GIÁM SÁT AN TOÀN MẠNG IOT

Hoàng Đăng Hải
Học viện Công nghệ Bưu chính Viễn thông
Email: haihd@ptit.edu.vn

Tóm tắt: An toàn mạng IoT (Internet of Things) khác với an toàn mạng truyền thống do những đặc thù của mạng IoT. Những mô hình, cơ chế, kỹ thuật an toàn mạng đã phát triển cho mạng truyền thống không thể áp dụng trực tiếp cho mạng IoT, đòi hỏi phải có sự thay đổi cho phù hợp. Cho tới nay, một số vấn đề trong hệ thống giám sát an toàn mạng vẫn chưa được xem xét cụ thể trong các công trình nghiên cứu cũng như trong thực tế, điển hình như kiến trúc phân lớp, tính toán kích cỡ hệ thống giám sát, lựa chọn đặc trưng sự kiện. Bài báo này đề xuất một mô hình kiến trúc hệ thống giám sát an toàn mạng IoT phù hợp với việc phân chia hai lớp Fog và Cloud của mạng IoT. Ngoài ra, bài báo đề xuất cách thức tính toán phù hợp thực tế cho thiết kế hệ thống giám sát an toàn mạng IoT, cụ thể cho kích cỡ bộ đệm xử lý sự kiện, dung lượng lưu trữ sự kiện, lựa chọn đặc trưng của sự kiện. Bài đưa ra một số ví dụ tính toán cụ thể minh chứng cho tính khả thi trong thực tiễn.

Từ khóa: An toàn mạng, mạng IoT, giám sát an toàn mạng, kiến trúc mạng giám sát.

I. MỞ ĐẦU

Internet vạn vật (Internet of Things) đang được phát triển rất mạnh trong một vài năm qua và được coi là động lực cho thời kỳ phát triển công nghiệp mới. Theo các thống kê của IDC [1] và Gartner [2], đầu tư cho IoT tăng từ 647 tỉ USD năm 2017 lên 772,5 tỉ USD năm 2018 (tăng 15%); thị trường IoT tăng từ 157 tỉ USD năm 2016 lên tới 457 tỉ USD năm 2020 (tăng 28,5%); số thiết bị IoT kết nối tăng từ 8,4 tỉ năm 2017 lên tới 20,8 tỉ năm 2020 (tăng 34%). IoT được cho là sẽ tạo ra nền tảng hạ tầng mạng cho mọi thiết bị và hoạt động của con người. Bảo đảm an toàn mạng IoT đã trở thành một vấn đề quan trọng và được quan tâm nhiều trong thời gian gần đây.

Giám sát an toàn mạng IoT là một thách thức lớn trong bảo đảm an toàn mạng IoT. Giám sát an toàn mạng nói chung là quá trình theo dõi, kiểm tra nhằm bảo đảm mạng hoạt động theo đúng chức năng đã thiết kế, phục vụ đúng đối tượng một cách tin cậy, chính xác, đạt hiệu năng mong muốn [3]. Trong quá trình đó, hệ thống giám sát mạng phát hiện các nguy cơ sự cố, tấn công mạng, đưa ra cảnh báo phục vụ cho việc xử lý, ngăn chặn tấn công, nâng cao chất lượng hoạt động. Các công nghệ, kỹ thuật giám sát an toàn mạng đã phát triển song hành với sự phát triển mạng máy tính và Internet qua các thời kỳ từ các hệ thống giám sát mạng đơn lẻ [4] cho đến các hệ thống giám sát diện rộng [5], mạng tùy biến và điện toán đám mây [6, 7]. Tuy nhiên, mạng IoT không chỉ gặp những vấn đề an toàn thông tin đã có trong Internet và các mạng truyền thống, mà còn đối mặt với nhiều thách thức mới [8].

