大量移動和物聯網設備的下一代（5G/6G及更高）網絡中，實現所需的用戶體驗質量（QoE）一直是一個主要關注的問題，特別是需要低延遲和無縫連接。因此，頻譜稀缺成為實現期望QoE的主要挑戰。為了滿足QoE需求，頻譜共享系統被視為下一代無線網絡的主要推動者。具體而言，第三代合作夥伴計劃（3GPP）已經標準化了在未經授權的5 GHz頻段中支持4G LTE授權輔助接入（LAA）網絡與WiFi的共存，以及在6 GHz頻段中支持5G New Radio Unlicensed（NR-U）與WiFi 6/6E的共存。

儘管大多數當前的共存解決方案和標準侧重於性能提升和QoE優化，但文獻中卻忽略了這些網絡環境的新興安全挑戰。獨立網絡（無論是5G還是WiFi）的安全框架假設從頻譜到核心功能的整個網絡資源的所有權。因此，在網絡內部安全系統內進行的對網絡的所有訪問均應經過身份驗證和授權，否則將被視為非法。然而，共存網絡環境可能導致前所未有的安全漏洞和侵犯，因為獨立網絡必須容忍未知和超出網絡範圍的訪問，特別是在媒體訪問方面。

在本文中，我們首次在文獻中回顧了在5G/WiFi共存網絡環境中出現的一些關鍵和新興的安全漏洞，這些漏洞在獨立網絡中以前未曾觀察到。具體而言，獨立的媒體訪問控制（MAC）協議以及由此產生的隱藏節點問題可能導致服務阻斷、惡意基站的部署和竊聽攻擊等濫用。我們從物理層身份驗證、網絡訪問安全和跨層身份驗證機制的角度研究了潛在的漏洞。這項研究開辟了一個新的研究方向，即分析和設計一個能夠應對共存網絡獨特挑戰的安全框架。

簡介

由各種異構設備產生的數據激增，包括智能手機、移動計算機、物聯網設備、自動駕駛車輛和智能基礎設施，一直是5G網絡發展的主要驅動力[1, 2, 3, 4]。這種以數據為中心的通信網絡觀念導致了服務基於架構（SBA）。SBA允許在雲端實現網絡功能，從而促進數據管理，同時提高了5G以外（B5G）網絡的可擴展性和可編程性[5]。網絡的初始架構已經被優化，以實現在5G網絡文獻中占主導地位的高用戶體驗（QoE）作為主要性能指標[6]。然而，安全架構的適應速度未能與支持QoE需求的新無線技術同步。這可能以新的安全威脅形式或擴大現有漏洞的攻擊面的方式開啟了嚴重的安全漏洞之路。

與低延遲和高數據速率的無縫連接對大量異構設備的支持通常被視為5G網絡的獨特特徵。QoE旨在根據這些需求評估5G網絡的性能。有關QoE的一個被廣泛接受的概念是基於用戶需求及時交付內容。因此，它是一個比傳統的服務質量（QoS）更高層次的目標，其特徵是提供給用戶的數據速率和延遲等指標。儘管QoE的定義很廣泛，並且在測量的系統化指標上尚無共識，我們注意到安全和隱私也是用戶體驗的重要方面。在這個觀點下，我們可以將網絡優化的問題視為在考慮問題的安全和隱私約束條件下最大化QoE，從而實現所需的QoS。

多種無線訪問技術（RAT）是5G網絡獨特特徵的一個突出例子，其目標是實現高QoE。然而，不同應用的頻譜稀缺，以及不同射頻傳播範圍的要求，是一個主要挑戰。重新分配未充分利用的頻譜帶是一個極具時效性的過程，面臨著現有用戶的抵制，並可能干擾至關重要的軍事和政府用途。頻譜共享是解決頻譜稀缺的一個有前途的解決方案，被認為是實現B5G網絡高QoE的一個主要推動者。

在美國，頻譜共享的早期例子包括商業利用電視白空間（TVWS）頻譜（基於位置的共享）和公民寬頻服務（CBS）與現有的海軍雷達和固定衛星系統共享3550-3650 MHz頻段[6]。3GPP還為LTE授權輔助接入（LAA）和增強的LAA標準化了在未經授權的5 GHz頻段中WiFi和4G蜂窩網絡之間的頻譜共享[7]。美國聯邦通信委員會（FCC）和歐洲委員會還批准了在6 GHz未經授權頻段進行頻譜共享。因此，3GPP為5G網絡中的New Radio Unlicensed（NR-U）在所謂的綠田頻譜上與IEEE 802.11ax標準的WiFi 6（基於IEEE 802.11ax標準）和在6 GHz頻段操作的WiFi 6E（網絡）共存）定義了頻譜共享規範[8]。

現有的網絡安全架構是基於獨立的獨立網絡擁有從頻譜到基礎設施的整個網絡資源的假設而設計和開發的。在本文中，獨立網絡指的是具有對頻譜的專屬訪問權限，並且不具有來自共存實體的任何網絡外傳輸的網絡基礎設施（基站和用戶設備）。在這種安全模型中，對頻譜和資源、通信流量和網絡活動的任何訪問都在單一網絡的安全框架內進行身份驗證和授權。

然而，5G網絡的出現，利用軟體定義網絡（SDN）和網絡切片需要在多個運營商和服務提供商之間共享網絡基礎設施，並具有不同的安全策略和隱私需求。因此，在核心網絡層面各種安全系統之間的互操作性已經成為一個具有挑戰性的問題。同樣，網絡的共存（WiFi和5G），以及通常的下一代頻譜共享系統，要求在多個私有實體之間共享頻譜。因此，在訪問網絡層次上對網絡外活動的寬容度也是至關重要的。

在共存網絡環境中的無保護頻譜共享為潛在的對手提供了一個無法被現有獨立網絡中的現有安全機制檢測的隱蔽通道。這個隱蔽通道為網絡上的安全攻擊提供了新的表面，沒有保護機制。獨立網絡的安全系統觀察和響應網絡內活動，而頻譜共享程序涉及網絡外的頻譜訪問。因此，沒有安全機制的頻譜共享允許攻擊者利用隱蔽通道部署新的安全攻擊和/或使用更高強度和更簡單的實現機制進行現有已知攻擊。

在本文中，我們專注於共存視角，研究了物理層和訪問網絡中的安全挑戰和攻擊。據我們所知，這是文獻中首次強調並專注於共存對無線網絡安全的影響的研究。為了了解無保護的頻譜共享可能促使和/或加劇哪些類型的安全攻擊，我們首先回顧了獨立5G和WiFi網絡中存在的一些現有漏洞。接下來，我們將討論由於無保護的頻譜共享而可能出現的一些安全挑戰。

最後，我們討論了在保護獨立網絡隱私的同時，具有加密證明的安全共存所面臨的挑戰。

5G和WiFi 6/6E中的漏洞

在無線網絡中，安全性和隱私是相互交織的概念。隱私指的是通過被動觀察傳輸信號來推斷有關用戶的信息[9]。這些信息可以簡單地包括用戶的位置和網絡流量。文獻中的被動竊聽攻擊等效於對無線通信的隱私攻擊，特別是在物理層。竊聽攻擊通常指的是在無線通信中的物理層攻擊，而隱私是一個更通用的術語，主要用於數據庫。

在本文中，由於頻譜共享的原因，我們將這兩個術語交替使用，焦點是無線通信中由於頻譜共享而產生的漏洞。

在無線通信的背景下，安全性通常涉及主動攻擊，例如，對手引入提高的干擾或智能阻塞信號以操縱用戶傳輸。主動攻擊的突出例子包括強迫設備使用替代的數據通道，例如改變MIMO波束成形系統中波束的方向，或通過干擾替代頻段的方式改變頻率通道。這些攻擊反過來可以用於部署中間人攻擊（MitM）、惡意基站、DoS等。本調查的重點是頻譜共享漏洞，主要引發了無線網絡的物理層和MAC層的安全/隱私問題。

2.1. 物理層安全性

在現有標準中，用於安全通信的加密證明是由通信協議堆疊中不同層次的安全協議提供的。這些安全條款始於身份驗證（用於用戶/設備識別）、金鑰協商協議，以及在第2層（OSI模型中的鏈路層）進行的通道加密。盡管物理層的安全性一直是一個活躍的研究領域，但由於RF傳播通道的變異性和不確定性、設備變異，以及在身份驗證之前（身份驗證）需要為大量設備進行分散秘密金鑰管理等挑戰，標準化框架在這一層次上缺乏安全證明。

