5G 安全自動化攻防框架

工研院能源與環境研究所前研究員 / 呂錫民

關鍵字：5G、安全、自動化攻防、框架

摘要

5G網路目前正在迅速發展，並致力於通過新技術、組件和服務，以連接互聯網的所有事物。由於5G的關鍵作用以及新的體系結構和設計，5G面臨著大量的安全威脅，並需要合適的安全技術。本文提出了針對5G安全的自動化攻防框架，旨在為5G安全研究提供探索性指導。我們首先從分層結構的角度回顧攻擊/防禦物件的安全挑戰，然後提出一種既支持單層安全又支持跨層安全的分層安全模型。根據分層模型，針對5G的已知和未知安全威脅，提出一種基於安全知識圖的自動化攻防框架，並為5G安全自動化建議可能的方向。

一、前言

由於移動設備的普及和移動無線通信技術的發展，出現了諸如移動互聯網和物聯網（IoT）之類的大量新的移動應用科技[1]。根據思科VNI報告，2017年全球移動設備數量為86億，到2022年將達到123億。到2022年，每月移動流量將達到77.5艾位元組(exabytes)[1] [2]。將來，移動無線通信將成為主流通信技術之一，並提供具有不同需求的各種服務，例如大型物聯網設備、高速移動設備和高流量應用。截至目前為止，儘管現有的移動無線網路可以滿足設備使用和流量需求，但可能難以滿足未來的服務需求。因此，將出現下一代移動無線網路，即5G網路。

5G 的主要服務可以分為三類 [3]：

- 具有高帶寬要求的增強型移動寬帶（eMBB），例如虛擬實境（VR）和擴增實境（AR）。
- 具有可靠性和延遲要求的超可靠低延遲通信（uRLLC），例如車聯網（IoV）、遠程控制和觸覺互聯網。

[1] 艾位元組（exabyte）= 2^{60} bytes。

- 大規模的機器類型通信（mMTC），具有大量多樣的設備使用要求，例如 IoT。

為了支持多樣化的新應用和服務，5G可以採用多種技術，從而可以實現「萬物互聯」的目標。5G中使用的技術根據不同層的需求進行劃分。實體層可以提供高級通信功能，例如低延遲、高數據帶寬、高覆蓋率和大規模連接。為了獲得這些功能，可以採用多種技術，例如多重全雙工通信、超密集網路、大規模多輸入多輸出和毫米波。邏輯層旨在通過網路虛擬化和網路切片來支持多樣化、高效和低成本的服務。因此，可以採用諸如網路功能虛擬化（NFV）、軟體定義的網路（SDN），新的轉發和路由模型[4]以及基於雲的網路等技術。

5G的安全性源於新技術和新場景的使用，引起了人們的廣泛關注。5G安全機制應在5G開始之初就考慮在內，並應集成到5G體系結構中。通過修補解決5G安全問題是不可行的，這可能會導致5G架構膨脹。集成的5G安全設計帶來兩個主要優點。首先，可以很大程度上避免修補解決方案。安全解決方案幾乎不會影響5G架構。其次，5G的抗攻擊能力將得到增強，對5G的攻擊將大大減弱和減少。

儘管已經廣泛研究了5G的關鍵安全問題，但仍然存在以下挑戰：

- 缺乏有關跨層安全性的考慮。由於 5G 應用受每一層技術的支持，因此攻擊可能會跨越多層而不是單層。
- 對未知的安全威脅缺乏考慮。發現零日 (0-day) 漏洞[2] 和發現未知攻擊（有助於處理潛在攻擊）在 5G 安全中起著重要作用。
- 缺乏有關安全自動化的考慮。手動安全方法不適用於各種複雜的 5G 場景。安全自動化被視為 5G 安全願景的原則之一 [5]。

為了解決上述挑戰，本文專門從自動化攻擊和防禦角度探討有關5G的安全框架。由於5G尚未廣泛部署，因此建議的框架是針對5G安全的探索性解決方案。本文的主要貢獻如下。

- 我們總結 5G 的分層框架，並審查每層的安全挑戰和解決方案。
- 研究跨層安全性，而不是專注於單層安全性。根據 5G 的層次結構，提出層次化的攻防模型。正式描述單層和跨層的安全威脅和解決方案。
- 根據設計模型，提出一種基於安全知識圖的自動化安全框架，以期為 5G 提供自動化攻擊和防禦功能。

本文其餘章節安排如下。首先調查國際組織與企業無線通訊安全框架，其次是國際自動化攻防技術調查，接著討論5G安全挑戰，然後設計了一款分層安全模型。其次，提出並討論一種基於安全知識圖的自動化安全框架，以及進行各類安全框架比較。在最

[2] 在電腦領域中，零日漏洞或零時差漏洞（zero-day vulnerability、0-day vulnerability）通常是指還沒有修補程式的安全漏洞，而零日攻擊或零時差攻擊（zero-day exploit、zero-day attack）則是指利用這種漏洞進行的攻擊。提供該漏洞細節或者利用程式的人通常是該漏洞的發現者。零日漏洞的利用程式對網路安全具有巨大威脅，因此零日漏洞不但是駭客的最愛，掌握多少零日漏洞也成為評價駭客技術水平的一個重要參數。

後一章中，我們總結了這篇文章。

二、國際組織與企業無線通訊安全框架

從全球蜂巢式網路（如GSM或2G）的出現開始，標準化就發揮了至關重要的作用。在此過程中，運營商和供應商就全球網路如何協同運作以及如何保護網路和用戶免受惡意攻擊者達成一致協議。網路供應商將商定的標準轉換為功能性的網路元件和系統。網路供應商執行的設計和開發是使最終網路產品成為高效且安全的關鍵元件。

在部署階段，網路還針對目標安全級別進行設計和配置，包括設置安全參數，並進一步增強網路的彈性。在操作階段，提升網路運作並提供目標安全級別的操作程序，高度依賴於網路的部署和操作SOP。

在實施和部署階段，規範中還包含有關虛擬化和雲部署的更多資訊。這些細節將於下文揭曉。

（一）3GPP

5G 3GPP標準是不可不知的，因為它足夠靈活，以允許無線接入網路（RAN）和核心網絡之間發生不同類型的實體和虛擬重疊，例如從遠端設備到核心網路。RAN和核心之間的功能分離引發有關競爭力和性能的問題。

3GPP標準化第四章專注於3GPP範圍內的安全機制，即功能元件和界面。下面框架則涵蓋與5G系統部署方案有關的其他安全注意事項，包括：

- 系統範圍的安全性（水平安全性）
  - 網路級
  - 切片
  - 應用程序級別的安全性
  - 機密性和完整性保護
  - 互連（例如，共享批次區（SBA））
- 5G 功能元件部署（垂直安全性）
  - 網路功能虛擬化（NFV）
  - 分佈式雲

