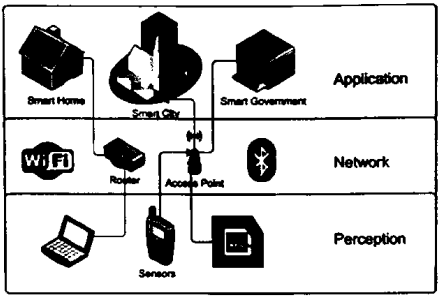
DƯƠNG THỊ THANH TÚ,
ĐỖ MINH HIỆP

1. Giới thiệu chung

Internet của vạn vật hay IoT mang tới một viễn cảnh về sự hợp nhất thông tin, nơi không chỉ hệ thống máy tính mà còn là tất cả những thiết bị điện tử xung quanh con người, đều sở hữu khả năng cảm biến, có thể hợp tác với nhau, nhằm tạo được sự tiện lợi và thông minh nhất cho cuộc sống con người. Thiết bị trong IoT là một bộ sưu tập về kích thước, công nghệ, có thể hoàn toàn khác nhau về mặt cấu trúc, chức năng cũng như đến từ nhiều nhà cung cấp thiết bị khác nhau. Điều này mang lại cho IoT sự phong phú về chủng loại và khả năng đáp ứng nhiều yêu cầu hơn, cũng như đa dạng hóa giá thành sản phẩm, nhằm làm hài lòng kể cả người tiêu dùng khó tính nhất mà vẫn đảm bảo cung cấp sự phục vụ chu đáo và tận tình [1]. Tuy nhiên chính do sự đa dạng từ mẫu mã, thiết kế, nguồn điện năng tiêu thụ cũng như khả năng xử lý chênh lệch lại gây ra các thách thức vô cùng lớn, trong việc định hình một cấu trúc chung cho IoT cũng như việc đảm bảo an ninh theo cấu trúc chung đó. Cho đến hiện nay, các chuyên gia vẫn chưa đưa ra được một kiến trúc thống nhất cho IoT, mặc dù đã có nhiều phương án được đề xuất. Tuy nhiên, từ những phương án đề xuất, mô hình kiến trúc cơ bản IoT hình thành với 3 phân lớp chính: lớp vật lý, lớp mạng và lớp ứng dụng [2].

- ***Lớp vật lý:*** Lớp này nhằm đảm bảo mục đích tập hợp thông tin và sử dụng các loại hình truyền thông khác nhau để tiến hành gửi và nhận dữ liệu tới lớp mạng.
- ***Lớp mạng:*** Lớp mạng của IoT phục vụ chức năng định tuyến và truyền dữ liệu từ các thiết bị IoT đến trung tâm xử lý dữ liệu và các thiết bị IoT khác. Tại đây, nền tảng điện toán đám mây, các cổng ứng dụng, chuyển mạch và các thiết bị định tuyến,... chuyển giao dữ liệu bằng cách sử dụng một số công nghệ rất mới như Z-wave, Zigbee, EPC Global, LTE-A, Bluetooth Low Energy (BLE), IEEE 802.14.5, 6LowPAN,... Trong đó các cổng ứng dụng có nhiệm vụ tập hợp, chọn lọc và truyền dữ liệu đến và đi từ các thiết bị cảm biến khác nhau.
- ***Lớp ứng dụng:*** Lớp này có vai trò tiếp nhận luồng dữ liệu đã được lọc bởi các cổng ứng dụng khác nhau, sau đó tiến hành phân tích và điều khiển thiết bị nhằm mục đích đưa ra quyết định nhanh chóng và chính xác nhất theo từng ngữ cảnh cụ thể. Hơn nữa chúng còn đảm bảo tính xác thực, tính toàn vẹn cũng như tính bí mật của dữ liệu. Chính nhờ khâu xử lý này mà muc đích chính của IoT (tạo ra một môi trường thông minh) đã đạt được.



Hình 1: Kiến trúc ba lớp của mô hình IoT cơ bản.

