**R09921088 李昕耘**

# 5G Edge Computing

## Security Challenges and Solutions in 5G MEC Environments

## 1. Introduction

藉由連結生活的方方面面，5G 目的在於使用技術以實現需要高服務可用性和高安全性的數位社會，因此雲端計算、霧計算、邊緣運算、SDN 和 NFV 以及一些相關技術將以靈活的網路運作方式及管理方式來滿足不斷增長的客戶群和服務需求。

## MEC

最近幾年一些移動設備、或 IoT 設備等邊緣設備的數量正在以肉眼可見的速度成長，傳統雲端運算的架構上，如 Figure 1 所示，當這些邊緣設備同時使用時，對網際網路的流量會是一個挑戰，可能會在多處出現網路瓶頸，進而導致服務中斷，因此把靠近用戶的並且是 delay-sensitive 的工作項目(如 AR/VR)自雲端轉移至邊緣是個合理的選擇，如 Figure 2 所示，在 edge 先對 data 做一些較為簡單的處理也能減少 response time，對於一些 real time 的工作尤為重要。另一方面，邊緣運算需要提供 load balancing 和 service clustering 的機制來確保這些 service 的可擴展性，也不會因為增加太多的邊緣設備而導致某個節點的流量暴增造成 conjestion. 在這種架構下，這些邊緣設備會逐漸從 data 的消費者轉型成 data 的生產者。

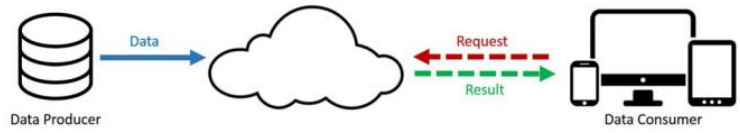


Fig. 1. Cloud computing paradigm.

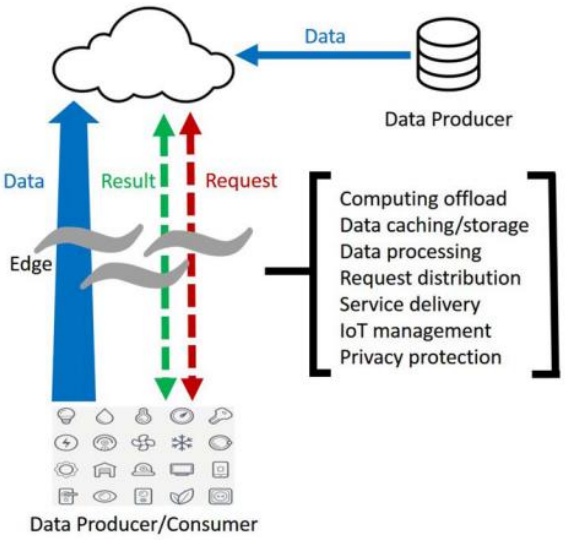


Fig. 2. Edge computing paradigm.

另一方面，當我們把運算的架構自雲端轉移至靠近使用者的邊緣時，可能會衍生出更多的安全問題，table 1 簡介了不同類型的安全威脅和攻擊，也呈現出網路中容易遭到攻擊的目標元素、服務或技術。本次研究將概略性探討一些 5G MEC 環境下的 5G Privacy、Communication Channels、SDN、NFV、MEC 可能會出現的潛在威脅，以及潛在解決方法。

