3 kịch bản ứng dụng IPv6 trong IoT trên thực tế

>TRẦN THỊ PHƯƠNG THẢO

Hiện nay việc nghiên cứu và triển khai áp dụng IoT đang diễn ra mạnh mẽ trên thế giới. Tuy nhiên việc triển khai áp dụng IoT vẫn còn gặp phải những thách thức trên nhiều khía cạnh, như vấn đề về nguồn năng lượng thấp của các thiết bị, lỗ hổng về an toàn thông tin khi gia nhập vào hệ sinh thái IoT, hay việc đảm bảo có đủ địa chỉ mạng cung cấp cho số lượng đối tượng khổng lồ tham gia vào IoT... Khi nghiên cứu và cho ra đời giao thức mạng IPv6, các chuyên gia nhận thấy triển khai IoT sẽ không thể tách rời IPv6 bởi những ưu điểm vượt trội của IPv6 so với IPv4 về số lượng địa chỉ, về vấn đề bảo mật thông tin...

Để có cái nhìn cụ thể hơn vai trò của IPv6 trong IoT, chúng ta cùng tìm hiểu qua ba kịch bản áp dụng thực tế IPv6 vào IoT đang được thực hiện từ dự án IoT6. Các trường hợp áp dụng thực tế được giới thiệu một cách tổng quan về phương thức hoạt động giữa các thiết bị khác nhau và làm sao để tạo ra sự tương tác giữa các dịch vụ trong IoT cloud. Cụ thể, kịch bản đầu tiên sẽ minh họa việc tích hợp các thiết bị đang hoạt động ngoài khối IoT cùng tham gia vào quá trình tương tác với các thiết bị bên trong khối bằng việc sử dụng giao thức IPv6 đồng nhất. Tiếp theo là một kịch bản phức tạp hơn với việc đưa thêm biện pháp an ninh vào trong kịch bản. Và cuối cùng, là kịch bản cụ thể ở chế độ bảo trì, với tình huống cần thay thế một thiết bị gặp trục trặc. Bối cảnh của cả ba kịch bản, đều diễn ra trong một tòa nhà có các thiết bị tự động được lắp đặt từ trước và một văn phòng Thông minh đang tham gia vào khối IoT cloud.

Trước khi đi vào giới thiệu từng kịch bản, chúng ta cần phải phân biệt được hai loại thiết bị/hệ thống được nhắc đến như sau:

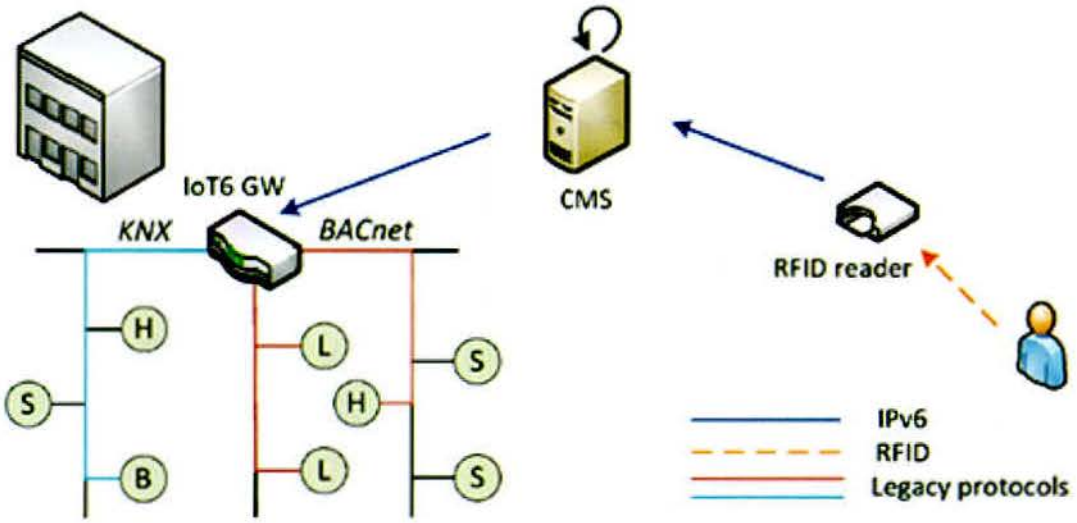
Một là các thiết bị hoạt động độc lập bên ngoài khối IoT (ở đây là tất cả các thiết bị tự động trong tòa nhà (kí hiệu là: (L), (S), (H), hay (A)).