2. Các hình thức tấn công, gây mất an toàn thông tin trong IoT

Mỗi lớp IoT nhạy cảm với các mối đe dọa an ninh và các cuộc tấn công khác nhau, có thể là tấn công bị động hoặc chủ động. Sự tấn công cũng có thể bắt nguồn từ các nguồn tấn công bên ngoài, trực tiếp gây dừng dịch vụ; trong khi các cuộc tấn công từ bên trong sẽ giám sát hay ăn cắp, thay đổi thông tin trong mạng IoT mà không cần cản trở dịch vụ của người dùng. Phần sau trình bày phân tích chi tiết về các hình thức tấn công, gây mất an ninh đối với từng lớp trong IoT.

Lớp vật lý:

Hệ thống các thiết bị IoT được tích hợp nhiều bộ phận cảm biến để tiến hành thu thập thông tin theo yêu cầu, đồng thời sử dụng các phương tiện truyền thông khác nhau để nhằm gửi và nhận thông tin điều khiển từ các nút xử lý tập trung. Điều này làm nảy sinh ba vấn đề an ninh chính tại lớp này.

- Vấn đề đầu tiên là công suất của tín hiệu không dây. Do đặc trưng chủ yếu là các tín hiệu được truyền giữa các nút cảm biến của IoT sử dụng công nghệ không dây mà tín hiệu vô tuyến có nguy cơ bị tổn hại cao.

- Thứ hai, các nút cảm biến trong các thiết bị IoT có thể bị ngừng hoạt động hoặc bị truy cập trái phép bởi những kẻ tấn công. Các thiết bị IoT thường hoạt động cả hai môi trường trong nhà và ngoài trời, dẫn đến các cuộc tấn công vật lý trên các cảm biến có thể làm xáo trộn các thành phần phần cứng các của thiết bị IoT.

- Vấn đề thứ 3 này sinh từ chính bản chất vốn có của mô hình mạng đó là các thiết bị IoT có thể phải làm việc trong khi phải tiến hành di chuyển liên tục. Điều này gây khó khăn cho phương pháp nhận dạng tấn số vô tuyến, do khả năng lưu trữ, tiêu thụ điện năng, và khả năng tính toán rất hạn chế khiến chúng dễ bị mắc nhiều loại mối đe dọa và tấn công.

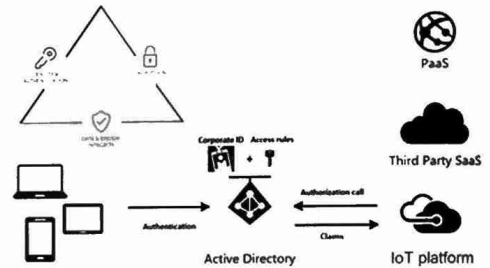
Lớp mạng:

Lớp mạng của IoT cũng dễ bị tấn công DoS (Man – in the Middle), kẻ thù cũng có thể bị tấn công bằng cách phân tích lưu lượng, nghe trộm và giám sát thụ động. Những cuộc tấn công có khả năng xảy ra cao bởi các cơ chế cho phép truy cập từ xa và trao đổi dữ liệu của thiết bị. Hơn nữa, tính không đồng nhất của các thành phần làm cho hệ thống mạng gặp khó khăn trong việc sử dụng các giao thức mạng hiện tại để thiết lập cơ chế bảo vệ hiệu quả. Nhằm bảo vệ lớp mạng thì cần có một giao thức vừa đảm bảo thích ứng chạy được trên nhiều chủng loại thiết bị vừa đảm bảo an ninh cho dữ liệu đã được định tuyến trên môi trường truyền.