實現加密的物理層的一種經典方法是使用展頻系統，無論是在時間還是頻率域。在直接序列展頻系統（DSSS）中，傳輸信號的時間域樣本被編碼為具有遠大於位周期的展頻碼。如果展頻碼是秘密的或加密的，DSSS系統除了具有對干擾的抵抗力和防欺騙特性之外，還在物理層提供身份驗證和保密性。一個著名的加密DSSS物理層的例子是全球定位系統（GPS）的Y碼和M碼軍用信號[10]。

多載波展頻（MCSS）是頻率域中直接序列展頻（DSSS）的等效物。MCSS系統主要因其能夠充分利用正交頻率分割多工（OFDM）和碼分多址（CDMA）在頻譜效率和對多徑衰落和干擾的強健性方面而受到歡迎[11, 12, 13]。在MCSS物理層中，OFDM信號的子載波使用展頻碼進行編碼。通過在頻率域中加密OFDM的基頻信號樣本或子載波，可以使用類似的方法實現加密的物理層[14, 15, 16, 17]。

2.1.1. 信息理论安全性

通道編碼已成為通信協議堆疊中物理層的不可避免的組件，用於增強和鞏固鏈路可靠性。3GPP規範在5G增強型移動寬帶（eMBB）網絡的數據通道和控制通道分別使用低密度奇偶校驗碼（LDPC）和極化碼。這些編碼方案也已被證明在窺探通道模型中提供信息理論安全性[18, 19, 20, 21]。

傳統的密碼和加密算法（包括公鑰和對稱密鑰）基於窺探者在不知道秘密密鑰的情況下嘗試解碼加密消息的計算複雜性，提供了安全性證明。信息理論安全性依賴於合法接收者和窺探者觀察到的不同通道條件。保密容量被定義為從發射機到預期接收者和從發射機到窺探者的通信通道的（信息理論）容量之間的差異。直觀地說，如果合法接收者觀察到的通道容量更大，則它可以攜帶窺探者無論其可用的計算能力如何都無法接收的信息。

通道編碼方案提供的信息安全性基於強密碼或弱密碼進行評估。如果窺探者接收的消息的傳輸碼和窺探者的互信息趨近於零（對於漸近長碼字），則可以獲得強密碼。弱密碼是指傳輸碼的每比特的平均互信息趨近於零的條件。實現窺探者通道容量的編碼方案也可以提供完美的保密性。基於這種關係，[22]和[23]引入了實現弱密碼的LDPC碼的設計。此外，[24]中引入的LDPC碼在預期接收者觀察到的通道無噪聲時提供強密碼。所有這些方案都假定窺探者通道的模型為二進制擦除通道（BEC）。

極化碼也已被證明在二進制無記憶通道中實現弱密碼，當窺探者的主通道不強於預期接收者的主通道時[25, 26, 27]。在二進制無記憶通道中，引入了一種多塊極化編碼方案，該方案實現了強密碼以及可靠性[28]。此外，[29]和[30]中的極化碼在提供強密碼的同時實現了具有機密信息的廣播通道的容量區域（在離散無記憶模型下）。[31]和[32]分別研究了極化-極化和極化-LDPC碼的串聯，以實現到保密容量的最小差距。

由於信息理論安全性依賴於通信通道條件，因此可以通過侵入RF環境的攻擊者進行操控。即使是被動窺探者也可以利用更先進的RF信號處理技術來優於合法接收者。儘管保密容量是通道中信息流的理論極限，但它仍然取決於接收信號到干擾和噪聲比（SINR）。接收信號的質量還取決於天線增益、RF前端噪聲指數、信號同步、過濾和解碼算法。因此，通過使用更高質量的RF前端電路、具有更高增益天線的波束形成，以及更先進且可能具有更高計算複雜性的信號處理算法，窺探接收者可能建立一個與合法接收者接近質量的通信通道。在這方面，我們指出信息理論安全性並不完全獨立於接收器的複雜性。

主動窺探者還可以通過降低合法接收者的通道條件，嚴重影響通道的保密性。窺探者可以在保持自身接收者的通道條件不變的情況下，簡單地增加合法接收者的干擾水平。這種攻擊可以通過使用自我干擾消除技術[33, 34]或針對合法接收者的定向干擾的波束形成來實現。我們注意到，在共存網絡環境中特別容易增加干擾水平，在這種環境中，將容忍來自未知源（來自共存網絡的干擾）的更高水平的干擾。因此，主動窺探者可以將保密容量降低到零。

另一種替代的主動窺探者可能會降低通道狀態信息（CSI）的估算。通道編碼方案在提供承諾的保密速率時需要對CSI進行完美的了解。在大多數無線網絡中，通常在定期的訓練階段使用導航信號來估算CSI。主動窺探者可能僅在訓練階段進行干擾，這種攻擊稱為導航污染，以降低通道估算的質量[35, 36]。在[37]中對時分雙工（TDD）網絡的導航污染攻擊已經顯示，它將將下行傳輸的保密速率降低到接近零。

2.1.2. 波束成形

波束成形是5G網絡中新無線電（NR）物理層的主要特徵之一。波束成形的主要承諾是通過提高鏈路可靠性，實現顯著更高的數據速率。波束成形通過提供大的天線增益、形成直接的視線通道以減輕多徑衰落，以及減少由於空分雙工而引起的干擾，從而增加信號到干擾和噪聲比（SINR）（因此提高可靠性）。然而，一系列的研究也聲稱使用波束成形來增強物理層安全性。直觀地說，波束成形允許在發射機和預期接收者之間構建高度定向（因此是秘密的）通道，最小化信息（信號功率）泄漏到其他方向。

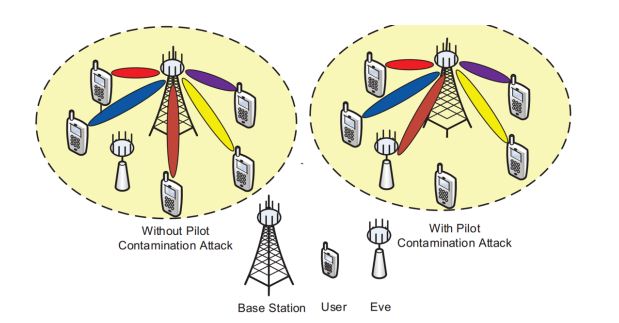


圖1：導航污染攻擊，其中主動窺探者導致基站波束指向攻擊者（Eve），而不是預期的用戶[18]。

從信息理論的保密觀點來看，波束成形導致信號功率的高度定向傳輸以及減少的多徑衰落效應使得預期接收者的通道條件得以鞏固，而同時對於位於不同方向的窺探者而言，通道條件顯著下降。因此，波束成形增加了保密容量，潛在地提高了數據安全性。例如，[38]的模擬結果顯示，在毫米波通信中使用波束成形可以達到每秒多吉比特的保密速率。

窺探者還可以利用波束成形來形成中間人（MitM）位置，通過與合法發射機和接收機建立秘密通道。這樣的攻擊者對於合法網絡用戶難以檢測。這與全向通信形成對比，其中窺探者和合法發射機的發射都可以被相應的接收機檢測到。在這種情況下，分析傳輸模式可以揭示主動攻擊者的存在。然而，波束成形潛在地可以促使MitM攻擊位置的出現。

除了MitM攻擊者之外，通過波束成形實現的可靠性和保密容量也可能因為類似於CSI估算的導航污染攻擊而明顯降低。在這種情況下，主動窺探者使用導航污染攻擊使方向性波束偏離預期接收者的方向，轉向其自身接收器。這種攻擊顯示在圖1中。攻擊者（Eve）在基站的培訓（通道估算）階段引起干擾。由此產生的基站波束被指向Eve而不是合法用戶。在這種情況下，合法接收者觀察到的通道條件優於窺探者，保密速率顯著降低[39, 40]。此外，由於偏離的波束方向，提供給預期接收者的更高通道容量也會降低。