Hai là các thiết bị/ hệ thống nằm trong khối IoT cloud, mỗi thiết bị/ hệ thống này luôn luôn giao tiếp bằng IPv6, và cung cấp một dịch vụ nhất định nào đó trong khối IoT cloud. Bao gồm: Máy quét thẻ RFID: RFID reader; Gateway: IoT6[1] GW; Bộ định tuyến thông minh: Smart Router; Hệ thống giám sát và điều hành: CMS; Máy chủ quản lý năng lượng tòa nhà: BEMS; Bộ tập hợp danh bạ địa chỉ tài nguyên chung: GRD; Máy chủ hỗ trợ vấn đề an ninh: StS; Thiết bị hỗ trợ chức năng Bảo trì: MaT; Dịch vụ tra cứu thông tin thành phần (Smart Things Information Service - STIS STIS); Hệ thống quản lý hàng hóa: IMS.

ỨNG DỤNG 1: VĂN PHÒNG THÔNG MINH VÀ VIỆC TÍCH HỢP VỚI CÁC THIẾT BỊ TRONG TÒA NHÀ

Khi tồn tại việc không đồng nhất về công nghệ của rất nhiều thiết bị cũng như mạng lưới trong một khu vực nhất định thì việc tích hợp tất cả khu vực đó vào Internet chỉ thông qua một giao diện duy nhất vẫn là một thách thức. Trong kịch bản này, thách thức được giải quyết bằng IPv6 và IoT. Trong đó, một số thiết bị tự động đang hoạt động theo những mạng từ trước (BACnet, KNX) (2) được tích hợp thông qua một gateway có nhiệm vụ chuyển đổi các gói tin nhắn của những giao thức mạng khác sang các gói IPv6 và ngược lại, điều này tạo ra việc điều chỉnh các thiết bị thuộc các mạng khác nhau vẫn có thể cùng hoạt động đồng bộ như một thành phần của IoT.

[1] IoT6: là cụm từ viết tắt của dự án nghiên cứu về IoT trong tương lai do nhóm nghiên cứu FP7 (7th Framework Programme) thực hiện trong vòng 3 năm từ tháng 10 năm 2011 đến tháng 9 năm 2014. Mục đích chính của dự án là tìm hiểu những lợi ích từ IPv6 với các tiêu chuẩn như (6LoWPAN, CORE, COAP..) để khắc phục những hạn chế của nền tảng IoT hiện nay.