Lớp ứng dụng:

Cho đến nay, IoT vẫn chưa có chính sách và tiêu chuẩn chung toàn cầu chi phối tương tác và sự phát triển của các ứng dụng, do đó có nhiều vấn đề liên quan đến bảo mật ứng dụng. Các ứng dụng khác nhau có cơ chế xác thực khác nhau, hơn nữa việc bảo vệ thông tin người sử dụng bên trong một tập hợp các ứng dụng được cài đặt trên rất nhiều thiết bị là một việc hết sức khó khăn. Một vấn đề khác

cần được xem xét khi thiết kế các ứng dụng trong IoT là cách người dùng khác nhau sẽ tương tác với các ứng dụng này, lượng dữ liệu của các người dùng có thể sẽ bị tiết lộ lẫn nhau. Người sử dụng phải có các công cụ để kiểm soát dữ liệu mà họ muốn tiết lộ và phải được chỉ rõ rằng dữ liệu đó có thể được sử dụng bởi ai, khi nào và tại đâu.



Hình 2: Xác thực và mã hóa dữ liệu

3. Giải pháp bảo mật theo từng lớp trong IoT

IoT đòi hỏi các biện pháp an ninh tại tất cả ba lớp: tại lớp vật lý để đảm bảo việc thu thập và truyền dữ liệu, tại tầng mạng cho việc định tuyến và truyền dẫn, và ở lớp ứng dụng để duy trì tính bảo mật và đảm bảo an toàn thông tin cho người sử dụng. Phần này sẽ đưa các biện pháp an ninh nhằm giải quyết các vấn đề bảo mật cụ thể, nhằm đặt mục tiêu an ninh cho hệ thống IoT.

3.1. Bảo mật lớp vật lý - Xác thực người dùng và mã hóa dữ liệu trên đường truyền

Để giúp các thiết bị tập trung sự chính xác trong quá trình thu và gửi dữ liệu, đã có nhiều biện pháp xác thực được đưa ra. Mục đích của những biện pháp này nhằm giúp các đối tượng đảm bảo việc dữ liệu nhận được là đúng, đồng thời đảm bảo việc

vận hành của thiết bị không bị truy cập và thay đổi từ những người dùng không được phép. Nổi bật lên trong những cơ chế xác thực là xác thực ID tại các nút cảm biến của IoT.

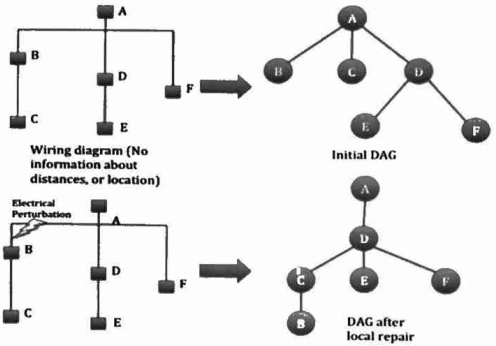
Đây là phương pháp bảo mật sử dụng một thuật toán mã hóa dựa trên cơ chế yêu cầu trả lời. Nó sử dụng các mật mã động được tạo bằng cách sử dụng một ma trận được chia sẻ trước giữa các bên giao tiếp. Các bên có thể tạo mật mã cách ngẫu nhiên sau đó phối hợp sử dụng các mật mã đó. Chính nhờ vào sự phối hợp này mà chìa khóa giải mã không thể bị chiếm đoạt được hết khi một nút mạng bị tấn công; do bản chất việc sử dụng mật mã được chuyển giao giữa hai bên. Tất cả các thông điệp được gửi bằng cách mã hóa chúng với chìa khóa phối hợp cùng với ID thiết bị và nhãn thời gian. Hai thiết bị giao tiếp bằng nhãn thời gian được chỉ ra trước đó, do vậy chúng có thể hủy bỏ phiên truyền thông dựa trên nhãn này. Mật mã phối hợp được thay đổi thường xuyên nên an ninh có thể được tối ưu hóa cho từng phiên kết nối IoT cụ thể. Tuy nhiên việc tạo mật mã trước khi chia sẻ cần phải được bảo vệ an toàn để có thể được áp dụng cho một số lượng lớn các thiết bị IoT.