另一種替代的被動窺探者可能會利用定向波束的反射，來危害波束成形提供的數據安全性。研究已經顯示，高度定向的毫米波的反射可以被窺探者利用，顯著降低保密容量[41]。該研究在毫米波軟體定義無線電（SDR）平台上進行實驗，以展示厘米尺度的物體或設備（如手機或筆記型電腦）的金屬表面可以產生足夠強度的反射，將保密容量降低32%。此外，在預期接收者方向上存在小信號阻塞的情況下，保密容量可能降低至零。

2.2. 5G接入安全性

在無線網絡中，接入安全性由構成第2層安全性基礎的認證和金鑰協定（AKA）來保護。3GPP標準定義了一個可擴展的認證協定（EAP），稱為EAP-AKA'，用於將非3GPP接入網絡與4G網絡集成。一個廣泛使用的非3GPP接入網絡是WLAN，它在WiFi Protected Access（WPA2）中也使用了EAP框架。EAP-AKA'也是5G網絡中支持的接入安全機制之一，另外還有一個非常相似的協議5G-AKA [42, 43]。主要的區別在於5G-AKA中，serving network的SEAF在將UE的響應發送到home network之前也會對其進行驗證。

EAP-AKA'的整體流程如圖2所示。以下我們將回顧對接入網絡安全性的幾種攻擊。

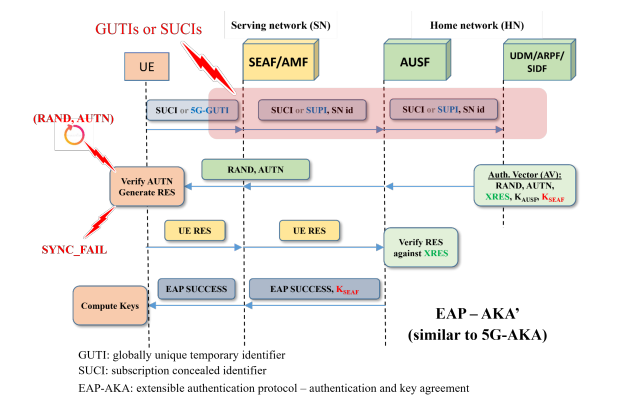


圖2：基於可擴展認證協議（EAP）的5G網絡接入安全，以及協議的不同攻擊點。

2.2.1. 身份保密性

不同世代的蜂窩網絡在保護用戶身份方面投入了大量努力。國際移動用戶身份（IMSI）是SIM卡的唯一身份識別。在5G網絡中的等效標識符是用戶永久標識符（SUPI），它不僅限於蜂窩服務，還可以在不同的5G環境中使用，如物聯網（IoT）網絡[44]。為了保護用戶的隱私，5G網絡使用訂閱隱藏標識符（SUCI），其中包含使用用戶家庭網絡的公鑰對SUPI的加密版本。在首次連接到網絡後（在此期間UE傳輸SUCI）並啟動無線通道加密後，UE被分配一個全球唯一的臨時標識符（GUTI），以防止頻繁傳輸SUCI。雖然定義了臨時標識符（如4G/5G網絡中的GUTI）降低了由於頻繁傳輸而暴露SUCI的可能性，但GUTI的值仍然有較長的生命周期。因此，暴露GUTI，例如通過竊聽通信通道，可能向敵對者提供用戶/設備的軟身份。特別是在結合攻擊中，用戶的位置隱私除了GUTI之外還受到影響，攻擊者可以攻擊用戶的隱私，並獲得諸如電話號碼、網絡活動、呼叫和短信等信息。此外，即使GUTI值得到刷新，攻擊者仍然可以跟踪用戶。因此，擁有長生命周期的GUTI的泄露可能產生與IMSI捕獲攻擊相似的效果。

儘管5G網絡使用SUCI和GUTI來保護設備的永久身份，但在5G網絡中仍然有可能讓UE以明文形式傳輸SUPI（或等效的IMSI）。在未經身份驗證的緊急呼叫情況下，無法保證SUPI的安全性，UE可能會傳輸明文的SUPI。緊急服務適用於無法進行身份驗證或無法進行身份驗證的情況。在共存網絡環境中，攻擊者可以主動訪問頻譜並引入故障，而不被識別為敵對者。因此，通過生成緊急情況，例如通過引入故障引起身份驗證失敗，攻擊者可以迫使UE以明文形式傳輸SUPI/IMSI。通過竊聽通信通道，攻擊者可以獲得IMSI。此外，攻擊者還可以設置一個流氓基站，冒充合法的gNB，使UE直接向攻擊者傳輸IMSI，以進行緊急服務請求。

2.2.2. 國際移動用戶身份（IMSI）破解

儘管5G網絡中使用的身份（SUCI）是加密的，但敵對者仍然可以使用不同技術的組合來破解隱藏的IMSI。IMSI是一個49位的標識符，其中18位是已知潛在攻擊者的通用國家代碼。此外，一種名為ToRPEDO（TRacking via Paging mEssage DistributiOn）的側通道攻擊可以用來恢復IMSI的7位，即使在每次呼叫後假定臨時移動用戶標識（TMSI）更改的情況下，也只需不到10次呼叫[45]。該攻擊基於追踪設備的呼叫分發的時間點（在低功耗空閒狀態下對待裝置進行掃描以查找待處理的服務）。與IMSI的7位相關的設備的呼叫分發的時間段對於蜂窩設備是固定的。因此，攻擊者可以通過觀察呼叫分發的時間點以及相應的IMSI的7位來驗證設備是否在附近（一種粗粒度的位置信息）。

IMSI的其餘24位可以通過利用5G身份驗證機制的安全弱點進行暴力攻擊而獲得。攻擊者擁有家庭網絡的公鑰後，可以通過加密對IMSI的猜測來伪造SUCI並將其發送到核心網絡進行識別。網絡的響應是AUTH\_REQUEST（身份在網絡中有效）或REGISTRATION\_REJECT（無效身份）。如果收到AUTH\_REQUEST響應，則將其轉發到設備以驗證所猜測的SUCI是否屬於受害者設備。設備的響應是AUTH\_RESPONSE（身份屬於設備）或AUTH\_FAIL（身份不正確）。一次真實的ToRPEDO攻擊在74小時內成功恢復了IMSI。

2.2.3. 位置機密性

上述討論的ToRPEDO攻擊可以提供有關蜂窩設備的粗粒度位置信息。攻擊者還可以使用RF信號處理技術，如到達角（AoA）估算和接收信號強度（RSS），以獲得和追踪設備的細粒度位置。一種稱為可追踪性攻擊的補充攻擊也可用於驗證特定設備（已經進行特徵化，例如使用ToRPEDO）是否在攻擊者附近。

可追踪性攻擊利用了5G網絡EAP身份驗證機制中的一個弱點，如圖2所示。通過竊聽設備在初始身份驗證期間的通信，攻擊者將挑戰消息（RAND，AUTN）與設備綁定。為了驗證設備的存在並跟踪其位置，攻擊者可以向設備重播挑戰消息。如果設備在附近，它將用SYNC\_FAIL消息回應[46]。因此，攻擊者可以在不需要與核心網絡進行消息交換的情況下追踪用戶。

2.2.4. 服務拒絕（DoS）

由於5G網絡預計將為大量設備提供連接，從移動設備到物聯網設備，因此DoS和分散式DoS（DDoS）也已成為更嚴重和有效的安全攻擊，具有更簡單的實現機制。這些攻擊屬於非侵入性精密網絡武器（UPCW）的範疇，它已經成為物聯網時代嚴重的網絡安全威脅。這些攻擊通常需要低的預先攻擊情報搜集和利用預先定位的漏洞，同時對網絡性能造成更有效的損害。UPCW攻擊可以消耗和過載網絡核心（如身份驗證服務器）和設備的資源，就像DDoS、電話服務拒絕（TDoS）和睡眠拒絕（DoSL）中的情況一樣。

5G網絡身份驗證協議的DoS攻擊目標的示例如圖2所示。攻擊者（惡意基站）可以向設備發送大量的身份驗證請求消息，從而過載設備的計算資源。另一方面，如果攻擊者向許多（IoT）設備發送這樣的消息（或通過安裝的惡意軟件強迫設備這樣做），那麼這些設備將向網絡核心（在服務網絡中的SEAF）發送其GUTIs。無論哪種情況，服務網絡都應將SUPI（對應於GUTI的）或SUCI發送到主網絡，以生成相應的身份驗證向量。只有在驗證設備的響應（RES）與預期響應（XRES）一致時，這些設備才能被驗證。如果在短時間內向網絡核心傳輸大量的身份驗證請求，則網絡的通信和計算資源將被耗盡。同樣，如果向設備發送大量的身份驗證請求，則它將被迫頻繁計算響應，從而過載其計算和電源資源。在物聯網設備的情況下，這導致電池的枯竭，即所謂的DoSL攻擊。