| Security Threat | Target Point/Network Element | Effected Technology | | | | Privacy |
|---|---|---|---|---|---|---|
| | | SDN | NFV | Channels | Cloud | |
| DoS attack | Centralized control elements | ✓ | ✓ | | ✓ | |
| Hijacking attacks | SDN controller, hypervisor | ✓ | ✓ | | | |
| Signaling storms | 5G core network elements | | | ✓ | ✓ | |
| Resource (slice) theft | Hypervisor, shared cloud resources | | ✓ | | ✓ | |
| Configuration attacks | SDN (virtual) switches, routers | ✓ | ✓ | | | |
| Saturation attacks | SDN controller and switches | ✓ | | | | |
| Penetration attacks | Virtual resources, clouds | | ✓ | | ✓ | |
| User identity theft | User information data bases | | | | ✓ | ✓ |
| TCP level attacks | SDN controller-switch communication | ✓ | | ✓ | | |
| Man-in-the-middle attack | SDN controller-communication | ✓ | | ✓ | | ✓ |
| Reset and IP spoofing | Control channels | | | ✓ | | |
| Scanning attacks | Open air interfaces | | | ✓ | | ✓ |
| Security keys exposure | Unencrypted channels | | | ✓ | | |
| Semantic information attacks | Subscriber location | | | ✓ | | ✓ |
| Timing attacks | Subscriber location | | | | ✓ | ✓ |
| Boundary attacks | Subscriber location | | | | | ✓ |
| IMSI catching attacks | Subscriber identity | | | ✓ | | ✓ |

Table 1. Seciruty challenges in 5G technologies

# 2. Potential Security Challenges and Solutions

## 2.1 Security Challenges: Privacy in 5G

5G 生活各方面連結到網路上，讓大多數用戶的資料儲存在線上，並且共享大量資源與資料，這樣一來會造成許多的安全漏洞，以下 1G 到 5G 常見的安全漏洞:

- 1G: 手機和無線的 channel 變成主要非法 clone 和偽裝的目標。
- 2G: 垃圾郵件數量增加，以及包含像是注入假消息或令人厭煩的廣告資訊。
  3G: 基於 IP 的通信讓網路安全漏洞和挑戰轉移到了無線的區域。
- 4G: 讓智能設備、多媒體流量、和新服務擴散到移動式的領域，導致更加複雜的動態和威脅格局。
- 5G: 安全威脅比以前需求更大，對隱私的關注度也更高。

Figure 3 中呈現了 5G 網路中重要安全和隱私的挑戰:

1. Flash 網絡流量: 大量的終端用戶設備及 IoT 地導致 flash traffic 需求 。
2. 無線電接口的安全性: 無線接口加密過的 key 可能通過不安全的 channel。
3. 用戶層的資料完整性: 用戶資料層並沒有受到加密完整性的保護。
4. 對基礎設施的 DoS 攻擊: 有可見到的網絡控制元素和未加密的 control channel。
5. 對終端用戶設備的 DoS 攻擊: 在用戶設備上的 OS、APP 以及配置的數據可能沒做好安全措施。
6. 共享的資訊危機: 如前所述，5G 環境建立在很多資源與資料的共享，導致一些敏感資訊也被共享出去。
7. 偵測邊緣設備的數據造成的威脅: 攻擊者可以藉由 sensor 偵測到他們目標的使用數據（例如用電量或用水量）中進行學習，以推測房屋是否空置。 因此，如何在不

損害隱私的情況下支持服務是一個挑戰。此外，現在有非常多 WiFi 網路並不安全，可能會被監聽傳輸中的封包，或類似上述的偵測方法來偵測某個區域 wifi 網路流量。