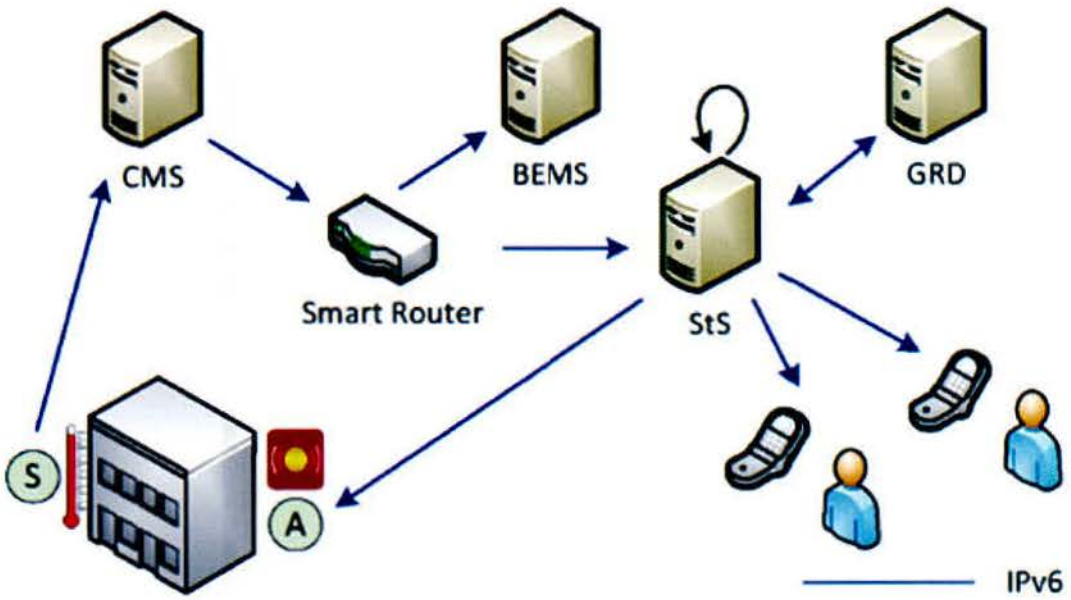
Mô hình kết nối Kịch bản 1

Kịch bản này bắt đầu khi một nhân viên muốn đi vào tòa nhà và quét thẻ RFID của mình tới thiết bị quét thẻ RFID của hệ thống. Khi đó thiết bị quét thẻ RFID sẽ truyền tín hiệu tới hệ thống CMS. Hệ thống CMS lấy ra hồ sơ cá nhân được lưu trữ của nhân viên đó và gửi đi những cài đặt và các lệnh tương ứng tới gateway IoT6 GW, thiết bị gateway IoT6 GW có nhiệm vụ truyền tín hiệu điều khiển tới các thiết bị khác nhau đang làm việc theo những mạng lưới tự động không đồng nhất và điều chỉnh cấu trúc các gói tin về cùng cấu trúc của gói tin IPv6 chung cho tất cả các thiết bị khi giao tiếp giữa bên trong và bên ngoài khối IoT. Bằng cơ chế này, IoT6 GW sẽ giúp chuyển đi các câu lệnh cụ thể từ hệ thống CMS tới các thiết bị bên ngoài khối IoT cloud như: thiết bị điều khiển hệ thống sưởi (kí hiệu là H) và hai thiết bị điều khiển ánh sáng (L) và hệ thống rèm che nắng kí hiệu (B) sẽ được điều chỉnh, mặc dù những thiết bị đang nằm trong những mạng khác nhau, cụ thể là BACnet, và KNX.

Tương tự, khi nhân viên rời khỏi văn phòng của mình, sẽ quét thẻ RFID cá nhân cho máy quét tần số RFID, hệ thống CMS lập tức nhận được tín hiệu rằng nhân viên sắp rời khỏi tòa nhà, và hệ thống sẽ thiết lập các chế độ tiết kiệm năng lượng và tắt đi các thiết bị văn phòng liên quan. Ngoài ra, còn có thể có một bộ cảm biến sự hiện diện nhân viên trong văn phòng cài đặt để đo khoảng thời gian vắng mặt của nhân viên để điều chỉnh chế độ tắt bật thiết bị văn phòng cho hợp lý hơn.

ỨNG DỤNG 2: HỆ THỐNG CÓ CHỨC NĂNG CẢNH BÁO AN TOÀN VÀ ĐỊNH TUYẾN ĐỘNG

Trong kịch bản này có sự phức tạp hơn một chút so với kịch bản đầu tiên. Như thiết lập ban đầu cho kịch bản, một bộ cảm biến nhiệt độ (thiết bị này có hỗ trợ IPv6) kí hiệu là S, sẽ định kỳ gửi các bản tin cập nhật giá trị nhiệt độ tới hệ thống CMS, và đây là một dịch vụ được cung cấp trong IoT cloud. Khi bộ cảm biến gửi về thông tin cập nhật nhiệt độ cao vượt ngưỡng nhiệt độ an toàn cho phép được cài đặt, hệ thống CMS sẽ phát hiện ra sự bất thường và gắn cờ đánh dấu lên những bản tin nhận được này thành một bản tin cảnh báo. CMS gửi các bản tin bao gồm cả bản tin bình thường và bản tính có gắn cờ cảnh báo đến bộ định tuyến thông minh, tại đây với những loại bản tin khác nhau, bộ định tuyến sẽ được lựa chọn theo những đường đi (route) khác nhau. Nếu nhận được các bản tin chứa nội dung thông báo nhiệt độ bình thường, bộ định tuyến thông minh sẽ gửi bản tin này đến một máy chủ quản lý năng lượng tòa nhà (BEMS) – máy chủ này sẽ làm nhiệm vụ lưu lại thông tin và báo cáo nhu cầu sử dụng năng lượng của tòa nhà. Tuy nhiên, khi có bản tin gắn cờ cảnh báo (nhiệt độ quá cao), bộ định tuyến thông minh sẽ phân loại mức độ ưu tiên của bản tin (cảnh báo) và theo cách gắn cờ của hệ thống CMS, sẽ gửi đi bản tin này tới máy chủ hỗ trợ vấn đề an ninh (StS) - máy chủ này có chức năng tiếp nhận xử lý và