除了操縱設備以過載網絡外，攻擊者還可以收集大量的GUTIs和/或SUCIs，並向網絡核心發送身份驗證請求。此外，攻擊者可能使用帶有惡意軟件的惡意或感染的設備發送假SUCIs。如圖2所示，服務網絡應將SUCIs發送到主網絡，以解密隱藏的標識並驗證SUCIs的真實性。因此，攻擊者甚至不需要與設備通信。

2.2.5. 移交安全性

在動態環境中，移交過程的安全性對於5G（以及更高版本）和WiFi（特別是廣域和企業）網絡來說是一個主要挑戰。特別是在高移動應用中，複雜的身份驗證和握手協議的延遲是無法容忍的。另一方面，在移交過程中，設備最容易受到安全攻擊，例如惡意基站和DoS，因為它們的連接性最弱。現有的安全架構利用初始身份驗證過程作為簡化移交過程安全機制的信任基礎。雖然這種方法與未來零信任架構的觀點相悖，但它滿足對於對延遲敏感的應用至關重要的延遲要求。

5G網絡中移交期間的安全握手過程如圖3所示。當基於路徑檢測、信道條件和用戶位置做出從源gNB到目標gNB的移交決策時，就啟動了安全握手。源gNB使用密鑰導出函數（KDF）使用物理小區ID（PCI）和絕對無線電頻率通道號（ARFCN）從當前密鑰KgNB派生會話密鑰K

∗

gNB。然後，源gNB將新密鑰和下一跳連鎖計數器（NCC）發送到目標gNB。該過程提供前向安全性；擁有當前密鑰不會揭示有關先前會話密鑰的信息。但是，不能保證後向安全性；如果攻擊者犧牲了源gNB，則所有未來的會話密鑰都將被揭示。為解決這個問題，移交機制還包括設備切換到目標gNB後的gNB內部過程（在用戶設備和目標gNB之間）。然而，gNB內部過程仍然帶來大量的通信開銷和計算複雜性。

上述移交過程的一個主要弱點是由於惡意基站（gNB）的重播消息而導致的失敗。攻擊者攔截gNB之間的第一條消息，即（K

∗

gNB，NCC），並在UE即將在兩個gNB之間切換時重播此消息。目標gNB無法驗證此消息的真實性。因此，它使用與UE一起收到的會話密鑰。它還將接收的NCC傳送回UE。然而，這個NCC與UE的本地計數器不同（因為它是一條重播消息），因此移交失敗。在一種類似的攻擊中，稱為干擾或解同步攻擊，對手可以更改NCC的值，這同樣導致移交失敗。這些攻擊是通過在移交過程中激活的惡意gNB實現的。

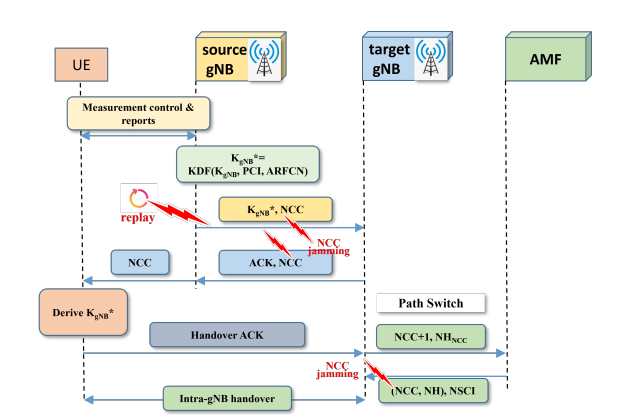


圖3：5G網絡中移交的安全協議，顯示了重播和干擾攻擊的不同弱點。

2.3. WiFi 6/6E存取安全性

WiFi網絡的存取安全性也是基於第2層的安全性（身份驗證），就像5G網絡一樣。在第三代中，WiFi系統利用WPA2中的EAP基礎身份驗證框架，而WiFi的第四代則採用基於IEEE 802.11標準化的Simultaneous Authentication of Equals（SAE）的WPA3。雖然WPA2框架存在與5G網絡相似的EAP漏洞，但由於計算複雜性較高，WPA3也容易受到降級攻擊、DoS和側信道攻擊的影響。以下我們將簡要回顧對使用WPA2和/或WPA3保護的WiFi網絡的存取安全性進行的一些攻擊。

2.3.1. 惡意存取點（AP）

對WiFi網絡存取安全性的一種眾所周知且有效的攻擊是惡意存取點，通常被稱為惡意孿生（evil twin）[48, 49]。由於AP的信標（beacon）包未加密，攻擊者可以輕松獲取網絡名稱（SSID）和其MAC地址（BSSID）。因此，攻擊者可以冒充合法AP（LAP），並迫使設備連接到惡意存取點（例如，通過以更高的信號強度進行發射）。如果設備已經連接到LAP，攻擊者可以進行去認證攻擊，促使設備連接到惡意存取點。

雖然WiFi的安全機制（特別是第三代及之前）容易受到惡意孿生攻擊的影響，但也有一些有效的保護技術來檢測惡意存取點。一個例子是驗證WiFi客戶端（用戶設備）與不同AP的重複關聯，當合法和惡意AP同時連接到客戶端相同信道時會發生。此外，網絡的安全策略規則可能阻止設備與未經網絡相互身份驗證的AP通信。然而，我們注意到這些規定都是特定實現的，並且不能提供加密保證以防範不同類型的攻擊。

除了中間人攻擊（MitM）之外，惡意孿生還可以在WiFi存取安全性上發動更簡單而有效的攻擊，被稱為服務阻塞。在這種攻擊中，攻擊者不與WiFi設備關聯，而是干擾WPA2的認證過程，從而導致對LAP的任何連接被阻止。

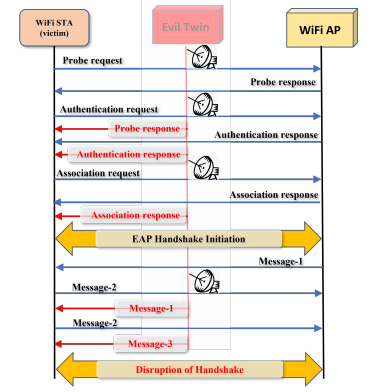


圖4: 在WPA2保護的WiFi中，使用惡意孿生協助的服務阻塞攻擊對EAP-based認證握手的影響。

圖4中的流程展示了對WiFi的WPA2認證協議進行服務阻塞攻擊。WiFi STA（設備）向LAP發送探測和身份驗證請求以初始化連接。LAP在每次請求後都會回應相應的響應。如圖所示，在客戶端發送身份驗證請求後，LAP和惡意孿生都向客戶端發送探測響應。同樣，身份驗證/關聯響應消息也在適當的時間點由LAP和惡意孿生發送到客戶端，如圖4所示。惡意孿生的響應以從圖的中部到WiFi STA的紅色水平線顯示。在從STA接收身份驗證響應後，它啟動4路EAP握手協議。無論客戶端首先從LAP還是惡意孿生那裡接收到EAP握手協議的消息1，它都會回應消息2。然而，在從另一個AP（惡意孿生或合法AP）接收到消息1後，握手協議失敗，與LAP的連接中斷。

2.3.2. 金鑰重新安裝攻擊

在WPA安全系統的相互驗證中，使用預先共享的對等主金鑰（PMK）生成稱為對等瞬態金鑰（PTK）的會話金鑰，該金鑰使用在AP端的隨機數SNonce和在客戶端的ANonce。金鑰重新安裝攻擊通過重播EAP握手協議中的消息3來實施，這導致重置隨機數和重播計數器 [50]。結果，先前正在使用的PTK將被安裝用於後續通信。

然而，要成功進行攻擊，攻擊者需要處於中間人(MitM)位置，在重新傳送消息-3之前，阻止消息-4到達AP。根據使用的安全協議，金鑰重新安裝允許進行進一步的重放攻擊、解密和偽造消息。