Để giải bài toán xác thực trên thì phương pháp xác thực danh tính và điều khiển truy cập dựa trên năng lực (IACAC) đã được đề xuất cho IoT. IACAC ngăn chặn các cuộc tấn công bằng cách sử dụng một nhãn thời gian trong việc xác thực giữa các thiết bị. Nó hoạt động theo ba giai đoạn: đầu tiên một khóa bí mật được tạo ra dựa trên thuật toán Elliptical cong Cryptography-Diffie Hellman (ECCDH) [2], sau đó việc thiết lập danh tính được thực hiện một chiều, các giao thức xác thực lẫn nhau và cuối cùng là kiểm soát truy cập sẽ được thực hiện.

3.2. Bảo mật định tuyến IoT

Việc định tuyến cũng như an ninh trong định tuyến của IoT không thể bỏ qua tính suy hao của mạng và mức công suất tiêu thụ có thể rất thấp tại các nút mạng. Một trong những giải pháp định tuyến đáp ứng được những yêu cầu trên đó là định tuyến với RPL (Routing for Low power and Lossy Networks). RPL dựa trên ý tưởng định tuyến phải thích ứng với các yêu cầu của riêng của người dùng, cũng như đối với từng mục đích của ứng dụng. RPL xây dựng một bản đồ đích đến hướng kết nối dạng xoắn (DODAG), nhằm xác định một DODAG ID cho mỗi thiết bị gốc, từ đó tính toán suy hao trên các liên kết, thuộc tính và trạng thái của từng nút để từ đó phân tích đường đi cụ thể cho từng mục đích định tuyến khác nhau [3].

RPL tạo ra một phương thức bảo vệ an toàn cho các bản tin điều khiển định tuyến khác nhau dựa trên ba chế độ bảo mật cơ bản [4]. Hình 4 minh họa định dạng của một bản tin kiểm soát RPL, nó chứa một trường bảo mật nằm sau trường tiêu đề 4-byte của gói tin ICMP. Bit bậc cao của bản tin cho phép sử dụng hoặc không sử dụng RPL cho mục đích bảo mật. Các thông tin trong trường bảo mật chỉ ra mức

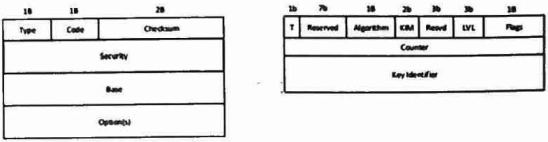


Hình 3: Ví dụ về topo định tuyến RPL

độ an ninh và các thuật toán mật mã sử dụng cho các bản tin được trao đổi. RPL có thể sử dụng thuật toán AES/CCM với các chìa khóa 128-bit cho MAC để hỗ trợ tính toàn vẹn của dữ liệu hay SHA-256 để mã hóa cho các bản tin hỗ trợ cho việc xác thực và bảo đảm toàn vẹn dữ liệu. Các mức bảo mật cho phép người sử dụng chọn được các cấp độ an ninh từ thấp tới cao, đáp ứng nhu cầu rộng rãi hơn. Ngoài ra để tăng cường tính toàn vẹn dữ liệu, RPL còn cung cung xác thực với MAC-32 và MAC-64 cũng như kí hiệu RSA-3072 bit.

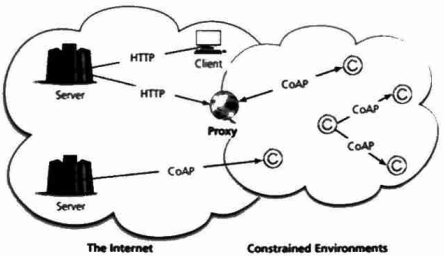
3.3. Bảo mật trong lớp ứng dụng

Trong thực tế, các ứng dụng trong IoT có thể gặp phải hai lỗ hổng an ninh lớn nhất thông qua việc chuyển quyền sử dụng và chuyển từ một chủ sở hữu này qua một chủ sở hữu mới khác, việc thiết lập ủy quyền cần được thống nhất giữa hai chủ sở hữu, nhằm tạo một quá trình chuyển đổi trơn tru của các thiết bị IoT liên quan đến kiểm soát và cho phép truy cập. Sự tin tưởng này được thành lập bởi hai cơ chế: chìa khóa và thông báo, cung cấp bởi giao thức CoAP tại lớp ứng dụng trong mô hình IoT cơ bản.