3GPP的5G系統標準提供了安全機制，該機制係以4G安全機制為基礎，但也包括針對以下的新增功能：加密、身份驗證和用戶隱私。

儘管3GPP安全機制為非惡意不良無線電條件提供可靠鏈接，但它們不能防範所有可能威脅，例如DDoS[3]和無線電干擾。防範DDoS攻擊和無線電干擾是實施和部署階段工作，例如 如果發生網路擁塞，則通過其他基地台重新路由流量；如果是DDoS，則採用縮放機制[4]和選擇性丟棄/限制作法。

3GPP TS 33.501 V15.1.0（2018-06）是SA3為5G安全性發布的最新規範。它定義

[3] DDoS（Distributed Denial of Service）中文翻譯為分散式阻斷服務攻擊，為 DoS（Denial of Service）（譯：阻斷服務攻擊）的延伸，通常會伴隨 Botnet（殭屍網路）進行。大量的殭屍電腦接收攻擊者控制命令，同時間對同一目標發動特定類型攻擊，將被攻擊者網路資源及系統資源耗盡，導致無法提供真正的使用者服務，伺服器看似異常停擺，因此稱作阻斷服務攻擊。由大量殭屍電腦造成的阻斷服務攻擊則稱做分散式阻斷服務攻擊。

[4] 自動縮放機制 (Scaling Mechanism) 是 DDoS 的重要防線。使用自動縮放功能，可以在線方式添加和刪除機器，以響應不斷變化的負載。

了安全架構：5G系統和5G核心的安全功能和安全機制；以及在5G系統（包括5G核心和5G新無線電（NR））中執行的安全程序。3GPP強調，原本計畫凍結的Release 16 ASN.1和Open API規格將持續在2020年6月進行。但是由於COVID-19疫情，後續版本Release 17 ASN-1和Open API的發佈時間預計將延遲到2021年12月。

（二）Ericsson

在Ericsson，電信網絡安全框架係由以下層次定義：

- 標準化；運營商、供應商和其他利益相關者通過此過程為全球網絡如何協同工作設定標準。這也包括如何最好地保護網路和用戶，以免受惡意行為者的攻擊。
- 網路設計；網路供應商設計、開發和實施商定的功能性網路元件和系統標準，這些標準在使最終網路產品在功能和安全方面起著至關重要的作用。
- 網路框架；在部署階段，網路配置成目標性安全級別，這對於設置安全參數並進一步增強網路的安全性和彈性至關重要。
- 網路部署和運營；允許網路運行並提供有針對性的安全級別的操作程序，係高度依賴於網路本身的部署和操作 SOP。

（三）Huawei

營運商的5G安全建議：除3GPP安全標準支撐外，運營商需要為網路設備及網路管理制定統一的端到端安全框架。在整個安全框架中，不僅要包括基地台、回傳網和核心網等網元，還必須考慮其他網元，如互聯閘道、防火牆和IT服務器（如DHCP[5]、DNS[6]/RADIUS[7]、伺服器[8]等），保證網路內部及網路邊界的安全。基於端到端的管理邏輯，5G網路安全需滿足以下幾個方面的要求：

- 網路安全框架
- 網路運營與運維
- 與外網（如互聯網）及內網相連的邊界安全防護。

監管機構的5G安全建議：制定法律法規，與所有公私合作夥伴進行討論，以確保安全框架的一致性。

其中網路安全框架可分為應用層（Application Stratum）、歸屬層（Home Stratum）、服務層（Serving Stratum）與傳輸層（Transport Stratum），這四層間是安全隔離的：

---

[5] 動態主機配置協定（Dynamic Host Configuration Protocol, DHCP），是一個用於 IP 網路的網路協定，位於 OSI 模型的應用層，使用 UDP 協定工作，主要有兩個用途：用於內部網路或網路服務供應商自動分配 IP 位址給用戶，以及用於內部網路管理員對所有電腦作中央管理。

[6] 網域名稱服務（Domain Name Service, DNS）主要目地是在解決機器的網域名稱（Domain name）與 IP address 的對應問題。提供 telnet、browser、ftp 等常用工具的基本服務。

[7] 遠端用戶撥入驗證服務（RADIUS, Remote Authentication Dial In User Service）是一個 AAA 協定，通常用於網路存取、或流動 IP 服務，適用於局域網及漫遊服務。

[8] 伺服器（Server）指：一個管理資源並為用戶提供服務的電腦軟體，通常分為檔案伺服器（能使用戶在其它電腦存取檔案）、資料庫伺服器和應用程式伺服器；或者，執行以上軟體的電腦，或稱為網路主機（Host）。伺服器通常以網路作為媒介，既可以通過內部網路對內提供服務，也可以通過網際網路對外提供服務。伺服器的最大特點就是其強大的運算能力，使其能在短時間內完成大量工作，並為大量用戶提供服務。

- 傳輸層：最底層的傳輸層安全敏感度較低，包含終端部分功能、全部的基地台功能和部分的核心網功能如 UPF[9]，基地台和這部分的核心網功能不接觸用戶敏感性資料，如使用者永久標識、使用者的根金鑰等，僅僅管理金鑰架構中的低層金鑰，如用戶接入金鑰。低層金鑰可以根據歸屬與服務層的高層金鑰進行推導、替換和更新，而低層金鑰不能推倒出高層金鑰。
- 服務層：服務層安全敏感度略高，包括運營商的服務網路的部分核心網功能如 AMF（接入和移動性管理功能）、NRF（網路存儲功能）、SEPP（安全邊緣保護代理）、NEF（網元功能）等。這部分的核心網功能不接觸用戶的根金鑰，僅管理金鑰架構中的中層衍生金鑰，如 AMF 金鑰。中層衍生金鑰可以根據歸屬層的高層金鑰進行推導、替換和更新，而中層金鑰不能推導出高層金鑰。這一層的安全架構不涉及基地台。
- 歸屬層：歸屬層安全敏感度較高，包含終端的USIM卡[10]和運營商的歸屬網路的核心網AUSF（鑒定服務功能）、UDM[11] 功能，因此包含的資料有使用者敏感性資料如使用者永久標識，使用者的根金鑰和高層金鑰等。這一層的安全架構不涉及基地台和核心網的其他部分功能。
- 應用層：應用層與業務提供商強相關，但與運營商網路弱相關。和 4G 一樣，對安全性要求較高的業務，除了傳輸安全保障之外，應用層也要做端到端地安全保護；例如移動支付，即使 4G/5G 網路保障了傳輸的安全，應用層也要做端到端地安全保障，以確保資金轉移不會出現問題。

三、國際自動化攻防技術調查

許多調查性和知識性文章都對5G網路的安全性挑戰進行了回顧[6-8]。現有的5G安全性研究可以分為兩個方面：實體層安全性和邏輯層安全性。實體層安全性通過實體層的各種技術，提供加密、認證、加密密鑰分發和管理等功能[6]。邏輯層安全性集中在NFV和SDN的安全性上，例如安全性隔離、切片間通信的安全性、配置錯誤、虛擬化威脅、虛擬機監控程序劫持等[7]。