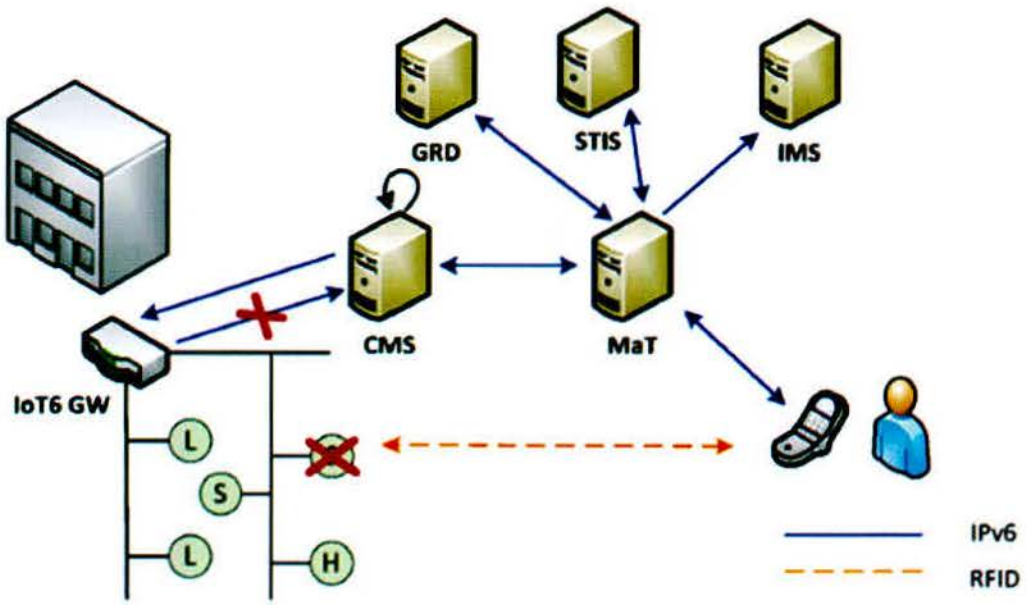


Mô hình kết nối Kịch bản 2

theo dõi các trường hợp cảnh báo. Khi StS nhận được giá trị bất thường, trước tiên nó sẽ trao đổi thông tin với bộ tập hợp danh bạ địa chỉ tài nguyên chung (GRD) để lấy thông tin về vị trí của cảm biến và thực hiện so sánh vị trí đó với vị trí các thiết bị báo động kí hiệu A (thiết bị A có hỗ trợ IPv6) và tiến hành kích hoạt các thiết bị báo động ở khu vực gần nơi có nhiệt độ cao. Nếu StS không chứa các thông tin về vị trí đặt thiết bị báo động, StS sẽ gửi truy vấn tới GRD yêu cầu cung cấp thông tin các thiết bị báo động ở khu vực gần vị trí cảm biến (ví dụ, trong bán kính 15 mét). Bất kỳ thiết bị báo động nào trong phạm vi được tìm thấy sẽ được yêu cầu bật chế độ báo động. Ngoài ra, bộ StS cũng có thể chứa danh sách điện thoại di động kèm vị trí khu vực hoạt động của số điện thoại của những người phụ trách (ví dụ như các nhân viên cứu hỏa, kỹ sư hệ thống) hoặc nó thể tra cứu thông tin về vị trí hiện tại của các số điện thoại di động trong danh sách bằng việc gửi truy vấn bổ sung đến GRD. Sau khi nhận được thông tin này, CMS có thể thông báo cho những người có trách nhiệm gần khu vực đó về tình huống cảnh báo thông qua điện thoại di động của họ. Tất cả các giao tiếp trong kịch bản đều được xử lý thông qua IPv6, cho thấy sự đa dạng của các thiết bị và các thành phần đều có thể được tích hợp trong IoT. Với các thiết bị hoạt động bên ngoài khối IoT, như bộ cảm biến hoặc thiết bị điều khiển tự động trong tòa nhà, chúng ta hoàn toàn có thể đặt thêm một thiết bị Gateway IoT6 để đồng bộ hóa như Kịch bản 1.