Tác giả liên hệ: Hoàng Đăng Hải
Email: haihd@ptit.edu.vn
Đến tòa soạn: 03/2018, chỉnh sửa: 04/2018, chấp nhận đăng: 05/2018

Do tài nguyên và năng lực xử lý thường bị hạn chế, hầu hết các thiết bị IoT thường có khả năng bảo đảm an toàn kém. Thậm chí, nhiều thiết bị IoT bị bỏ qua tính năng an toàn thông tin trong khi chúng thường xuyên đặt trong các ứng dụng hoạt động liên tục 24/7. Do đó, các thiết bị IoT trở thành mục tiêu hấp dẫn cho tin tặc. Trong khi đó, các cơ chế giám sát và bảo vệ đã được phát triển cho các mạng truyền thống không thể áp dụng trực tiếp cho mạng IoT được do những đặc điểm riêng của mạng IoT. Ví dụ, chúng ta đã có khá nhiều cơ chế, kỹ thuật bảo vệ khá phức tạp cho các thiết bị giàu tài nguyên và hiệu năng cao trong mạng tuyền thống. Ngược lại, ta chỉ có thể áp dụng các cơ chế, kỹ thuật bảo vệ hạng nhẹ (lightweight) cho mạng IoT và phải cân bằng giữa yêu cầu an toàn và vấn đề tài nguyên hạn chế/năng lực xử lý có hạn. Mặt khác, môi trường mạng IoT khá đa dạng về công nghệ, loại thiết bị và ứng dụng. Do vậy, các tấn công mạng IoT cũng rất đa dạng và khó phát hiện hơn. Có tới 70% thiết bị IoT sử dụng các dịch vụ mạng không có sự bảo vệ. Tấn công của mã độc Mirai Botnet tháng 10/2016 đã tác động đến hoạt động của hơn 400,000 thiết bị IoT kết nối trên mạng [9].

Bảo đảm an toàn mạng IoT nói chung và cụ thể là giám sát an toàn mạng IoT đã là chủ đề của một số nghiên cứu mới đây, ví dụ trong [10-18]. Các bài báo nêu trên đã hệ thống hóa các vấn đề thách thức trong bảo đảm an toàn mạng IoT và chỉ ra các giải pháp tiềm năng. Kiến trúc hệ thống an toàn mạng liên quan đến các vấn đề như các loại tấn công [10, 13], ứng dụng [11, 15], kiểm soát [12, 13] đã được đề cập, phân tích và đưa ra giải pháp. Đặc biệt, các bài báo [14, 16, 17] đã tóm tắt một cách khái quát các kiến trúc, công nghệ, kỹ thuật liên quan đã được nghiên cứu, phát triển trong thời gian qua. Một hệ thống giám sát an toàn mạng IoT cỡ nhỏ cũng đã được nghiên cứu và đề xuất trong [18]. Trong [19], các tác giả cũng đã đưa ra một mô hình hệ thống theo dõi, giám sát và phát hiện bất thường cho mạng IoT. Tuy nhiên, có thể thấy, giám sát và phát hiện tấn công mạng IoT vẫn chưa được đề cập một cách hệ thống. Một số vấn đề đặc thù của mạng IoT, điển hình như khả năng lưu trữ và xử lý hạn chế, tính đa dạng của thiết bị, phạm vi và tính phức tạp của hệ thống, vẫn chưa được xem xét. Như đã đề cập trong [19], khái niệm về lớp "sương mù" (Fog) đã được đưa ra. Một Fog được hiểu là kiến trúc mạng phủ quanh các thiết bị IoT có kết nối, nhằm thu

thập và xử lý các sự kiện từ các thiết bị IoT gần với nguồn dữ liệu hơn là thu thập và xử lý tại trung tâm giám sát. Đặc điểm này của mạng IoT vẫn chưa được đề cập đến trong kiến trúc một hệ thống giám sát hiện có tới nay. Việc lựa chọn kiến trúc hệ thống giám sát phù hợp với mạng IoT thế nào vẫn còn là vấn đề chưa được đề cập. Ngoài ra, một số vấn đề vẫn chưa được làm rõ hoặc xem xét cụ thể, như: tính toán kích thước bộ đệm xử lý sự kiện, tính toán dung lượng lưu trữ sự kiện, lựa chọn các đặc trưng trong sự kiện, lựa chọn phương pháp phân tích sự kiện, phát hiện sự cố an toàn mạng.