根據層功能，邏輯層可以繼續劃分為多個層，包括虛擬層、服務（切片）層和應用

[9] 用戶平面功能（UPF）是 3GPP 5G 核心基礎系統架構的基本組成部分。UPF 表示控制和用戶平面分離（CUPS）策略的數據平面演變，該策略首先由 3GPP 在其第 14 版規範中作為對現有演進分組核心（EPC）的擴展引入。CUPS 使分組網關（PGW）控制和用戶平面功能解耦，從而使數據轉發組件（PGW-U）可以分散化。這允許在更靠近網路邊緣的地方執行數據包處理和流量聚合，從而在減少網路壅塞的同時提高帶寬效率。CUPS 的主要目標是支持 5G 新無線電（NR）實施，以實現早期的 IoT 應用和更高的數據速率。致力於控制和用戶平面分離的完整實現是一個複雜的主張，它針對採用 5G 用戶平面功能提供優勢子集，例如網路切片。用戶平面功能部署在動態雲本地計算基礎架構中，為基於服務的體系結構（SBA）提供了數據包處理基礎。

[10] USIM 卡（UMTS Subscriber Identity Module），是用於 UMTS 網絡中的用戶身份識別模組。USIM 卡還可以儲存使用者資料、電話號碼、認證資料及為短訊提供儲存空間。USIM 卡通常被認為是 SIM 卡的升級。

[11] UDM（Unified Dimensional Model，統一維度模型）技術，以屬性（Attribute）為基礎，發展出由下而上的彈性維度架構，試圖提供更佳的存取效率和資料整合模式。

層。虛擬層採用虛擬化技術將不同的實體設備轉換為統一的虛擬資源，並將網絡功能從基於硬體的應用程序轉移到基於軟體的應用程序[8]。

對於無線信道，由無線電傳播的開放性[9]引起的竊聽攻擊和未經授權的訪問是兩個主要挑戰。加密和授權機制也可以用來解決這兩個挑戰。無線信道的固有安全屬性，包括唯一性、多樣性和互惠性，使第三方無法測量、重建和復制無線信道。基於這些屬性，可以通過使用竊聽編碼技術、安全的多天線技術、基於CSI[12]/RSS[13]/基於相位/代碼的密鑰生成技術、基於竊聽代碼的身份驗證、RF識別方法等，獲得增強的加密和身份驗證機制[10]。

在邏輯層上，對實體資源進行虛擬化和切片以支持服務。存在三個主要的安全挑戰。（1）共享資源引起的數據洩漏。儘管不同對象的資源在邏輯上是分開的，但它們可能屬於同一實體設備。資源的重新分配可能會將資源從一個用戶轉移到另一個用戶，並導致數據洩漏。同時，不良的隔離策略也可能導致數據洩漏或攻擊。VM/切片隔離、授權、數據擦除、加密和安全通信協議（TLS[14]、SSH[15]）等方法是很有前途的解決方案[9]。（2）軟體和協議的漏洞。

自動化漏洞挖掘技術（Automated Vulnerability Mining Technology）[16]可自動從軟體或協議中查找漏洞。模糊技術與符號執行技術相結合，例如AFL[17]，並且始終使用其改進方法[11]。

使用數據流併接技術來劫持程序控制流的資料面向利用[12]是一種很有前途的技術，但成功率和通用性問題應得到解決。

由於物件眾多使得5G網路環境十分複雜，因此基於以前的評估方法來改進5G網絡的風險評估是有其必要的。自動化漏洞修復技術為漏洞提供了自動化修復策略，例如，自動修補、基於搜索的程式修復、基於語義的程式修復[13]等等。

[12] 信道狀態信息（CSI）是 WiFi 協議的一部分，其提供關於 WiFi 信號狀態的一般信息。

[13] Really Simple Syndication（非常簡單的聚合），它是一種用來分發和匯集網頁內容（例如：新聞標題、網誌 title 等）的 XML 格式。RSS 的使用，供應網頁內容的人可以很容易地產生並傳播新聞鏈結、標題和摘要等資料。簡單的說，其實就有點像是以 Email 的接收訊息之方式接收資訊。

[14] 傳輸層安全性 (TLS) 是一套加密通訊協定，可用於保護網際網路通訊安全。如果您在瀏覽器的網址列中看到一個鎖定圖示，且 URL 開頭是 https://，代表該連線使用 TLS。

[15] Secure Shell（安全外殼協定，簡稱 SSH）是一種加密的網路傳輸協定，可在不安全的網路中為網路服務提供安全的傳輸環境。SSH 通過在網路中建立安全隧道來實現 SSH 客戶端與伺服器之間的連接。SSH 最常見的用途是遠端登入系統，人們通常利用 SSH 來傳輸命令行界面和遠端執行命令。SSH 使用頻率最高的場合是類 Unix 系統，但是 Windows 作業系統也能有限度地使用 SSH。

[16] 目前，漏洞挖掘技術主要包括手動測試、模糊測試、靜態分析、diff 和 bindiff 技術以及運行時分析技術。

[17] American Fuzzy Lop 是一種免費軟體模糊測試工具，它採用遺傳算法來有效地增加測試用例的代碼覆蓋率。到目前為止，它有助於檢測數十個主要的免費軟件項目中的重大軟體錯誤。

四、分層 5G 框架中的安全挑戰

目前有關5G安全的研究和概論文章[14]始終專注於特定安全問題的安全方法。與之前不同，此處5G安全框架被視為一個整體。我們首先總結5G架構的層次結構，然後根據層次結構回顧相應的安全挑戰和解決方案。

（一）5G 的層次結構

不少學者已經提出多種5G方案[15]，但沒有統一的架構。通過這些方案的架構分析，可以提取5G的分層結構。圖1顯示了層次結構。5G的架構從下至上分為四個層：實體層、虛擬層、服務層和應用層。後三層可以統稱為對應於實體層的邏輯層。

實體層提供統一的實體資源以及上層的相應通信技術。通過虛擬化實體資源，邏輯層可用於支持特定的5G應用。為了滿足5G場景的不同要求，通過結合SDN，網路切片以及相應的管理和編排，將虛擬化資源定制為各種服務（圖1的右側）。詳細過程如下。基於虛擬化技術，將統一的實體資源轉換為虛擬層上的虛擬資源，並且將傳統的硬體支持網路轉換為SDN[8]。通過管理和編排虛擬資源，可以獲得用於特定服務的網路切片（即，虛擬網路）。然後，網路切片為特定應用提供資源，例如，IoT服務可用於支持智慧工廠、智慧城市等。