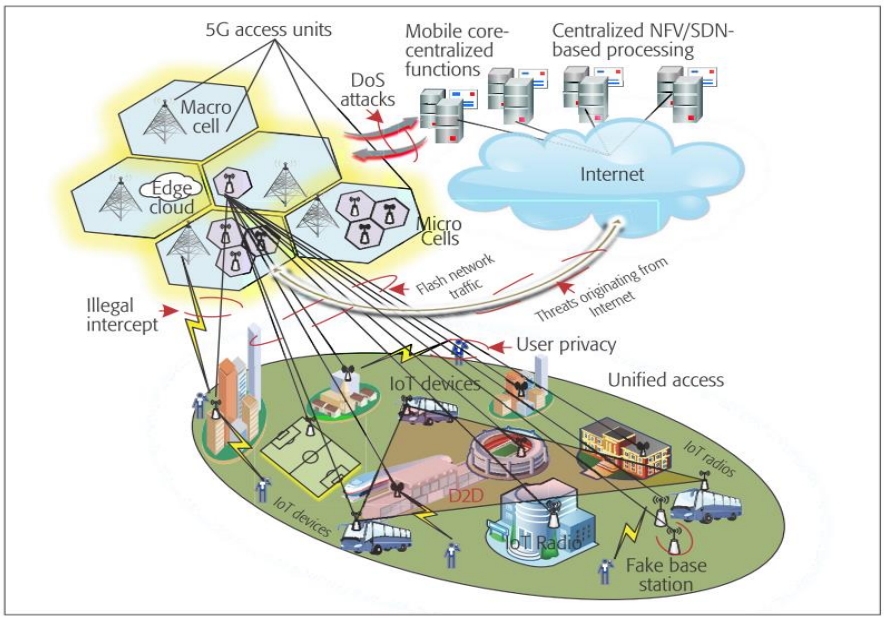


Figure 3. 5G network and the threat landscape

## Solutions

1. Flash 網絡流量: 利用 SDN 在需要的時候把資源(如頻寬)分配給網路的特定部分，SDN 控制器透過網路設備的南向 API 收集網路的統計信息，查看流量是否增加以進行資源分配，用 NFV 將來自核心網路雲的服務轉移到邊緣來滿足用戶的需求。
2. 無線電接口的安全性: 使用類似基於 Host Identity Protocol (HIP)的方案來安全地交換加密的密鑰。
3. 用戶層的資料完整性: 利用相同 end-to-end 的加密協議來維持用戶層面的完整性
4. 對基礎設施的 DoS 攻擊: 運用一些可以檢驗 DoS、DDoS 的方法來防止攻擊。
5. 對終端用戶設備的 DoS 攻擊: 運用一些可以檢驗 DoS、DDoS 的方法來防止攻擊。
6. 共享的資訊危機: 使用基於混和雲的方法: 運營商決定在何處共享數據，如在本地儲存和處理高敏感數據，在公有雲中儲存和處理非高敏感的數據。另一方面，對於位置隱私必須使用匿名技術，使用基於加密的方法來隱藏用戶真實身分。

## 2.2 Security Challenges in Communication Channels

在 5G 網絡之前，移動網絡有基於 GTP 和 IPsec 隧道的專用通信通道。只在移動網路中使用的通信接口需要高水平的專業知識才能攻擊這些接口，但在 based on SDN 的 5G 網路不會有這樣的專用接口，而是通用的 SDN 接口，而這些接口的開放性會增加被攻擊的可能性。基於 SDN 的 5G 移動網絡有三個通信通道，data channel、control channel、inter-controller channel。於當前的 SDN 系統中，這些通道使用 TLS/ SSL 來保護，但是 TLS/SSL 很容易受到 IP 層攻擊、SDN 掃描器攻擊，且缺乏強大的身份驗證機制。

### Solutions

5G 網路不只要防止攻擊，也要保持 SDN 的其他優勢，如集中策略管理、可程式化和全球網絡狀態可見性。只需要稍作修改，就可以用 IPsec 隧道來保護 5G 通信通道。此外，LTE 通信的安全性是透過各種安全演算法來提供的，如身份驗證、完整性、加密。但是這種安全方案的缺點是資源消耗大、開銷大、缺乏協調。所以這些解決方案不適用於 5G 一些關鍵 infrastructure 的通信。因此會使用一些新的安全機制，如射頻指紋的物理層安全、非對稱安全方案及根據情況來動態改變安全參數。End-to-end 的用戶通信也可以用之前提到的 HIP 加密協議來保護。

## 2.3 Security Challenges in SDN

1. SDN controller 更新或修改 flow 規則時。這種控制信息的流量容易被識別，讓 controller 在往網絡中變成可見實體，並成為 DoS 的首選目標。
2. 網絡控制的集中化容易讓 controller 在飽和攻擊的情況下變成整個網絡的瓶頸。
3. 因為可程式化，大多數網絡功能都可以實現成 SDN 的應用程式。當惡意應用程式被授予訪問權限，或一些比較關鍵的 API 暴露在預期之外的軟體時，則問題可能會在網絡中蔓延。

