

5G và những vấn đề an ninh bảo mật mạng

TS Nguyễn Thị Xuân Thu

Học viện Cảnh sát nhân dân

5G hiện đang là công nghệ mạng không dây thế hệ mới nhất, được ứng dụng trong nhiều lĩnh vực, dịch vụ mới như: xe tự lái, chăm sóc sức khỏe từ xa, máy bay không người lái, điều khiển máy nông nghiệp từ xa... với những ưu điểm nổi bật như tốc độ nhanh hơn, độ trễ thấp hơn so với công nghệ 4G và khả năng tích hợp đa dạng thiết bị. Cùng với sự phát triển nhanh chóng của mạng 5G, các loại hình thông tin cơ động, đa môi trường, đa nền tảng sẽ phát triển mạnh mẽ, dẫn đến khả năng kiểm soát thông tin ngày càng trở nên phức tạp. Việc rò rỉ thông tin ngày càng tăng, đặt ra nhiều vấn đề về an ninh bảo mật mạng cần phải giải quyết.

Ưu thế vượt trội của công nghệ 5G

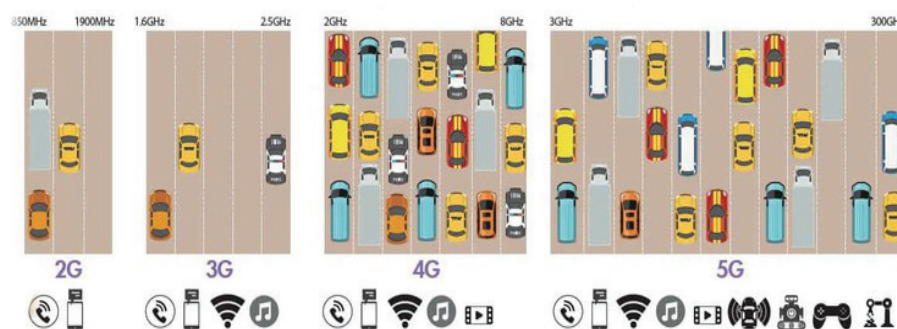
Công nghệ mạng 5G được phát triển trên nền tảng công nghệ 4G với khả năng mở rộng và hỗ trợ đa nền tảng. Các chuyên gia dự báo, 5G sẽ là xu thế công nghệ của tương lai với tốc độ nhanh vượt trội, ổn định, đáng tin cậy và khắc phục được vấn đề phủ sóng (do dùng sóng vệ tinh); sẽ có khoảng 3,5 tỷ thiết bị sẽ được kết nối 5G vào năm 2023, chiếm 20% tổng lưu lượng băng thông rộng di động trên thế giới, gấp 1,5 lần tổng lưu lượng hiện nay của 4G/3G/2G; số lượng dữ liệu sẽ tăng gấp 8 lần.

Mạng 5G được thiết kế sử dụng các dải tần số cao, hoạt động trong băng tần bước sóng milimet, dao động trong khoảng 30-300 GHz. Do đó, theo lý thuyết, tốc độ mạng 5G có thể đạt đến 10 Gb/s, thậm chí cao hơn. Trong điều kiện lý tưởng và ổn định, tốc độ mạng 5G sẽ tương đương với tốc độ cáp quang. Trên thực tế, tại Việt Nam, mạng 5G của Viettel đã đạt tốc độ truyền dữ liệu kỷ lục

là 4,7 Gb/s, cao hơn 40 lần tốc độ 4G hiện có.

Công nghệ mạng 3G có độ trễ khoảng vài trăm mili giây (ms). Mạng 4G trên lý thuyết có độ trễ là 10 ms, nhưng thực tế ban đầu có độ trễ 100 ms và hiện nay đã giảm xuống còn khoảng 30-70 ms. So sánh với công nghệ 3G, 4G, mạng 5G có độ trễ cực thấp (trong khoảng 5-20 ms) và có tham vọng cải tiến tối ưu, đẩy độ trễ xuống chỉ còn 1 ms. Điều này có ý nghĩa rất quan trọng trong việc ứng dụng công nghệ 5G vào một số lĩnh vực đòi hỏi độ trễ của tín hiệu cực thấp như xe tự lái, máy bay tự lái...