儘管有關檢測和防止消息-3的重播的實現特定條款，但許多硬件平台仍然容易受到金鑰重新安裝攻擊的威脅。例如，大多數安全實現可能僅接受消息-3的重新傳輸的加密版本。其中一些例子包括OpenBSD、OS X和macOS，這些系統要求對消息-3進行加密。然而，在實施握手協議的組件（例如，CPU）和數據機密性協議（例如，網絡接口控制器）之間存在競爭條件，這種情況仍然可能在金鑰刷新操作期間被利用。

圖5展示了金鑰刷新期間金鑰重新安裝攻擊的流程，其中消息-3也被加密。金鑰刷新交換的過程與4路EAP握手相似，不同之處在於消息現在使用當前金鑰進行加密。如圖所示，在階段1期間，在圖表的階段1中建立了初始金鑰。在階段2（需要刷新金鑰時），開始了具有加密消息的EAP握手。攻擊的目標是握手的（加密的）消息-3。攻擊者需要形成中間人(MitM)位置。在這種情況下，當消息-3（使用當前PTK進行加密）從AP傳送到客戶端時，攻擊者阻止了消息。因此，AP重新傳送消息-3。在這一點上，攻擊者一次性將兩個消息發送到客戶端設備。無線網絡訪問控制器（NIC）解密消息（使用當前PTK），並將其發送到CPU。在接收到第一條消息後，CPU刷新PTK。同樣，CPU接收第二條消息（使用舊PTK進行加密），並再次安裝PTK。這導致與PTK關聯的隨機數值重新從1開始。

即使在要求在重新鑰匙期間對消息-3進行加密的安全實現中，上述金鑰重新安裝攻擊也是由於系統中不同安全模塊之間的競爭條件而導致的。具體而言，現代NIC支持用於數據機密性的高級加密協議。然而，不同安全組件之間的區分使得即使存在諸如強制加密消息的條款，仍然可能出現新的安全漏洞。

2.3.3 Dos攻擊

為應對金鑰重新安裝攻擊，WiFi聯盟引入了WPA3，其中包括基於SAE框架的Dragonfly握手協議變體，用於WiFi安全系統[51]。此外，它定義了一種過渡模式，該模式支持WPA3和WPA2，以實現向後兼容。儘管基於SAE的WiFi握手協議承諾提供更好的安全性，但它會產生大量的計算開銷，從而導致DoS攻擊。因此，在商業現成產品（COTS）上實現WPA3安全性具有挑戰性。

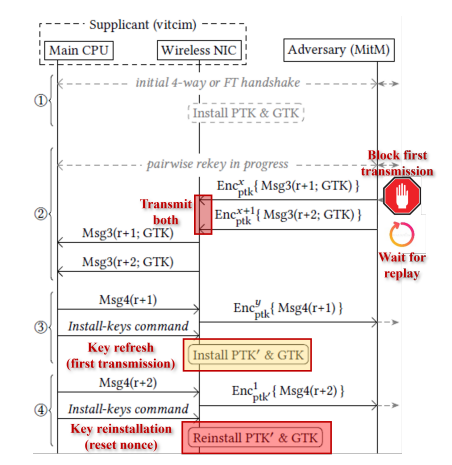


圖5：對WPA2保護的WiFi中基於EAP的身份驗證握手的金鑰重新安裝攻擊，帶有中間人攻擊(MitM)。

WPA3的Dragonfly握手支援橢圓曲線加密（ECC）和有限域加密（FFC）兩種方式，用於從預共享金鑰/密碼進行金鑰衍生和相互身份驗證。Dragonfly協議使用嘗試並增量循環機制，將密碼的哈希轉換為橢圓曲線（或乘法群）上的有效點。為了防止定時攻擊，這個過程需要大量的操作（比替代方法的數量級要大）。因此，Dragonfly還採用了一種防塞機制，以防止攻擊者利用大量開銷進行DoS攻擊。然而，防塞機制並不能保證免受DoS攻擊的保護。在一個實驗中，使用一個擁有700MHz CPU的Raspberry Pi B+作為攻擊者站，攻擊一個具有1200MHz CPU的專業AP。實驗結果顯示，攻擊者每秒僅偽造8次Dragonfly協議的提交交換，就能使AP的CPU使用率達到100%。

在過渡模式中，同時支援WPA3和WPA2，WPA3/WPA2的相應身份驗證協議使用相同的密碼。因此，通過部署降級攻擊（例如，伪造信標消息並強制WiFi站點使用WPA2），密碼可以通過攻擊WPA2安全協議來恢復。為了防止降級攻擊，過渡模式中的WPA2握手包含具有所有支持的協議套件列表的Robust Security Network Element（RSNE）。因此，客戶端設備可以檢測到來自對手的伪造信標消息。

上述的防御機制仍然容易受到降級攻擊的影響。攻擊者可以向客戶端發送包含合法AP（支援WPA3）的SSID的WPA2-only網絡的信標。由於握手的第一個消息未經身份驗證，客戶端將連接到攻擊者的AP並發送第二個已經身份驗證的消息。在這一點上，攻擊者可以使用第二個消息進行離線字典攻擊以恢復密碼。在這種攻擊中，對手甚至不需要處於中間人的位置。

另一種降級攻擊針對橢圓曲線或乘法群的集合。SAE框架定義了不同的群組，由用戶進行優先排序和配置。選擇群組的協商機制可以被攻擊者利用，以強制一個對特定攻擊更有利的群組。這種攻擊是在中間人的位置上部署的，攻擊者可以阻止某些協商交換，只允許那些對應到首選群組的消息。這尤其重要，因為不同的群組可能對侧信道攻擊（如定時攻擊和緩存攻擊）展現出不同類型的弱點。因此，攻擊者可以迫使用戶選擇最容易受到此類攻擊的群組。

3. 協同存在和非授權頻譜共享如何加劇安全挑戰

在協同存在的網絡環境中，頻譜共享為獨立網絡的安全系統增加了一個額外的攻擊表面。獨立網絡的第一層安全是身份驗證框架（第2層），它假設任何頻譜訪問都屬於同一網絡並且必須經過身份驗證。頻譜共享的主要挑戰來源於現有的安全框架不承認超出網絡範圍的訪問。然而，在協同存在的環境中，網絡實體（基站或設備）必須首先與其他網絡（很可能是具有獨立和私有安全機制的網絡）競爭頻譜。只有在獲得訪問權後，網絡的安全框架才能進行身份驗證和授權。在這種環境中，敵對方可以作為合法實體競爭頻譜，而獨立網絡中沒有能夠檢測到這樣的攻擊者的安全機制。這種漏洞在圖6中有概念性地描述。

現有的協同存在網絡的頻譜共享解決方案不包含任何安全機制，並且專注於網絡性能指標，特別是體驗質量（QoE）。它們更傾向於將安全保障推遲到通信協議堆疊較高層的訪問安全框架。這導致了如圖6（a）所示的即時漏洞；在這樣的環境中，攻擊者與合法網絡用戶的共存是不可避免的。攻擊者與合法網絡用戶的共存是頻譜共享系統中的一個新的攻擊表面，在獨立網絡中並不存在這種情況。這種觀點揭示了在頻譜共享中需要一個安全機制的必要性，因為僅在訪問頻譜之後，網絡內的安全機制才有關。為了強調安全頻譜共享的重要性，我們簡要回顧攻擊者利用未受保護的頻譜共享並部署新攻擊或實施現有已知攻擊的機會，這些攻擊具有更大的影響和更簡便的機制。

3.1 頻譜共享系統的安全性

由於5G和WiFi網絡的共存是一種新興趨勢，為了應對下一代無線網絡中的頻譜稀缺問題，有限的研究探討了共存對網絡安全性的影響。傳統的頻譜共享（SS）系統是一種與之密切相關的、更為傳統的網絡解決方案，用於提高頻譜使用效率，與具有許可頻譜帶的獨立網絡相對。

傳統SS系統和協同存在網絡環境之間的主要區別在於兩者的頻譜訪問分別是非對稱和對稱的。傳統SS系統由佔用者或主用戶（PU）組成，他們與次用戶（SU）共享頻譜。這被稱為雙層頻譜共享機制。頻譜訪問的優先權始終屬於PU。只有在沒有PU存在時，允許SU使用頻譜。儘管此方案允許在地理區域或時間槽中重複使用沒有PU用戶的頻譜，但它仍未提供兩個（或更多）網絡用戶之間的精細頻譜共享，這可能實現整體網絡容量的提高。