Bài báo này đề xuất một mô hình kiến trúc hệ thống giám sát an toàn mạng IoT phù hợp với việc phân chia hai lớp Fog và Cloud của mạng IoT. Để tính kích cỡ hệ thống giám sát, bài đề xuất một phương pháp tính toán khả thi cho bộ nhớ đệm xử lý và dung lượng lưu trữ sự kiện trong các phân hệ giám sát. Ngoài ra, bài báo phân tích khả năng lựa chọn các đặc trưng lưu lượng mạng IoT và phương pháp phân tích, phát hiện bất thường theo hàm Entropy. Phần còn lại của bài báo như sau. Trong phần II, bài trình bày về vấn đề giám sát an toàn mạng, đặc trưng của mạng IoT và các yêu cầu cơ bản về hệ thống giám sát an toàn mạng IoT. Trong phần III, bài đề xuất một kiến trúc hệ thống giám sát với hai phân cấp: Fog và Cloud, đồng thời trình bày và đưa ra một số kết quả tính toán cụ thể cho kiến trúc giám sát. Phần IV là kết luận của bài.

II. VẤN ĐỀ GIÁM SÁT AN TOÀN MẠNG IOT

A. Giám sát an toàn mạng

Chức năng cơ bản của một hệ thống giám sát an toàn mạng là thu thập dữ liệu về các sự kiện, xử lý phân tích, phát hiện và đưa ra cảnh báo về nguy cơ sự cố, các hành vi tấn công mạng.

Qua khảo sát về các hệ thống giám sát an toàn mạng, có thể hệ thống hóa theo bốn giai đoạn phát triển như sau:

- Giai đoạn 1: Giám sát và cảnh báo sự cố được coi là một lĩnh vực trong hệ thống quản lý mạng (Network Management System) nhằm giám sát truy nhập, theo dõi hoạt động và cảnh báo, khôi phục sự cố [3,4]. Hệ thống sử dụng chủ yếu các công cụ phần mềm đơn lẻ như phát hiện xâm nhập trái phép, kiểm soát truy nhập, phát hiện tấn công,… Nhiều công cụ phần mềm và thành phần giám sát đơn lẻ được phát triển mạnh, ví dụ các công cụ Nmap, Nagios,… Hạn chế của các hệ thống này là còn mang tính thụ động, khả năng kiểm soát thông tin thấp.

- Giai đoạn 2: Phát triển các hệ thống có tích hợp các công cụ, kỹ thuật, phần mềm đơn lẻ vào một hệ thống chung. Đặc trưng là sự phát triển đi sâu vào các công nghệ mới áp dụng cho phát hiện và ngăn chặn xâm nhập như IDS, IPS, công nghệ thu thập thông tin và bẫy nhử như Honeypots, Honeynet, công nghệ phát hiện điểm yếu và mã độc,…[3]. Tuy nhiên, việc kết hợp nhiều công cụ đơn lẻ vào một hệ thống còn gặp nhiều khó khăn do tính phức tạp cao, khả năng tương thích kém, hạn chế về khả năng linh hoạt, mềm dẻo, mở rộng,…

- Giai đoạn 3: Đặc trưng của giai đoạn này là sự phát triển của các hệ thống quản lý tập trung. Hệ thống quản lý tập trung là một bước tiến mới trong lĩnh vực giám sát an toàn mạng [5]. Nhiều hệ thống lớn được xây dựng. Các hệ thống quản lý tập trung có những ưu điểm nổi bật so với các kiến trúc của giai đoạn trước về khả năng tích hợp các công nghệ vào một hệ thống thống nhất. Tuy nhiên, các hệ thống này có những khó khăn, thách thức về mặt kỹ thuật như: sự thay đổi nhanh về công nghệ đòi hỏi phải có tính thích ứng và cập nhật kịp thời. Hệ thống thường lớn, có sự tích hợp hỗn hợp công nghệ nên khó kiểm soát, khó liên kết, khó mở rộng; năng lực xử lý thường bị hạn chế; chi phí thường rất cao.

- Giai đoạn 4: Đặc trưng là sự bùng nổ của dữ liệu lớn, điện toán đám mây, tốc độ phát triển nhanh của thiết bị di động, Internet vạn vật [6, 7, 13, 16]. Để khắc phục những hạn chế về tính phức tạp, tăng hiệu năng hệ thống, các hệ thống giám sát ATTT đặc thù đã ra đời phục vụ cho các kiến trúc mạng cụ thể.

Kiến trúc, công nghệ, kỹ thuật cho các hệ thống giám sát an toàn mạng đặc thù vẫn đang là trọng tâm của nhiều công trình nghiên cứu trên thế giới, điển hình như một số phát minh, sáng chế mới tại Mỹ.