五、安全挑戰與解決方案

易受攻擊且需要保護的目標稱為攻擊/防禦物件。在這裡，我們從每一層的攻擊/防禦物件而不是特定技術的角度來回顧5G的安全

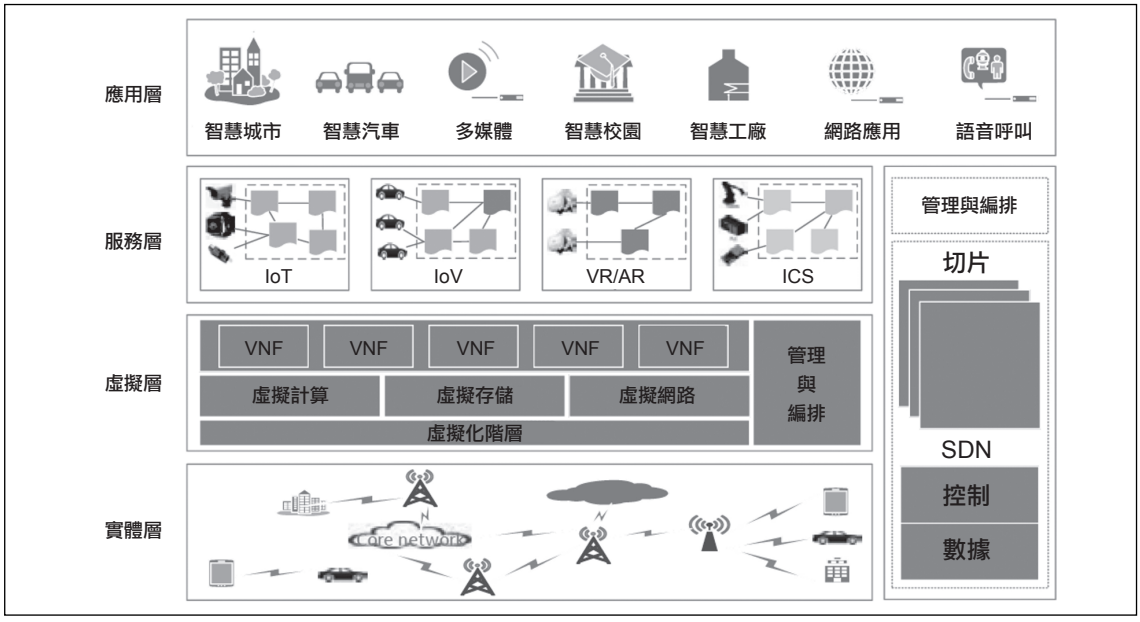

圖 1　5G 的層次結構

資料來源：本研究整理

挑戰。我們的安全框架也圍繞攻擊/防禦物件構建。表1粗略地總結5G的攻擊/防禦目標，並包含傳統物件（例如操作系統和應用軟體）以及與5G相關的物件（例如虛擬實體和控制軟體）。物件可以繼續被分割。例如，可以使用特定軟體供應商和軟體版本來詳細描述表中的控制軟體。

表1前兩列中的物件（硬體設備和無線頻道）屬於實體層。對於硬體設備，偽造設備、旁頻道攻擊和惡意破壞是主要的安全挑戰，可能導致欺騙、數據洩漏和設備不可用。為了解決這些安全威脅，可以使用安全管理、授權和加密機制。安全管理使設備與攻擊者隔離。授權和加密機制可用於識別攻擊者並防止數據被破壞和洩漏。由於無線電傳播的開放性[9]，無線頻道面臨兩個主要挑戰：未經授權的使用和竊聽攻擊。為了解決這兩個挑戰，必須防止攻擊者測量、複製和重建無線頻道。根據5G的獨特性、互惠性和多樣性，提出一些新的5G相關安全技術來滿足要求，例如射頻識別方法、竊聽編碼技術、使用隨機特徵（例如頻道狀態信息、接收信號強度、相位信息）、安全的多天線技術等等[10]。

表 1　5G 網路的物件

類別	物件
硬體設備	基地台、轉發器、路由器、交換機、伺服器、智慧設備等
頻道	無線頻道、光纖、電纜等
虛擬實體	Openstack、VMWare、虛擬機管理程序、泊塢窗、vSwitch、虛擬機（VM）、虛擬資源等
操作系統（OS）	Enea OSE、C/OS、Linux、Windows 等
控制軟體	SDN 控制器、切片控制器等
應用軟體	網路瀏覽器、數據庫、智慧手機應用軟體等
協議	通信協議、網路協議、授權協議、API 等

表1中的其餘物件屬於邏輯層。主要的安全挑戰如下。

1. 數據洩漏：通過使用NFV和網路切片，5G的實體資源在不同服務之間共享。使用差的隔離方法，攻擊者可能會破壞隔離，從而非法使用其他服務的數據。另外，由於實體資源總是從一個服務重新分配給另一服務，因此來自先前服務的殘留數據可能會洩漏給後者。因此，一些有前途的方法被研究，例如VM/切片隔離、數據擦除、數據加密和安全通信[9]。

2. 硬體、軟體和協議的漏洞：5G的關鍵組件之一是控制器，即管理和編排軟體。控制器的漏洞可被利用並用於對網路切片和相應服務發起攻擊。除了控制器漏洞之外，5G鼓勵使用新的軟體和協議，但是它也提供了未知的軟體或協議漏洞，這些漏洞對5G構成了新的威脅。

3. 外部安全威脅：Dos、DDos和MITM[18]等外部對5G關鍵組件的攻擊可能會導致嚴重問

[18] 中間人攻擊（Man-in-the-middle attack, MITM）在密碼學和電腦安全領域中是指攻擊者與通訊的兩端分別建立獨立的聯絡，並交換其所收到的資料，使通訊的兩端認為他們正在通過一個私密的連接與對方直接對話，但事實上整個對談都被攻擊者完全控制。在中間人攻擊中，攻擊者可以攔截通訊雙方的通話並插入新的內容。在許多情況下這是很簡單的（例如，在一個未加密的 Wi-Fi 無線存取點的接受範圍內的中間人攻擊者，可以將自己作為一個中間人插入這個網路）。

表 2　各種自動化攻擊和防禦框架比較

名稱	架構層次	安全機制	關鍵元件
3GPP	• 水平系統範圍(網路級、切片、應用程序級別、機密性和完整性保護、互聯） • 垂直 5G 功能元件部署（網路功能虛擬化、分佈式雲）	• 加密 • 身份驗證 • 用戶隱私	• 水平層：無線電接入單元、光學設備、以太網橋、IP/MPLS 路由器 SDn 控制器 • 垂直層：eMBB、mMTC、URLLC
Ericsson	• 標準設定 • 網路設計 • 網路部屬 • 網路運營	• 基地台重新路由流量 • 縮放機制 • 選擇性丟棄 / 限制	• 硬體：CPE、OLT、BNG、ONOS、UE • 界面：API、路由、服務閘道
Huawei	• 應用層 • 歸屬層 • 服務層 • 傳輸層	• 營運商的 5G 安全：使用者永久標識和使用者根金鑰 • 監管機構的 5G 安全規範與協定	基地台、回傳網、核心網、互聯閘道、防火牆和 IT 服務器
本研究	• 實體層 • 邏輯層（包括：虛擬層、服務層和應用層）	• 安全管理、授權和加密機制 • 射頻識別方法、竊聽編碼技術、使用隨機特徵、安全多天線技術	• 基地台、轉發器、路由器、交換機、伺服器、智慧設備 • 虛擬實體、操作系統、OS、控制與應用軟體、協議