ỨNG DỤNG 3: TRƯỜNG HỢP CẦN BẢO TRÌ TRONG TÒA NHÀ

Kịch bản thứ ba liên quan đến việc thực hiện quá trình bảo trì. Ở kịch bản này, yêu cầu một số hệ thống thành phần trong IoT được kết hợp với nhau để phát hiện được lỗi hoặc gián đoạn xảy ra trên những thiết bị trong tòa nhà và xác định nguyên nhân. Các thiết bị cảm biến tham gia làm việc trong môi trường IoT thông qua một gateway IoT6, để đảm bảo tất cả các thiết bị luôn làm việc trong môi trường mạng đồng nhất với giao thức IPv6 (như trong Kịch bản 1). Kịch bản này bắt đầu khi một cảm biến nhiệt độ bị hỏng. Thông thường, hệ thống CMS sẽ luôn theo dõi việc gửi bản tin chứa giá trị nhiệt độ của thiết bị, để có thể phát hiện các tình huống khẩn cấp hoặc lấy số liệu cho báo cáo sử dụng năng lượng của tòa nhà (như trong Kịch bản 2). Khi cảm biến bị hỏng, việc nhận được bản tin cũng bị mất, hệ thống CMS sẽ để chế độ chờ bản tin trong khoảng thời gian nhận định, quá thời gian này mà không được nhận bản tin, CMS sẽ xác định cảm biến nhiệt độ gặp trục trặc. Khi đó, một bản tin được tạo ra ở CMS sẽ gửi sang thiết bị có chức năng thực hiện



Mô hình kết nối Kịch bản 3

bảo trì của tòa nhà – MaT (Mantainance Tool) để thông báo. Đôi khi thiết bị MaT có thể đặt luôn trong hệ thống CMS (nếu như có cấu trúc không quá phức tạp); tuy nhiên trong kịch bản này, MaT là một thành phần tách riêng trong khối IoT cloud. Ngay khi thiết bị MaT nhận được thông báo có sự cố, nó sẽ tạo ra một ticket cảnh báo và gửi thông báo lỗi tới một loạt thiết bị điện thoại di động của những người có trách nhiệm (ví dụ: kỹ sư hệ thống) bằng việc tra cứu vị trí thông qua gửi truy vấn tới GRD (như Kịch bản 2). Sau khi tiếp nhận được thông tin có trục trặc của cảm biến, kỹ sư chịu trách nhiệm sẽ dùng ứng dụng bảo trì thiết bị trên điện thoại di động để quét thẻ RFID của thiết bị và thông tin được chuyển tới MaT để tìm ra thiết bị liên quan đến thẻ RFID tương ứng. Và sau đó, MaT tiếp tục truy vấn GRD để lấy ra địa chỉ vị trí đặt dịch vụ thông tin thông minh (Smart Things Information Service - STIS), một dịch vụ giống như cơ sở dữ liệu cung cấp thông tin chi tiết giữa các thẻ RFID và thiết bị tương ứng. MaT tiếp tục gửi lại thông tin này cho ứng dụng bảo trì đang chạy trên thiết bị di động của kỹ sư chịu trách nhiệm để người này thêm thông tin về thiết bị. Với sự trợ giúp của thông tin này, kỹ sư có thể sẽ chẩn đoán được lỗi của thiết bị. Hệ thống CMS sẽ hoạt động như thiết bị chuyển tiếp thông tin giữa MaT và IoT6 Gateway, giúp nhận và gửi đi các gói tin qua lại của 2 thiết bị. Trong trường hợp thiết bị được chẩn đoán là phải thay thế, thiết bị MaT sẽ thực hiện việc này bằng cách: với thông tin có được từ STIS, nó sẽ sử dụng để trực tiếp đặt hàng thiết bị phù hợp trên hệ thống quản lý hàng hóa (IMS), một dịch vụ khác trong IoT (MaT sẽ lấy thông tin địa chỉ của IMS từ việc truy vấn GRD). Đôi khi, hệ thống IMS hoàn toàn có thể là một phần của MaT, và không cần tách riêng thành hai thiết bị.

Chúng ta đã tìm hiểu tổng quan về ba kịch bản được áp dụng trong thực tế khi triển khai dự án IoT6 - một dự án kết hợp IPv6 vào IoT. Tất nhiên, để hiểu được cặn kẽ về cách thức làm việc trong mỗi mô hình, chúng ta còn cần hiểu sâu hơn về các cơ chế, và cách thức làm việc, cũng như cấu trúc bản tin trong mỗi đường truyền, hay rất nhiều vấn đề chi tiết khác. Tuy nhiên, một cách tổng quan, bài viết cũng hy vọng đã mang đến cho người đọc một góc nhìn phù hợp.❖

Tài liệu tham khảo

[1] http://www.iot6.eu/iot6usecases

[2] https://en.wikipedia.org/wiki/Building_automation