Chủ đề nghiên cứu về hệ thống giám sát khá đa dạng. Tuy nhiên, có thể hệ thống hóa theo các nhóm:

- Kiến trúc hệ thống: bao gồm các vấn đề về mô hình kiến trúc, các phân hệ trong hệ thống, cơ sở dữ liệu, phân cấp quản trị, kiến trúc xử lý thời gian thực, kiến trúc hệ thu thập dữ liệu,…

- Thu thập dữ liệu: bao gồm các vấn đề định dạng dữ liệu, công nghệ agent, phân loại dữ liệu, lọc và chuyển đổi dữ liệu,…

- Phân tích, xử lý, phát hiện: bao gồm các vấn đề về phân tích dấu hiệu tấn công, nguy cơ sự cố, phát hiện bất thường trên mạng, vấn đề phân tích dữ liệu lớn, xử lý thời gian thực,…

- Lưu trữ, thống kê, cảnh báo, hiển thị: bao gồm các vấn đề về ghi vết, lưu trữ an toàn, các phương pháp thống kê và hiển thị cảnh báo,…

Sự phát triển bùng nổ của mạng IoT đang đặt ra nhiều vấn đề thách thức mới như đã được phân tích chi tiết trong các tài liệu [8-17].

B. Những đặc trưng của mạng IoT

Xét về bản chất, mạng IoT thực tế là sự mở rộng của Internet. An toàn mạng trong môi trường IoT cũng có thể coi như tương tự trong các mạng khác. Tuy nhiên, môi trường mạng IoT có những đặc trưng điển hình như sau:

- Các thiết bị IoT hầu hết có giá thành khá thấp, được sản xuất với số lượng lớn. Các tính năng an toàn mạng thường được bỏ qua để giảm thiểu chi phí.

- Khá nhiều thiết bị IoT có tính năng thông minh, có khả năng kết nối đa dạng.

- Các kết nối của thiết bị IoT nhìn chung có băng thông hạn chế. Tốc độ kết nối không cao. Do vậy, khó lòng áp dụng các giao thức truyền thống thường đòi hỏi về tốc độ và băng thông lớn.

- Các thiết bị IoT thường có tài nguyên (năng lực CPU, bộ nhớ, băng thông kết nối) hạn chế. Do vậy, chúng thường sử dụng các hệ điều hành cỡ siêu nhỏ.

Khả năng áp dụng các cơ chế bảo vệ bị hạn chế, đòi hỏi các giải pháp hạng nhẹ (lightweight). Định dạng dữ liệu cũng bị hạn chế.

- Năng lực xử lý của các thiết bị IoT thường thấp hơn nhiều so với các máy tính phổ biến khác. Ngoài ra, nguồn năng lượng đa phần là dùng pin. Do vậy, cần có các giải pháp tiết kiệm nguồn pin.

- Các thiết bị IoT khá đa dạng, sử dụng nhiều loại công nghệ mạng khác nhau như WiFi, ZigBee, 3G/4G/5G,…

- Ứng dụng của IoT khá đa dạng, có các yêu cầu về mức độ an toàn khác nhau.

C. Yêu cầu đối với hệ thống giám sát an toàn mạng IoT

Các yêu cầu cơ bản đối với một hệ thống giám sát an toàn mạng bao gồm:

- Thu thập dữ liệu về các sự kiện an toàn mạng: Cần thu thập những dữ liệu đặc trưng cho các sự kiện an toàn mạng. Lượng dữ liệu và các thuộc tính lưu lượng mạng cần vừa đủ cho phân tích, phát hiện sự cố. Một lượng dữ liệu lớn với nhiều thuộc tính có thể cho kết quả phát hiện chính xác, song chưa chắc đã hiệu quả do chi phí tính toán cao dẫn đến tốc độ phát hiện chậm, thậm chí khiến cho hệ thống quá tải. Cho tới nay, một lượng dữ liệu và số thuộc tính lưu lượng mạng vừa đủ vẫn còn là một vấn đề cần xem xét trong hệ thống giám sát.

- Bộ đệm xử lý sự kiện: Là vùng nhớ cần cấp phát trong quá trình phân tích, xử lý sự kiện an toàn mạng. Các hệ thống giám sát an toàn mạng hiện có chưa thấy đề cập đến yêu cầu này.