題，例如服務不可用和偽造數據。

表2表示本章設計框架與第二章所示的國際組織企業框架(3GPP、Ericsson、Huawei)四者之間的匯總比較。

六、分級攻防模型

先前回顧的安全威脅特定於每個層。但是，對5G的大多數威脅是由攻擊組合而不是單個攻擊引起的。多種攻擊的組合可以稱為攻擊鏈。與傳統的攻擊鏈定義不同[16]，這裡的攻擊鏈著重於如何跨多個物件構建指向一個物件的攻擊路徑，而不是發起攻擊的詳細步驟。但是，5G的攻擊鏈缺乏關注。此外，針對5G的攻擊鏈不限於單層。跨層攻擊也是5G的關鍵面向。在此，首先提出一種分層的攻防模型，從而可以表達單層和跨層的攻擊鏈以及相應的防禦策略。然後，討論模型與5G之間的關係。

（一）層次模型

層次模型是以攻擊/防禦物件為基礎。在本節中，對象不是粗略的劃分，而是具有特定廠商和版本的特定攻擊/防禦物件。根據5G的層次結構和相應的安全性挑戰，攻擊/防禦物件分佈在每一層。對於同一層中的兩個物件，兩個物件之間可能存在關係。基於圖層中的物件關係，可以構建出相關圖式。如圖2a所示，共有四層，每層包含一個圖形。在圖中，節點表示攻擊/防禦物件。邊緣由兩個節點之間的關係確定。如果兩個節點之間存在一個或多個關係，則存在一條邊。節點之間的關係被視為邊緣屬性，並由攻防要求決定。例如，對於實體層上的兩個物件，可以使用連接關係。對於邏輯層上的兩個物件，可以使用函數關係。

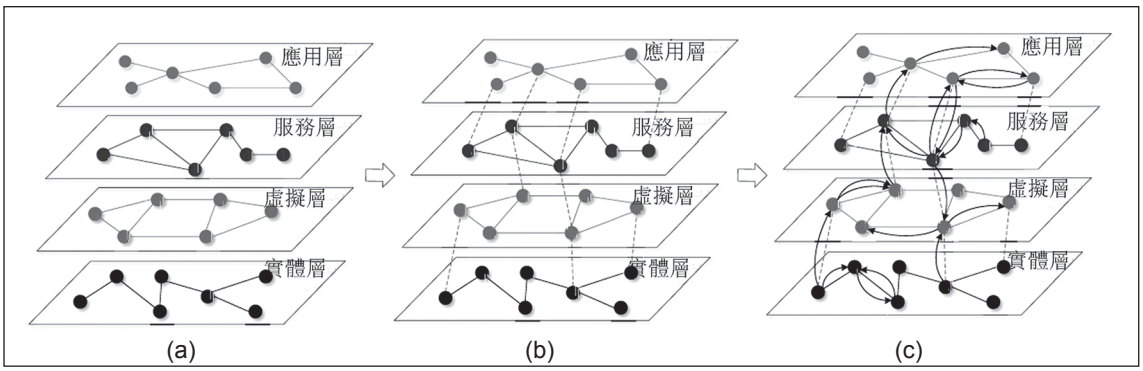

圖 2　分層攻擊和防禦模型

資料來源：[17]

物件關係不限於一層。兩層之間可能存在垂直邊緣。諸如管理、業務流程、功能支持和資源共享之類的多個關係可以用作邊緣屬性。基於垂直邊緣，獲得層次圖。圖2b顯示層次圖。虛線表示垂直邊緣，並連接所有單獨圖形。注意，切片的服務層可以具有多個切片，並且選擇一個切片來表示該層。

以層次圖為基礎，對攻擊/防禦物件的攻擊可以用三元組<obj，atk，atk_rst>表示。obj表示相應的物件。atk是一個元組，包含兩個元素：攻擊條件和攻擊方法。 atk表示為<cdt，mtd>。atk_rst是與受atk影響的另一個物件相對應的結果列表。它可以表示為一個元組列表，每個元組包含兩個元素：受影響的物件aft_obj和攻擊結果per。根據獲取的權限，攻擊結果包含多個權限，例如禁用、可讀、可寫、可執行等。因此，攻擊結果表示為<<aft_obj1，per1>，<aft_obj2，per2> <aft_objk，perk>>。基於形式化的攻擊<obj，atk，atk_rst>，在受攻擊物件和受影響物件之間建立有向邊。如果多個物件受到影響，則會建立多個有向邊。例如，三元組<Obj1，<Cdt，Akt>，<< Obj2，Readable>，<Obj3，Executable >>>表示物件Obj1在攻擊條件Cdt下受到攻擊方法Atk的攻擊。兩個物件Obj2和Obj3受到影響，並且獲得可讀和可執行權限。因此，從Obj1到Obj2和Obj3建立兩個有向邊。

根據三元組<obj，atk，atk_rst>，獲得從受攻擊對象到層次圖上受影響物件的有向邊。圖2c顯示層次結構圖，其中有向邊由黑色箭頭線表示。因此，分層圖變為分層有向圖。有向邊緣分佈在一層或兩層之間。基於有向圖，多個相鄰的有向邊緣可以形成攻擊鏈。在給定初始物件和目標物件的情況下，攻擊鏈提供兩個節點之間的攻擊路徑，並且可以逐步發起攻擊。但是，並非所有定向路徑都可以用作攻擊鏈。攻擊鏈上的每次攻擊都應滿足其攻擊條件。對於任意兩個相鄰的邊，如果通過對第一條邊的攻擊獲得的攻擊結果滿足最後一條邊的攻擊條件，則兩個相鄰邊形成一條攻擊鏈。

防禦策略也可以用三元組<cost，mtd，

dfs_rst>表示。每個三元組對應於一次攻擊（有向邊緣），並且可以是邊緣的屬性之一。cost表示該策略所需的防禦資源。mtd表示詳細的防禦方法。dfs_rst表示防禦效果。響應攻擊鏈，可以實現一系列防禦策略。但是，並非所有防禦策略都需要執行。我們只需要根據安全性要求選擇一些特定的防禦策略或針對攻擊鏈進行關鍵攻擊的防禦策略，就可以打破攻擊鏈的連通性。