Theo chuẩn công nghệ 5G, các trạm phát 5G phải hỗ trợ cho ít nhất một triệu thiết bị kết nối trong mỗi km². Các nhà cung cấp dịch vụ đã giới thiệu công nghệ 5G với các trạm cơ sở kích thước siêu nhỏ, có mức tiêu thụ năng lượng thấp, được lắp đặt ở bất kỳ đâu. Với sức chứa lớn hơn 4G từ 10-100 lần, mạng 5G sẽ biến kỷ nguyên IoT thành sự thật trong tương lai không xa khi mọi thiết bị như ổ cắm, điều hòa, tủ lạnh, đèn giao thông, camera... đều có thể kết nối internet và tích hợp vào hệ thống với tốc độ nhanh, độ trễ thấp.



Tốc độ và sức chứa của mạng 5G so với các công nghệ cũ.

Công nghệ 5G có khả năng tương thích ngược với mạng khác, nó sẽ bổ sung thêm kiến trúc mới cho mạng truy nhập vô tuyến đám mây với các trung tâm dữ liệu nano hỗ trợ các chức năng mạng dựa trên máy chủ như cổng IoT công nghiệp, bộ nhớ đệm video và chuyển mã cho định dạng UltraHD (độ nét siêu cao). Mạng 5G còn hỗ trợ cấu trúc liên kết với các mạng không đồng nhất, tạo thuận tiện hơn cho người dùng, mang đến sự gia tăng đáng kể trong các trạm gốc và các yêu cầu mới cho đường truyền kết nối giữa nhà cung cấp dịch vụ với các trạm phân phối tới người dùng đầu cuối.

Rủi ro tiềm ẩn về an ninh bảo mật

Công nghệ 5G có nhiều ưu điểm vượt trội so với các thế hệ công nghệ trước đây, giúp tiết kiệm năng lượng, mang đến nhiều trải nghiệm internet tốt hơn. Tuy nhiên, sức ảnh hưởng của nó, cũng như những nền tảng công nghệ mới khác, tiềm ẩn nhiều rủi ro an ninh bảo mật. Theo những dự đoán về công nghệ mạng 5G của Kaspersky, sự gia tăng vượt trội về số lượng và tốc độ truyền phát dữ liệu của các thiết bị, phần mềm sẽ dẫn đến nhiều mối đe dọa. Những rủi ro tiềm ẩn về an ninh bảo mật mạng 5G mà kẻ tấn công có thể lợi dụng gồm: lấy cắp, truy cập bất hợp pháp dữ liệu; kiểm soát các dịch vụ quan trọng; phá hoại kết cấu cơ sở hạ



Mạng 5G mang tới nhiều thách thức bảo mật.

tầng; gây gián đoạn kết nối; gây ảnh hưởng về an toàn thông tin, an ninh kinh tế, chính trị.

Lỗ hổng bảo mật của dịch vụ viễn thông và cơ sở hạ tầng: khi công nghệ 5G ngày càng phát triển, kéo theo sự gia tăng của các thiết bị phần cứng, phần mềm mới cũng như những mô hình, cách thức quản trị mới. Điều này dẫn đến các lỗ hổng bảo mật để những kẻ xấu tấn công, phá hoại kết cấu hạ tầng mạng, gây gián đoạn, làm giảm chất lượng đường truyền; gây ảnh hưởng lớn đến an ninh kinh tế, quốc phòng của không chỉ một quốc gia mà có thể là cả một khu vực quốc tế. Kẻ tấn công có thể lợi dụng các lỗ hổng bảo mật để phát tán mã độc nhằm phá hủy hệ thống hay lợi dụng thực hiện tấn công từ chối dịch vụ DDoS.

Quyền riêng tư và an toàn của người dùng dễ bị tổn thương: sự phổ biến của 5G cùng với xu thế IoT đồng nghĩa với việc mọi thiết bị có kết nối internet, các trạm thu phát sóng siêu nhỏ được triển khai ở mọi nơi. Như vậy, kẻ tấn công có thể thu thập và theo dõi chính xác vị trí của người dùng, dễ dàng hơn trong việc nắm bắt hành vi và lịch sử truy cập của người dùng. Một vấn đề khác là các nhà cung cấp dịch vụ mạng sẽ có quyền truy cập sâu hơn, rộng hơn vào lượng dữ liệu lớn được gửi tới từ nhiều thiết bị của người dùng. Qua đó, có thể làm lộ thông tin riêng tư của người dùng hoặc sử dụng cho các mục đích như quảng cáo, môi giới.