協同存在網絡方案為兩個或多個網絡的用戶提供對頻譜的細粒度訪問，無論是在頻率還是時間域上，都是公平的（並採用對稱機制），如下一節所述。由於兩個網絡對頻譜具有對稱訪問權，因此各自的用戶經歷的斷線次數較少，這反過來提高了整體網絡容量。在[8]中提供了對5G和WiFi共存環境中實現的網絡吞吐量的研究。然而，共存的安全性影響與傳統SS系統相似，因為這兩種方案共享相同的頻段。因此，預期類似的安全挑戰也轉移到了協同存在網絡方案中。在本節中，我們將回顧這些SS系統的已知安全挑戰。

對於雙層頻譜共享系統而言，一種眾所周知的攻擊是主用戶模擬（PUE）攻擊，其中對手模擬並傳送主用戶的信號。雖然這種攻擊可以被主用戶檢測到，使用主網絡的安全機制，但次用戶沒有機制來驗證PUE的訪問的合法性。因此，PUE攻擊者可以阻止次用戶訪問頻譜。這也被稱為動態頻譜訪問（DSA）DoS攻擊。PUE攻擊還可以被利用來發起更複雜的攻擊，如頻譜蜜罐[52]。在這種攻擊中，對手通過佔據其他頻道，強迫SU使用目標頻道。此攻擊可用於促進中間人攻擊，或僅僅是操縱SU在目標頻道中產生更多的干擾。

除了PUE之外，SU還可能對PU產生增加的（潛在的不需要的）干擾。如果SU無法感測到PU的信號，例如由於多徑衰落通道，它將訪問頻譜，進而對PU產生有害的干擾。一種解決方案是使用SU在訪問頻譜時的分布式感測和集中決策機制。在這種情況下，所有SU向集中的頻譜訪問系統（SAS）報告他們的頻譜感測結果，SAS授權SU進行傳輸（如果未檢測到PU信號）。然而，此機制容易受到頻譜感測數據篡改（SSDF）攻擊的影響，其中對手冒充SU並向SAS發送虛假數據[53]。有關基於感測和數據庫共享機制的雙層SS系統的不同攻擊的全面回顧可在[54]中找到。

頻譜共享的自然結果是可能的竊聽攻擊（主動或被動）。為了防止在共享頻譜中的干擾，網絡的信號必須可被外部用戶檢測到。通過這種方式，外部用戶也可以分析網絡的活動和流量，這違反了用戶的隱私。有關隱私利用的研究，以位置信息泄漏為例，可參見[55]。該研究提出了一種博弈論解決方案，以保護PU和SU的位置信息免受彼此的影響。除了位置信息外，對手還可以攔截合法用戶的信號，以提取私人和/或敏感信息。在MIMO系統中，一種解決方案是使用波束成形建立具有高保密性容量的數據通道，如第2.1.2節所述。在這些系統中還使用了智能（友好的）干擾信號，以增加保密容量。一個例子是在合法通信對之間的通道的空間中傳輸的人工噪聲[56, 57]。然而，這些技術需要對信道狀態信息（CSI）進行估算，這可能是主動竊聽攻擊的目標。

對於頻譜共享的安全性的大多數現有研究都研究了多層系統（非對稱頻譜訪問）中的漏洞。儘管在協同存在環境中也存在類似的漏洞，但在具有對稱頻譜訪問的共存網絡中存在特定的安全問題。在接下來的幾節中，我們將回顧共存環境中特定的潛在漏洞的一部分，同時也揭示了與多層系統相似之處。

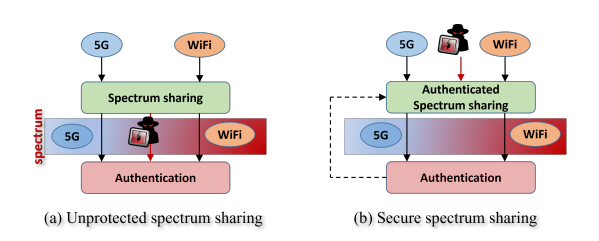


圖6：（a）未受保護和（b）安全的頻譜共享的比較，允許攻擊者訪問（劫持）頻譜。

3.2. 頻譜劫持

由於頻譜共享發生在獨立網絡啟動任何安全機制之前，攻擊者可以偽裝成一個共享頻譜的合法網絡實體，而不被識別為對手。這導致了一種稱為頻譜劫持的攻擊，在獨立網絡中並不存在類似的情況。這種共存漏洞嚴重降低了QoE，而共存網絡的主要承諾是提供高QoE保證。除了QoE降低，頻譜劫持攻擊可能對公共安全和任務關鍵通信構成嚴重威脅。在5G和WiFi 6/6E網絡中，無縫連接和低延遲的承諾是處理公共安全技術的基本要求，包括自動車輛、智能城市和基礎設施、應急應對者以及監視系統。這些應用程序中的許多也對延遲敏感，即及時交付內容對其運作至關重要。然而，最簡單的頻譜劫持攻擊可能會干擾網絡連接性，或者至少在提供所需服務的時候引入很大的延遲。頻譜劫持攻擊得益於獨立安全機制和獨立網絡的隱私需求。防止這種攻擊的一種解決方案是使用可信的第三方為不同的網絡（5G和WiFi 6/6E）提供訪問安全服務（即，身份驗證服務）。這樣，每個網絡都可以使用從可信方接收的訪問令牌驗證訪問的合法性。然而，這種方法需要在網絡的安全架構中進行實質性的更改，這似乎是不切實際的。此外，獨立網絡中的隱私需求，包括保護標識符和網絡流量，阻止了在網絡之間共享用戶信息。

3.3. 服務劣化

共存攻擊者可以利用未受保護的頻譜共享導致不同網絡之間的傳輸干擾，進而導致服務質量（QoS）降低（高延遲和低吞吐量）。為了理解這種攻擊，我們考慮5G和WiFi 6/6E共存中頻譜共享現有解決方案的基本思想，如圖7所示。每個無線設備首先使用一系列基於LBT的協議爭奪自由頻譜。WiFi 6系統支持單用戶（SU）和多用戶（MU）兩種模式。在SU模式中，每個WiFi站點（STA）都獨立競爭頻譜。WiFi 6/6E的MU模式非常類似於5G網絡的上行OFDMA。在此模式中，WiFi AP或5G gNB競爭頻譜。成功獲得空閒頻譜後，AP/gNB會在OFDMA單元中安排用戶。

在共存網絡中，頻譜共享機制的一個主要挑戰是隱藏節點問題。如果一個網絡的基站對另一個網絡是隱藏節點，那麼很可能兩個網絡會在相同的OFDMA單元中安排各自的用戶。因此，兩個網絡的傳輸會相互干擾。在獨立網絡中，通過使用媒體訪問控制（MAC）協議，可以檢測和/或避免隱藏節點。然而，在共存環境中，由於網絡的獨立MAC協議和它們之間缺乏信息共享，網絡之間的隱藏節點是不可避免的。這可能在共存環境中引起安全問題。

在共存網絡中，隱藏節點問題可以被攻擊者利用以嚴重降低QoS。一種簡單的攻擊利用潛在的隱藏節點存在可以導致服務劣化，即使基站實際上不在隱藏節點位置。假設基站競爭頻譜，AP/gNB成功獲取某些通道（例如，OFDMA單元）。攻擊者可以偽造gNB/AP的控制通道封包，並在AP/gNB已經獲取的相同通道中安排網絡的相應用戶。結果，兩個網絡的用戶將在相同的OFDMA單元中傳輸。儘管已安排的用戶仍然使用LBT協議進行傳輸，但這種情況可能會顯著降低QoS。首先，用戶必須等待通道釋放，這會增加網絡延遲。其次，在傳播延遲較長的更寬區域中，來自不同網絡的封包碰撞的可能性非常大。第三，來自不同網絡的無線設備可能處於隱藏節點位置，這將導致來自不同網絡的封包碰撞。