（二）層次模型的討論

分層攻防模型不僅可以支持單層威脅的安全描述，還可以支持跨層威脅的安全描述。例如，將來5G可以用於智慧工廠。可能會對工業控制過程造成一些攻擊，例如篡改監視或控制數據。攻擊過程可能會跨越多個層次。首先使用輪渡攻擊來使用實體服務器，然後可以使用NFV管理器漏洞來找到相應的工業控制服務切片。基於切片資源，確定智慧工廠的邏輯拓撲，並根據具體應用進行數據篡改攻擊。整個攻擊過程跨越所有層次。根據5G架構的分層特性，從一層開始並傳播到其它層或同一層中的物件的攻擊將是5G的主要威脅之一。

分層安全模型具有三個優點：

- 可以正式表示並深入分析複雜的安全威脅，以便可以採用有效的策略來應對安全威脅。
- 基於定向路徑，可以發現未知的安全威脅，從而在可能時避免安全風險。
- 層次模型本質上是一個圖，並且適合於支持自動化攻擊和防禦。但是，分層模型只是 5G 的理論模型。如何應用該模型解決特定的安全問題仍然是有待解決。在下一章中，我們將通過使用此模型來介紹一個自動化的攻擊和防禦框架。

七、自動化的攻擊和防禦框架

大多數5G安全性研究都是依賴專家的知識，因此需要人工干預。難以滿足解決安全威脅的可伸縮性、準確性和效率的要求。因此，自動化攻防成為5G安全的關鍵研究領域之一。提出的分層攻防模型實質上是一個包含所有層中的物件及其關係圖形。相應地，它可以通過安全知識圖來實現。基於這種知識圖，可以將特定物件、漏洞、攻擊、防禦策略等相互關聯。因此，給定攻擊/防禦物件，可以根據安全知識圖上的關係自動化進行攻擊或防禦。

以安全知識圖為基礎構建自動化攻防框架，如圖3顯示的框架結構為例，該框架由四個組件組成：安全知識圖、自動化攻擊技術、自動化防禦技術和5G安全測試平台。以大量安全數據為基礎，首先構建知識圖，並通過使用已知知識，來將其用於支持自動化攻擊和防禦。然後，為了探索未知的安全威脅和有效的防禦策略，研究自動化攻擊技術和自動化防禦技術，以便向知識圖提供反饋。為了驗證新的安全技術，需要5G安全測試平台。

（一）安全知識圖

安全知識圖基於分層的攻防模型，從大量分散的安全知識中識別出多個實體（物件），並提取相應的屬性和關係。圖4顯示安

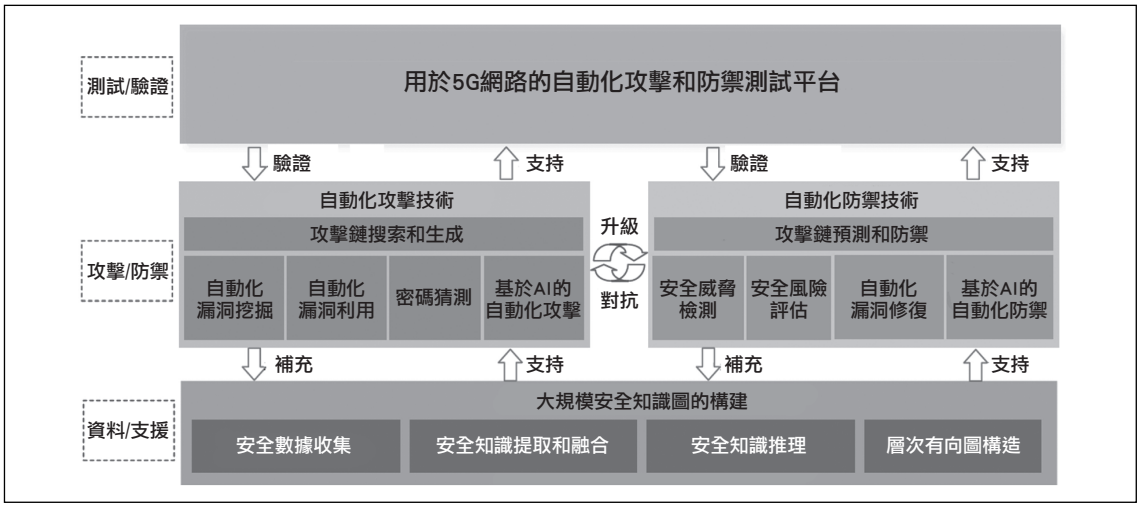

圖 3　自動化的攻擊和防禦框架

資料來源：本研究綜整

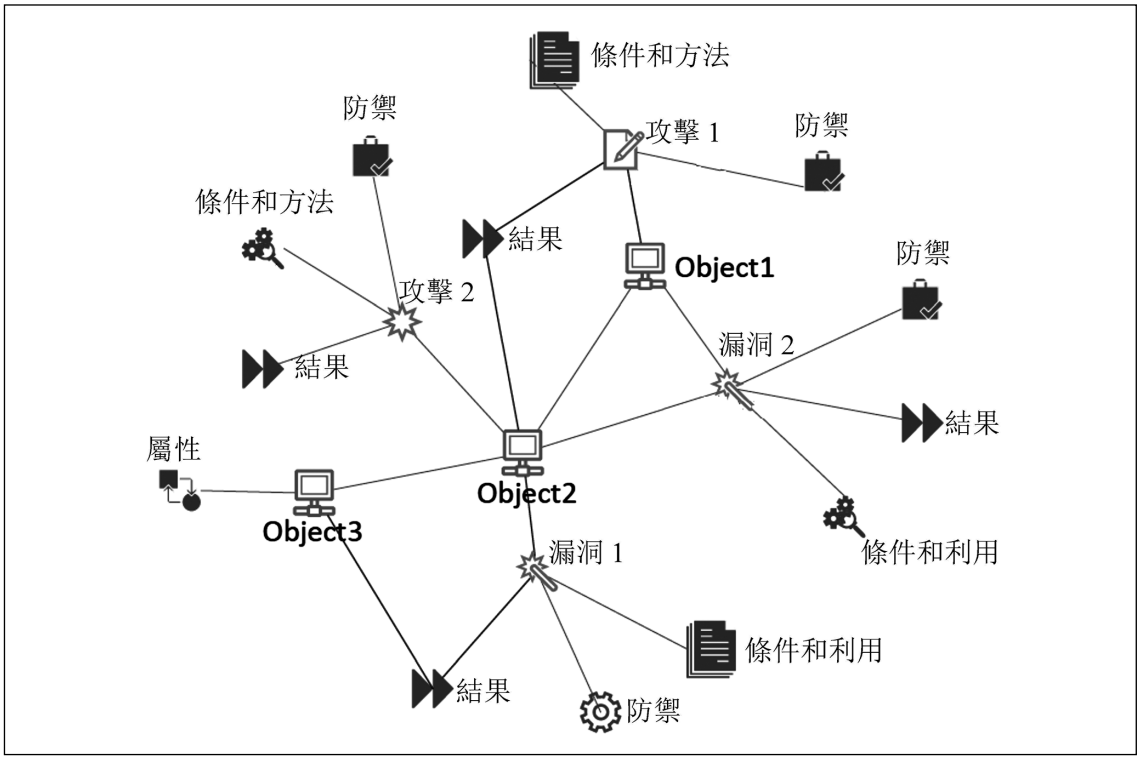

圖 4　安全知識圖的示例

資料來源：[17]