Trong một thế giới vạn vật kết nối, bất kỳ một đe dọa nào trong mạng lưới cũng sẽ gây ảnh

hưởng lớn tới toàn bộ hệ thống mạng. Do vậy, sự phụ thuộc vào mạng 5G càng cao thì rủi ro càng lớn, thậm chí có thể gây ra thảm họa ở quy mô quốc gia hoặc quốc tế. Ví dụ như sự cố trong điều khiển hoạt động từ xa có thể cướp đi sinh mạng của bệnh nhân đang phẫu thuật; xe tự lái có thể gây tai nạn nếu mất kết nối; thành phố thông minh, hệ thống giao thông thông minh, nhà máy tự động hóa... có thể ngừng hoạt động khi bị mất điện, mất internet; rò rỉ thông tin mật khiến an ninh quốc gia bị đặt vào tình huống nguy cấp...

Giải pháp cho an ninh bảo mật mạng 5G

Khi vạn vật được kết nối thì cơ hội phá hoại và các cuộc tấn công mạng cũng gia tăng. Cơ quan An ninh mạng châu Âu (ENISA) đã cảnh báo: mạng di động 5G với tốc độ vượt trội và sự phát triển nhanh chóng sẽ kéo theo nguy cơ rất cao về an ninh mạng. Bên cạnh đó, cấu trúc phức tạp của mạng di động 5G cũng khiến việc bảo vệ hệ thống khó khăn hơn nhiều so với các mạng trước đó. Tuy nhiên, 5G không phải là mối đe dọa mà là một công cụ hữu ích có thể mang lại những giá trị vô cùng lớn khi được triển khai đúng cách, đặc biệt khi được triển khai với một chiến lược an ninh bảo mật mạng hiệu quả. Để đảm bảo được an ninh, an toàn các ứng dụng trên nền

tầng 5G, các quốc gia, các tập đoàn, doanh nghiệp, nhà cung cấp hạ tầng, công nghệ và các cá nhân phải cùng nhau hợp tác trên nhiều khía cạnh, cụ thể là:

Thứ nhất, các quốc gia cần xây dựng các bộ luật, ban hành các quy định về chuyển đổi số, xây dựng chính phủ điện tử, làm rõ trách nhiệm của các bộ, ban, ngành trong việc khai thác, ứng dụng công nghệ 5G.

Thứ hai, ngành công nghệ thông tin cần thúc đẩy việc thiết lập các tiêu chuẩn 5G và xác định các tiêu chuẩn ứng dụng, yêu cầu an ninh bảo mật theo từng giai đoạn để hỗ trợ các ngành khác trong việc sử dụng công nghệ 5G.

Thứ ba, các nhà cung cấp dịch vụ mạng, hạ tầng, công nghệ cần xây dựng một hệ thống mạng đủ mạnh, bền vững, đảm bảo khả năng ứng phó với các cuộc tấn công mạng có mức độ phức tạp và quy mô rộng.

Thứ tư, đơn vị cung cấp giải pháp công nghệ thông tin và truyền thông cần xây dựng hệ thống đảm bảo an ninh mạng một cách đồng bộ, đảm bảo an ninh bảo mật của các sản phẩm và dịch vụ đang được cung cấp; tăng cường đầu tư đổi mới công nghệ, phát triển và sử dụng các công nghệ tiên tiến trong đảm bảo an ninh, bảo mật mạng 5G.

Thứ năm, người dùng cá nhân cần nâng cao nhận thức

về an ninh bảo mật mạng 5G, hiểu rõ những kiến thức về mạng internet và các mối đe dọa trên môi trường internet, hình thành thói quen sử dụng mạng an toàn, bảo mật.

Bên cạnh đó, cần có sự đổi mới, sáng tạo trong xây dựng an ninh bảo mật mạng 5G. Công nghệ 5G được coi là tương lai của internet với nhiều ứng dụng mới và sáng tạo. Ngành công nghệ thông tin và truyền thông cần tăng cường giao lưu, hợp tác với các ngành khác để cùng khai thác, phát triển mạng 5G; chú trọng tới những tổ chức, doanh nghiệp có yêu cầu bảo mật kinh doanh đặc thù; định nghĩa rõ hơn về các tiêu chuẩn của mạng 5G... Chỉ có như vậy mới phát huy được hết giá trị của mạng 5G và giảm thiểu các nguy cơ có thể xảy ra ✍

TÀI LIỆU THAM KHẢO

1. <https://securelist.com/5g-predictions-2020/95386/>.
2. <https://docs.fcc.gov/public/attachments/DOC-354283A1.pdf>.
3. J.M. Lopez-Soler, et al. (2020), "A survey on 5G usage scenarios and traffic models", *IEEE Communications Surveys & Tutorials*, **22(2)**, DOI:10.1109/COMST.2020.2971781.