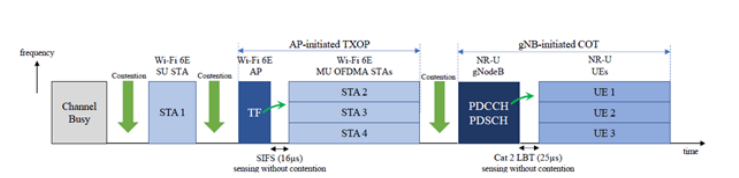


圖7：基於先聽後發（LBT）協議的5G和WiFi 6/6E共存的頻譜訪問[8]。

3.4. 類中間人攻擊

大多數現有的對無線網絡訪問安全性的攻擊，如前幾節所討論的，要麼是由中間人攻擊者啟用或促使的。一個突出的例子是針對WiFi的WPA2和WPA3安全性的密鑰重裝和降級攻擊。在這些攻擊中，對手需要有選擇性地阻塞、傳輸或重播身份驗證握手協議中的消息的中間人攻擊者。從WPA3降級到WPA2的攻擊可能不需要中間人的位置，但在這樣的攻擊者手中，檢測的機會更低。同樣地，使用邪惡的雙胞胎對WiFi進行服務阻塞攻擊在中間人攻擊位置上可能更加有效。我們討論了邪惡雙胞胎的存在導致WiFi設備的重復聯接，這可能會引起惡意AP的存在。然而，在中間人攻擊位置上的邪惡雙胞胎更難檢測。

中間人攻擊者還可能對5G網絡的訪問安全性構成嚴重威脅。例如，中繼消息來傳輸大量的重新驗證請求，以及對UE或核心網絡發起DoS攻擊。雖然在這種情況下中間人攻擊不是必需的，但它可以通過分析基站的頻譜活動降低檢測攻擊者的機會。儘管5G網絡中進行了幾次安全增強，但惡意基站或等效的中間人攻擊者仍然被視為對網絡的嚴重威脅。

攻擊者可以利用共存環境來形成一個類似中間人的位置（偽中間人），具有相似的攻擊能力。通過利用隱藏節點問題，攻擊者可以在上行傳輸期間為基站生成干擾，同時還可以接收用戶的消息。一個類似的攻擊可以針對選定的用戶設備在下行傳輸中進行。然後，攻擊者可以有選擇性地向基站/設備重播消息。這與經典的中間人攻擊稍有不同，其中攻擊者攔截用戶和基站之間的整個通信。

攻擊者還可以採用上述討論的類似機制，促使惡意基站的部署。攻擊者通過在基站處生成干擾來阻塞通信通道，同時與用戶進行通信。在這段時間內，攻擊者可以說服用戶連接到惡意基站。在這些情景中，基站無法區分共享頻譜的合法網絡的干擾，還是攻擊者的惡意干擾。

3.4.1. 物理層安全

現有的安全規範並不包括標準化的物理層安全協議。然而，目前正在進行的研究和對利用射頻特徵定義身份驗證協議的興趣，作為物理層安全的一種條款。在5G和WiFi 6的新無線電（NR）物理層中，這些技術的著名例子包括射頻指紋識別和波束成形，用於設備的唯一識別。儘管這些解決方案看似有前景，但仍然存在需要解決的挑戰，包括在設備、時間和射頻傳播通道上的不確定性和變異性。

物理層安全機制仍然主要針對獨立網絡，而共存環境會對它們的效力提出挑戰。例如，這些技術可以為網絡內的設備提供額外的識別信息，用於身份驗證。然而，在共存環境中，來自網絡域外的未知設備仍然必須被視為合法的。與其他攻擊一樣，這可能會降低此類安全機制的效力。

具有諷刺意味的是，被提出作為安全條款的物理層機制也可以幫助攻擊者部署更有效的攻擊。在利用共存環境和NR特徵的結合攻擊中，保護免受此類攻擊變得更加具有挑戰性。在圖8中所示的示例中，攻擊者可以有效地使用波束成形模擬對合法基站的隱藏節點干擾，而不影響用戶通信。與此同時，攻擊者還可以通過在適當的方向形成另一個波束竊聽來自受害設備的通信。在此過程中，基站無法接收來自用戶的消息，因為它正在經歷干擾。由於共存條件，它也無法將干擾區分為惡意或合法。此外，用戶對攻擊者的存在一無所知。

為了進一步複雜化上述攻擊，攻擊者可以利用射頻指紋識別來唯一識別其目標用戶設備。因此，攻擊者甚至無需設備識別符（例如5G-GUTIs）即可跟踪受害者的活動並竊聽其通信。此示例演示了在共存環境中利用NR特徵（如波束成形和OFDM調製）可能會危害個別網絡安全的重要性。因此，對於頻譜共享的安全機制的重要性是不可否認的。

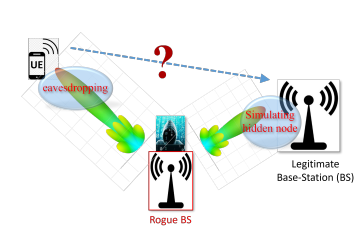


圖8: 利用波束成形和共存網絡環境部署有效的中間人位置。

4. 緩解計劃和未來研究方向

在下一代無線網絡的高度動態環境中應對安全挑戰，並在QoE約束下進行多方優化是一個多面向的問題。在這個問題中經常遇到的三難困境如圖9所示。在區塊鏈安全的上下文中（通過將可訪問性替換為去中心化），也討論了類似的三難困境 [58, 59]。

無縫連接（可訪問性）通過多種RAT技術是5G/6G網絡的主要承諾。可擴展性是無線網絡的不可避免的特性，因為它們預計將在物聯網時代支持大量移動設備。在維護隱私的同時提供安全性，預期將對網絡和設備產生最小的通信和計算開銷。改進這三個屬性中的任何兩個可能需要在第三個屬性上進行妥協，特別是在當前靜態安全框架的背景下。

現有的安全問題的解決方案通常在圖9的三難困境中的一個屬性上進行妥協。它們可能需要更多的消息交換，或者更複雜的加密算法，以實現身份驗證和識別的集中安全性，這會增加延遲並降低可訪問性。解決方案的一部分需要預共享的密鑰，這對預計將在網絡中運行的數十億設備來說是一個挑戰（可擴展性挑戰）。基於零信任架構（ZTA）的下一代網絡安全模型，正如 [60] 中所討論的，可能提供達到這個三難困境中的最佳點（甜點）的機制。

現有安全解決方案的更為關鍵的問題是對所有網絡資源擁有權的假設，以及對共存特性的忽視，特別是在媒體訪問控制（MAC）方面。後者是一個嚴重的問題，因為任何解決方案都應該容忍來自共存網絡的未知訪問。此外，由於嚴格的隱私約束，網絡運營商之間無法共享網絡和相應的機密信息和使用要求的身份。因此，在實踐中，基於合作式媒體訪問的解決方案具有挑戰性。因此，一個安全的共存框架應該處理未知的訪問，同時保護個別網絡用戶的安全性。在接下來的部分，我們首先回顧了解決前幾節中獨立網絡的安全問題的一些現有建議。接下來，我們將討論在共存環境中解決安全挑戰的可接受解決方案的要求。

4.1. 物理層安全解決方案

如第2.1節所討論的，加密的物理層可以通過加密證據保護模擬信號免受截取，提供安全性。然而，這樣的解決方案在密鑰協定和分發方面遇到可擴展性問題，因為預計無線網絡將支持大量不斷增長的設備。密鑰交換協定，如Diffie-Hellman（D-H），可以幫助生成密鑰，然而，對於公鑰基礎結構和相關的證書機構仍然是一個問題。考慮到下一代網絡中存在大量的私有5G納米基站和WiFi接入點，情況變得更加惡化。此外，DH協定及相關的公鑰密碼學對資源受限設備產生大量通信和計算開銷。

通信通道的保密容量，尤其是在5G網絡的NR物理層中使用波束成形，可以被利用來實現密鑰協定。這種方法已經在[61]中用於具有基站天線陣列的時分雙工系統，並且在存在信號污染的情況下。基站向合法用戶發送隨機序列，而竊聽者試圖偽造用戶的訓練信號以引起波束方向的偏移。然後，基站使用竊聽者的傳輸來估算信息洩漏並相應地調整密鑰的長度。[61]中使用了類似的方法，進行了雙向訓練（上行和下行），展示了估算竊聽者通道的改進，因此密鑰協定的效率提高。檢測主動竊聽者通道的隨機發射也已經在其他作品中使用，例如[62, 63]。