全知識圖的一部分。為了區分對攻擊/防禦物件的不同攻擊，安全威脅（例如攻擊、漏洞等）也被視為物件，而防禦策略被用作相應的屬性。圖中的紅線表示從Object1到Object3的攻擊鏈。除了所呈現的物件之外，還存在其他物件、關係和屬性。這些未在圖中顯示。

安全知識圖的構建包括三個步驟：數據收集、知識提取和融合以及知識推理。儘管成熟的技術可以直接用於構建，但應考慮5G的特殊環境。對於數據收集，應滿足大規模和動態的要求。可以通過許多現有方式獲取安全數據，例如漏洞數據庫、exploit-DB[19]、GitHub[20]、暗網[21]、安全競賽和安全事件分析。為了支持5G安全，需要一個集中式5G安全數據平台。數據提取和融合面臨準確性和完整性的挑戰。由於存在多源和非結構化數據，一個實體的兩種表示形式可能會被識別為不同的實體，因此很難準確、完整地提取關係。多源知識融合以及半結構化和非結構化數據處理應進一步研究。安全知識推理可用於發現隱藏的關係，而效率是主要挑戰。考慮到大規模知識圖，基於子圖的知識推理或基於AI的知識推理可能是有前途的方法。

如果知識圖中存在從一個物件到另一個物件的攻擊鏈，則可以自動化獲取攻擊或相應的防禦策略。否則，應添加新的條件和關係。為了支持未知的安全威脅，需要自動化攻擊和防禦技術。

（二）自動化攻擊技術

對自動化攻擊的研究集中在兩個面向。首先研究自動化攻擊的關鍵技術，例如漏洞挖掘和利用、密碼猜測、基於AI的自動化攻擊等。其次研究攻擊鏈的搜索和生成，以找到現有的和潛在的攻擊鏈。

漏洞挖掘可自動化挖掘硬體、軟體和協議中的漏洞。其中，模糊技術結合符合執行一直被使用。自動化漏洞利用技術自動地定位程式堆疊器的可跳轉位址，然後使用配置記憶體將可跳轉位址替換為shellcode[22]位址，從而可以執行該shellcode。由於5G中的物聯網設備數量眾多，物聯網硬體和新協議的漏洞需要進一步研究。對於密碼猜測，用於密碼庫中基於AI密碼生成是一種很有前途的技術。基於密碼庫，密碼猜測工具（例如HashCat和John the Ripper）用於猜測密碼，它們可能起著重要作用，尤其是在處理5G

[19] Exploit-DB 是一介面向全世界駭客的漏洞提交平台，該平台會公佈最新漏洞的相關情況，這些可以說明企業改善公司的安全狀況，同時也以幫助安全研究者和滲透測試工程師更好的進行安全測試工作。Exploit-DB 提供一整套龐大的歸檔體系，其中涵蓋了各類公開的攻擊事件、漏洞報告、安全文章以及技術教程等資源。

[20] GitHub 是一個商業網站，是目前全球最大的 Git Server。在這邊，你可以跟其它厲害的開發者們交朋友，你可以幫忙貢獻其它人的專案，其它人也可以回饋到你的專案，建立良性循環。

[21] 暗網（Dark Web）只能用特殊軟體、特殊授權、或對電腦做特殊設定才能存取，不能夠被正常網路搜尋引擎（如 Google、雅虎等）索引。

[22] shellcode 是一段用於利用軟體漏洞而執行的代碼，shellcode 為 16 進位之機械碼，以其經常讓攻擊者獲得 shell 而得名。shellcode 常常使用機器語言編寫。可在暫存器溢出後，塞入一段可讓 CPU 執行的 shellcode 機械碼，讓電腦可以執行攻擊者的任意指令。

IoT設備時。為了繞過安全檢測，進而研究一種基於AI的自動化攻擊，例如，通過使用AI技術動態更改設備使用的特性和規則，可以繞過基地台的DDoS攻擊檢測。

以上技術用於向知識圖提供反饋知識。為了利用知識圖，可以研究攻擊鏈搜索技術和攻擊鏈生成技術來發現現有的威脅和潛在的威脅。

由於現有的攻擊鏈已經記錄在知識圖中，因此可以通過攻擊鏈搜索技術獲得從某個物件開始或針對某個物件的攻擊鏈。給定一個物件，可以根據某些條件（例如最小成本和最大威脅）獲得具有從該物件開始的樹結構的多個攻擊鏈。同樣，也可以找到針對物件的攻擊鏈。從總體上看，效率是攻擊鏈搜索技術的主要重點之一。在大圖上的路徑搜索可能是一種有前途的技術。

可以使用攻擊鏈生成技術以現有知識為基礎來預測和建構未知攻擊鏈。基於AI的技術（例如圖神經網路）是一種很有前途的技術。首先通過訓練AI模型來學習現有的攻擊鏈，然後將訓練後的AI模型用於預測潛在的攻擊鏈。基於潛在攻擊鏈，探索每個邊緣的特定攻擊以確定潛在攻擊鏈是否有效。

（三）自動化防禦技術

與自動化攻擊技術類似，對自動化防禦技術的研究也包括兩個面向：

- 相互關聯的關鍵自動化防禦技術，包括安全威脅檢測、風險評估、漏洞修復和基於AI的自動化防禦。
- 攻擊鏈的預測和防禦，可以預測攻擊鏈並選擇相應的防禦策略。

為了檢測相關5G攻擊/防禦物件的攻擊，因此採用安全威脅檢測技術，並且安全態勢感知被認為是一種很有前途的檢測方法。但是，由於跨層安全威脅，傳統的態勢感知變得有限。所以，檢測實體層的變化並支持NFV、SDN和網路切片是進一步研究的主要重點。為了保證防禦策略的有效性，因此採用安全風險評估技術對安全威脅進行定量評估。由於物件數量眾多且5G環境複雜，以前的評估方法不再適用於5G，因此需要改進的方法。動態檢測可能是一種有前途的方法[18]。針對漏洞，可以採用自動化漏洞修復技術[13]。與基於AI的攻擊技術相對應，可以採用從現有防禦或攻擊方法中學習動態防禦方法的基於AI的防禦技術。除上述防禦技術外，還可以應用傳統的防禦技術，例如加密、認證和密鑰管理[19]。