### Solutions

1. TopoGuard: 是 OpenFlow controller 中的一個安全插件，藉由修復網絡拓撲中的漏洞來保護 OpenFlow controller。一旦檢測到拓撲更新，TopoGuard 的拓撲更新檢查器會驗證主機遷移的合法性以及 LLDP packet 和 switch 端口屬性的完整性和來源。
2. LineSwitch: 是一種基於機率和黑名單的解決方案，可以有效解決大量 SYN request 的飽和攻擊以保護 controller 和 SDN buffer。
3. MinDos: 這種機制會根據用戶的信任程度把 flow 請求劃分為多個不同優先級的緩衝隊列，控制器採用 double polling 機制對流請求進行調度和處理，保護控制器免受 DDoS 攻擊。

## 2.4 Security Challenges in NFV

NFV 的私有部署容易受到惡意內部人員的攻擊。由於基礎設施的可訪問性，惡意用戶或受感染的 VNF 供應商可能通過插入惡意軟體或操縱網絡流量來干擾基礎設施的運作。

### Solutions

身份和訪問管理機制（如基於角色的訪問控制）可用於減輕內部攻擊的影響，藉由持續的監控每個用戶的資源消耗，並根據 IP address 的黑名單阻止惡意 request，這種方法可以防止基礎設施級別的攻擊。

## 2.5 Security Challenges in MEC

1. 由於 MEC 將雲端計算能力擴展到移動網絡的邊緣，與傳統的大型數據中心相比，能為邊緣主機提供的保護級別較低。且因為 cloud 分層的架構也讓能受到攻擊的地方增加。
2. 支持雲的物聯網環境，開發人員向 MEC 應用程式提供內容的開放 API 可能會產生漏洞，第三方形式的對手可以對這樣的 MEC 環境發起各種攻擊。

### Solutions

1. 現代 MEC 的安全解決方法大多圍繞在虛擬化技術的使用、重新設計加密方法、動態分配數據處理點。藉由每個終端節點都會通過雲端 VM 來連結到某個特定虛擬的 instance，透過每個用戶的虛擬化連結和其他用戶做隔離來提供安全性。
2. 對於一些 DoS 攻擊，用基於學習的系統來得到一定數量的封包作為樣本，再對這些封包樣本進行分析來檢測威脅程度。
3. 對於保護移動終端，最簡單的就是加裝一些防毒軟體在移動終端，或是直接從雲端託管服務。
4. 在 resource 的角度來看，任何在 edge server 上的應用程式都需要對想存取這些 application resource 的用戶進行身分驗證來避免被入侵。在移動設備的角度來看，移動設備也要對這些 edge application 進行身分驗證來產生一個相互的身分驗證。並且移動式邊緣計算平台需要保證數據的完整性。

# Reference


[1] P. Garcia Lopez, A. Montresor, D. Epema, A. Datta, T. Higashino, A. Iamnitchi, M. Barcellos, P. Felber, E. Riviere, Edge-centric Computing: Vision and Chal- lenges, SIGCOMM Comput. Commun. Rev. 45 (5) (2015) 37–42.

[2] D. Sabella, A. Reznik, D. Lopez “MEC security: Status of standards support and future evolutions” 1st edition - May 2021. ETSI White Paper No. 46

[3] Ijaz Ahmad et al. “5G security: Analysis of threats and solutions”. In: 2017 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE. 2017, 193–199.

[4] Román, Rodrigo et al. “Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges.” Future Gener. Comput. Syst. 78 (2018): 680-698.

[5] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila and A. Gurtov, "Overview of 5G Security Challenges and Solutions," in IEEE Communications Standards Magazine, vol. 2, no. 1, pp. 36-43, MARCH 2018, doi: 10.1109/MCOMSTD.2018.1700063.

[6] I. Ahmad, S. Namal, M. Ylianttila and A. Gurtov, "Security in Software Defined Networks: A Survey," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2317-2346, Fourthquarter 2015, doi: 10.1109/COMST.2015.2474118.

[7] 王麗娜, 王斐, 劉維杰. “面向 SDN 的安全威脅及其對抗技術研究”. 武漢大學學報(理學版),2019, 65(2): 153-164.