Hình 4 : Cấu trúc trường bảo mật trong RPL

Bất kỳ một tài khoản mới nào được tạo ra sẽ được gán một mã do một hệ thống ủy quyền tạo ra. Khóa này được tạo bởi các máy chủ điều khiển. Các mã thông báo



Hình 5: Truyền thông lớp ứng dụng IoT với bảo mật CoAP

được tạo ra bởi nhà sản xuất, hoặc chủ sở hữu hiện tại, và mã thông báo này được kết hợp với việc xác minh trên từng thiết bị. Cơ chế này đảm bảo việc thay đổi quyền truy cập bằng cách chủ sở hữu mới sẽ gán lại các mã và xóa bỏ đi những mã của chủ sở hữu cũ. Những thẻ trên cũng được thay đổi bởi các chủ sở hữu với điều kiện là mã thông báo cũ phải được cung cấp, để thay thế các quyền sử dụng và kiểm soát truy cập của chủ sở hữu trước đó trước. Để tăng tính bảo mật, người dùng có thể yêu cầu trả lời câu hỏi mỗi khi muốn truy cập lên thiết bị của mình. Phương pháp này được tiến hành cụ thể bằng cách mỗi khi có một sự truy cập bất kì lên một ứng dụng đã được chủ sở hữu định ra trước đó, ngoài việc phải cung cấp mật khẩu chính xác thì người muốn sử dụng phải tiến hành trải qua một quá trình bảo mật nhiều bước: trả lời câu hỏi bí mật, cung cấp mã số qua tin nhắn nhận được từ trung tâm xử lý... Hai phương pháp trên đáp ứng yêu cầu an ninh trong lớp ứng dụng của IoT, giúp giữ an toàn trước sự xâm nhập trái phép và bảo đảm an toàn thông tin cho người dùng.

5. Kết luận

Khái niệm IoT ngày càng xuất hiện nhiều hơn và đã được triển khai tại một số nơi trên thế giới, nơi mạng lưới thiết bị cảm biến đang được kết nối với nhau thông qua Internet. Bên cạnh sự có mặt của một số lượng lớn thiết bị với đủ kích cỡ, hình dáng, chức năng, công suất được duy trì trên mạng thì vấn đề an ninh trở nên quan trọng và cấp bách hơn bao giờ hết, nhằm đảm bảo an toàn cho thông tin khách hàng cũng như ngăn chặn việc truy cập điều khiển trái phép thiết bị. Với phương pháp bảo mật dựa trên mô hình kiến trúc của IoT, nội dung bài viết giới thiệu giải pháp bảo mật trên từng lớp, nhằm nâng cao tối đa hiệu quả an ninh và tiện lợi cho cả nhà sản xuất cũng như người sử dụng. Bài viết mong có thể mang đến một đóng góp có ý nghĩa cho cộng đồng nghiên cứu, cũng như góp phần phát triển các giải pháp mới để giải quyết an ninh trong bối cảnh IoT hiện tại.

Tài liệu tham khảo:

1. ALA AL-FUQAHA, "Internet of Things: A Survey on Enabling Technologies, Protocols and Applications", Communications Surveys & Tutorials, 2015.

2. RWAN MAHMOUH ET AL., "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures", The 10th International Conference for Internet Technology and Secured Transactions, 2015.

3. "RPL: The IP routing protocol designed for low power and lossy network", IPSO Alliance, 2011.

4. JORGE GRANJAL ET AL., "Security for the Internet of Things: A Servey of Exiting Protocols and Open Research issues", IEEE Communications Surveys & Tutorials, 2015.