基於以上技術，可以實現攻擊鏈的預測和防禦技術。當檢測到對某一物件的攻擊時，可以預測攻擊鏈路徑和潛在的最終目標。因此，可以獲得相應的防禦策略。由於攻擊和防禦的動態特性，攻擊鏈的預測和防禦策略的選擇可以採用基於博弈論的方法。此外，強化學習也有助於選擇防禦策略。最好的獎勵措施可以通過反覆試驗來學習。因此，兩種技術的結合可能是一種有前途的方法。

（四）5G 安全測試平台

5G測試平台在5G安全中起著重要作用。

它為攻擊和防禦實驗提供一個平台，並為新的安全技術提供一種驗證方法。通過使用5G安全測試平台，對現有安全問題進行廣泛而深入的研究，可發現未知的安全威脅並對其進行快速有效的響應。

目前已經存在幾個5G測試平台，但是仍然缺乏安全測試平台，尤其是對於自動化攻擊和防禦技術而言。在這裡，我們不關注特定的技術細節，而是討論實現5G安全測試平台的一些有希望的方向。根據5G安全測試平台的規模，可以從三個面向進行進一步研究：

- 可以構建具有所有層的集成測試平台，以進行大規模安全測試。
- 可以研究用於單層的水平測試平台的相應層的安全性，例如，實體層的測試平台和虛擬層的測試平台。
- 還可以構建垂直服務的測試平台。

八、5G 自動化攻擊和防禦框架

自動化攻擊和防禦框架不是5G安全的萬能框架。該框架並非旨在完全解決5G安全問題，而是為5G安全自動化提供可能的指導和一些有用的想法。

自動化攻防框架有助於應對5G中單層和跨層的綜合攻擊威脅。自動化攻擊和防禦框架還可以應對5G的已知和未知安全威脅。由於現有的攻擊鏈和防禦策略都存儲在安全知識圖中，因此可以在知識圖中自動化地找到它們。相對而言，通過使用自動化攻擊技術和自動化防禦技術，可以發現對5G的未知威脅並將其記錄在知識圖中。

該框架採用基於安全知識圖的開放架構。對於攻擊或防禦技術，它可以由安全知識圖支持，並用於發現新知識以向知識圖提供反饋知識。技術之間的關係大多是鬆散耦合的。因此，框架中使用的技術不限於現有技術。還可以對符合5G特性的新技術進行進一步研究，並將其集成到框架中。面向5G的現有安全技術和針對5G的新安全技術都值得研究。

九、結論

本文重點介紹5G安全性，並探討5G的潛在方向。提出了針對5G安全的自動化攻防框架。通過回顧5G的架構和挑戰，提出一種既支持單層安全又支持跨層安全的分層安全模型。安全模型對應於安全知識圖。基於這樣的安全知識圖，可以獲取5G安全框架，並將其用於應對已知和未知的5G安全威脅。

參考文獻

1. Du X., and H. Chen, “Security in Wireless Sensor Networks,” 2008, IEEE Wireless Commun., 15(4), 60–66.
2. Cisco, 2017, “Cisco Visual Networking Index: Global Mobile Data Traffic Forecast update (2016-2021),” Cisco White Paper, Feb. 2017.
3. Ji H., Park S., Yeo J., Kim Y., Lee J., and Shim B., 2018, “Ultra-Reliable and Low-Latency Communications in 5G Downlink: Physical Layer Aspects,” IEEE Wireless Communications, 25(3), 124-130, doi: 10.1109/MWC.2018.1700294.
4. Tian Z., Gao X., Su S., and Qiu J., 2020, “Vcash: A Novel Reputation Framework for Identifying Denial of Traffic Service in Internet of Connected Vehicles,” IEEE Internet of Things Journal, 7(5), 3901-3909, doi: 10.1109/JIOT.2019.2951620.
5. Alliance N. G. M. N., 2015, “NGMN 5G White Paper,” Next Generation Mobile Networks, White paper, Feb. 2015, 1–125.
6. Wu, Y. et al., 2018, “A Survey of Physical Layer Security Techniques for 5G Wireless Networks and

Challenges Ahead," IEEE Journal on Selected Areas in Communications.
7. Ahmad, I. et al., 2018, "Overview of 5G Security Challenges and Solutions." IEEE Communications Standards Magazine 2.1, 36-43.
8. Hawilo H., Shami A., Mirahmadi M., and Asal R., 2014, "NFV: state of the art, challenges, and implementation in next generation mobile networks (vEPC)," IEEE Network, 28(6), 18-26, doi: 10.1109/MNET.2014.6963800.
9. Wang X., Hao P., and Hanzo L., 2016, "Physical-layer authentication for wireless security enhancement: current challenges and future developments," IEEE Communications Magazine, 54(6), 152-158, doi: 10.1109/MCOM.2016.7498103.
10. Liu Y., Chen H., and Wang L., 2017, "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges," IEEE Communications Surveys & Tutorials, 19(1), 347-376, doi: 10.1109/COMST.2016.2598968.
11. Klees G., et al., 2018, "Evaluating Fuzz Testing," Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, ACM.
12. Hu, H. et al., 2015, "Automatic Generation of Data-Oriented Exploits," USENIX Security Symposium.
13. Mechtaev S., Yi J., and Rovchoudhury A., 2016, "Angelix: Scalable Multiline Program Patch Synthesis via Symbolic Analysis," Proc. 38th Int'l. Conf. Software Engineering, 691–701.
14. Wu Y., Khisti A., Xiao C., Caire G., Wong K., and Gao X., 2018, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," IEEE Journal on Selected Areas in Communications, 36(4), 679-695, doi: 10.1109/JSAC.2018.2825560.
15. Agiwal M., Roy A., and Saxena N., 2016, "Next Generation 5G Wireless Networks: A Comprehensive Survey," IEEE Communications Surveys & Tutorials, 18(3), 1617-1655, doi: 10.1109/COMST.2016.2532458.
16. Hutchins E. M., Cloppert M., and Amin R., 2011, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proc. 6th Int'l Conf. Information Warfare and Security, 1(1), 113–125.
17. Sun Y., Tian Z., Li M., Zhu C., and Guizani N., 2020, "Automated Attack and Defense Framework toward 5G Security," IEEE Network, 1-7, doi: 10.1109/MNET.011.1900635.
18. Qiu J., Du L., Zhang D., Su S., and Tian Z., 2020, "Nei-TTE: Intelligent Traffic Time Estimation Based on Fine-Grained Time Derivation of Road Segments for Smart City," IEEE Transactions on Industrial Informatics, 16(4), 2659-2666, doi: 10.1109/TII.2019.2943906.
19. Mungara R.,, Rao K. V., and Pallamreddy V. S. R., 2009, "A Routing-Driven Elliptic Curve Cryptography based Key Management Scheme for Heterogeneous Sensor Networks," IEEE Trans. Wireless Commun., 8(2), 1223–1229.