引入人工噪聲（AN）和匹配濾波預編碼，對於多輸入多輸出（MIMO）系統來說，是對抗信號污染的一種常見防禦方法[64, 39]。此外，[39]中引入的空零子空間技術有助於通過使用用戶天線的相關多樣性來緩解竊聽者的利用。在某些正交性條件下，研究表明該技術可以防止竊聽者降低秘密傳輸速率。這些技術通常需要對信道狀態信息（CSI）的精確了解。[65]中採用了一種半盲技術，用於估算合法用戶的信號，不需要CSI。該信道是使用數據信號來估算的。[66]中使用了類似的數據輔助技術，在大規模MIMO系統的訓練階段估算上行信道。

物理層身份驗證（PLA）通過將模擬通信通道和/或設備的獨特特徵納入身份驗證協定，以巩固訪問安全性。[67]提供了基於CSI、頻率和身份水印的各種PLA技術的調查。在[68]中，採用了預先共享的秘密密鑰和CSI的組合，用於實現挑戰-響應協議。指紋嵌入也是PLA的一種常見技術[69]。在[70]中研究了在具有對CSI的不完美了解的情況下使用AN來隱藏基於哈希的消息驗證碼（HMAC）。在[71]中，研究了使用到達角（AoA）實現PLA技術的方法。同樣，已經在[72]中研究了使用合法用戶的AoA信息估算竊聽者通道的基站性能的理論界限。

為了在第2層身份驗證機制中提供完美的前向保密性，[73]提出將D-H密鑰交換協議整合到5G-AKA中。該方案還保護來自對長期秘密密鑰了解的被動竊聽者的會話密鑰。這種技術防止了在被動竊聽攻擊中揭示5G-AKA協議中的挑戰nonce，因此是會話密鑰的攻擊。會話密鑰是從長期秘密密鑰和挑戰nonce生成的。在身份驗證開始時進行密鑰協商交換是一種類似的方法，正如WiFi Protected Access（WPA3）機制所使用的那樣，其使用的是Dragonfly握手而不是D-H [51]。

[74]中還提出使用D-H密鑰交換來防止身份泄露和重放攻擊。在D-H握手中生成的會話密鑰用於加密標識符，從而保證身份的機密性。此外，與5G核心網絡的消息交換附帶有消息身份驗證碼（MAC），可以防止偽造消息，並防止重放攻擊。對消息SYNC\_FAIL和MAC\_FAIL的加密還可以防止可追踪性攻擊，這在第2.2.3節中討論過。

解決公鑰機制挑戰的文獻中的一種常見解決方案，特別是在建立信任方面，是使用區塊鏈，正如[75]中所提出的那樣。將區塊鏈技術與公鑰基礎設施（PKI）憑證相結合已成為實現輕量且可信的訪問安全平台的熱門解決方案，特別是在設備對設備和車輛通信中[76]。在[77]中，引入了一種用於記錄VANET中用戶訪問特權相關憑證的區塊鏈結構，同時保證了用戶身份的隱私。在[78]中，也基於以太坊區塊鏈開發了一種類似的方法。

跨層身份驗證技術也引起了關注，作為保護身份和位置機密性、防止消息偽造、竊聽和惡意基站的手段。這些技術將物理層身份驗證（PLA，如前面所討論的）與第2層身份驗證機制結合在一起。[79]提供了使用PLA的跨層身份驗證機制的綜述。在這些技術的大多數中，物理層特性被用作第2層身份驗證機制中的指紋參數，用於初始識別和隨機生成 [80]。這種方法在[81]中使用CSI，在[82]中使用接收信號強度（RSS）作為指紋特徵。

為應對5G網絡的動態特性，[83]引入了PLA和上層身份驗證機制之間的耦合跨層機制。該工作使用具有物理層多個指紋特徵的PLA，以提高可靠性和穩定性。此外，上層身份驗證機制還用於更新PLA的模型參數，以適應低計算複雜性的環境。這與在[84]中使用PLA的解耦方法形成對比，該方法在成功進行第2層身份驗證之後進行。

4.3物理層安全

現有的安全規範並未包括物理層安全的標準化協議。然而，目前有一些正在進行的研究和對利用射頻特徵的身份驗證協議的興趣，作為物理層安全的一種提供。5G 和 WiFi 6 中的新無線電（NR）物理層的突出示例是 RF 指紋識別和波束成形，用於設備的獨特識別。儘管這些解決方案看似有前景，但仍然存在一些需要解決的挑戰，包括設備、時間和射頻傳播通道的不確定性和變異性。

這些物理層安全機制仍然針對獨立網絡，而在共存環境中，它們的有效性受到挑戰。例如，這些技術可以為在網絡內進行身份驗證的設備提供額外的識別信息。然而，在共存環境中，來自網絡域外的未知設備仍然必須被視為合法的。與其他攻擊一樣，這可能降低這些安全機制的有效性。

具有諷刺意味的是，作為安全保護的物理層機制也可以幫助攻擊者部署更有效的攻擊。在利用共存環境和 NR 特徵的組合攻擊中，對抗此類攻擊變得更加困難。在示例中，攻擊者可以有效地使用波束成形來模擬對合法基站的隱藏節點干擾，而不影響用戶通信。同時，攻擊者還可以通過在適當方向上形成另一個波束來竊聽來自受害設備的通信。在此過程中，由於正在遇到干擾，基站無法接收來自用戶的消息。由於共存條件的存在，它也無法將干擾區分為惡意或合法。此外，用戶對攻擊者的存在一無所知。這個例子演示了 NR 特徵在共存環境中如何危害個別網絡的安全。因此，確保安全的頻譜共享機制的重要性是不可否認的。

區塊鏈和數據庫頻譜共享的一個主要局限性在於對數據庫的網絡訪問要求。這在需要訪問頻譜以進行網絡連接的點對點無線網絡中是具有挑戰性的。然而，在具有集中控制的無線網絡中，如 5G 和 WiFi，基站可能會授權對頻譜的訪問並為移動設備安排通道。即使在這些網絡中，對於相對於基站處於隱藏節點狀態的敵對方，仍然可以對移動設備造成干擾。攻擊者可以模擬隱藏節點，例如通過針對設備的波束成形。這些脆弱性的一部分在第 3.2 至 3.4 节中進行了討論。

在共存網絡環境中，更高程度的干擾也是預期的特徵。這種情況促使了與非正交多址接入（NOMA）系統 [87, 88] 相似的安全挑戰。攻擊者可以利用這種環境來增加干擾程度，而不被識別為惡意。這可能導致通道編碼中的保密容量明顯降低。此外，這樣的隱蔽攻擊者可能危及利用保密容量和利用 CSI 和 RF 通道指紋技術的 PLA 技術進行的密鑰交換協議的安全性，如前一節所討論的。處理惡意干擾並區分攻擊者和合法用戶是一個具有重要影響的共存安全的未解決問題。

在共存環境中，波束成形物理層和大規模 MIMO 系統的安全性也可能受到顯著挑戰。正如在第 2.1.2 节中所討論的，污染攻擊可能導致天線陣列的波束偏離預期方向。共存環境為攻擊者提供了在部署污染攻擊方面前所未有的機會。基於檢測和估計竊聽器通道的現有防禦機制依賴於一個假設，即除竊聽器之外的所有傳輸都是合法的並遵循已知的協議。然而，在共存環境中，來自共存網絡的合法用戶的干擾可能導致相同或甚至更強的干擾，與竊聽器相當。

結論

共存網絡環境引入了獨特的安全挑戰，這些挑戰在網內安全框架和協議中尚未得到解決。在共存環境中，獨立的網絡機制不能再假設所有訪問都應由網內機制進行身份驗證和授權，這是一個不再成立的前提。這種網絡環境的獨特特徵為攻擊者提供了前所未有的利用方式，可以大幅降低網絡容量並促使惡意基站的部署。

我們回顧了可能導致與共存網絡相關的嚴重安全漏洞的主要攻擊。共存的一個主要挑戰是各個網絡中獨立的介質訪問控制（MAC），這導致了隱藏節點的出現。攻擊者可以利用這種狀況來訪問頻譜，無論是簡單地占用大部分頻譜還是增加干擾程度，而不易與合法用戶區分。這種簡單攻擊者的第一效應是網絡容量大幅下降。此外，在這種環境中更容易實施惡意基站的部署、中間人攻擊和重放消息。這項研究顯示了有必要重新檢討現有的安全解決方案，並將共存環境的特定特徵納入考慮，以應對下一代網絡的挑戰。