- Dung lượng lưu trữ sự kiện: Trong và sau quá trình phân tích, các sự kiện được lưu giữ tại hệ thống giám sát. Tuy nhiên, chưa có nghiên cứu nào trình bày cụ thể cách tính toán dung lượng lưu trữ sự kiện này.

- Số lượng dữ liệu đặc trưng (số thuộc tính của lưu lượng mạng): Một số nghiên cứu, ví dụ [18-21] đã trình bày về việc chọn dữ liệu đặc trưng này. Sự lựa chọn phụ thuộc nhiều vào phương pháp phân tích, vị trí giám sát và mức độ yêu cầu giám sát.

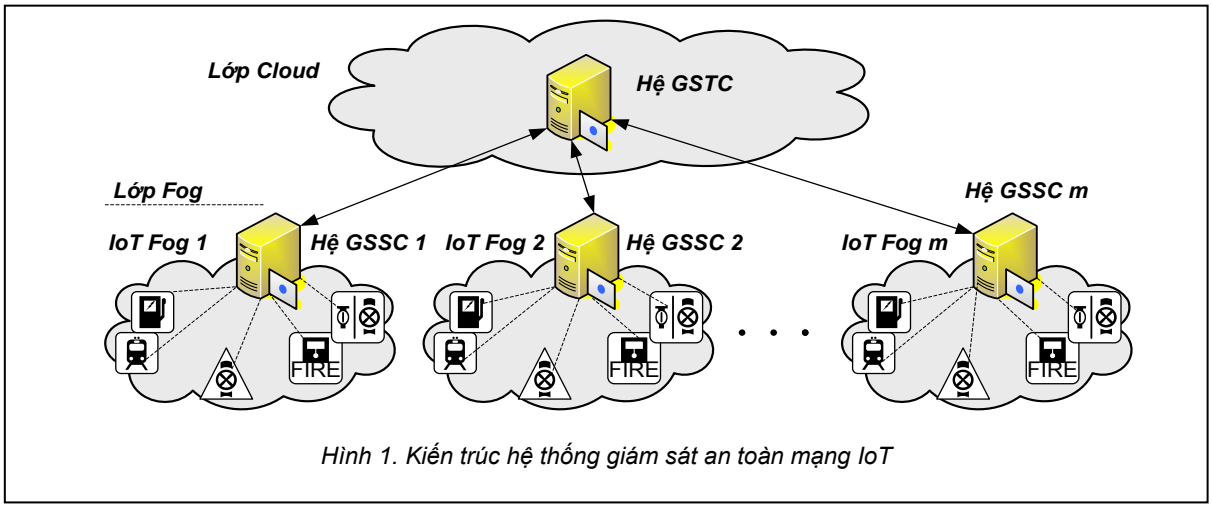
- Phương pháp phân tích, phát hiện sự cố an toàn mạng: Cho đến nay đã có nhiều phương pháp được đề xuất (ví dụ [18-21]). Mỗi phương pháp đều có những ưu nhược điểm riêng. Việc lựa chọn phương pháp thường phụ thuộc vào phạm vi, quy mô và mức độ yêu cầu giám sát của hệ thống.

- Kiến trúc hệ thống giám sát: Như đã nêu ở phần trên, hệ thống giám sát có thể có kiến trúc phân tán hoặc tập trung, hoặc kết hợp cả hai. Việc lựa chọn kiến trúc hệ thống phụ thuộc vào các ứng dụng giám sát an toàn mạng đặc thù và yêu cầu giám sát cụ thể.

III. HỆ THỐNG GIÁM SÁT AN TOÀN MẠNG IOT

A. Mô hình kiến trúc hệ thống

Kiến trúc hệ thống giám sát an toàn mạng IoT được đề xuất theo mô hình kết hợp phân tán và tập trung, phân tán tại lớp Fog gần sát với các thiết bị IoT và tập trung tại trung tâm giám sát (xem hình 1). Mô hình này phù hợp với thế hệ thứ 4 của các hệ thống giám sát và đáp ứng nhu cầu hai phân lớp chính của mạng IoT là phân lớp mạng Fog và phân lớp Cloud.



Hình 1. Kiến trúc hệ thống giám sát an toàn mạng IoT

Giải pháp thu thập dữ liệu về các sự kiện an toàn mạng có thể được thực hiện theo hai cách: thu thập trực tiếp từ các thiết bị IoT (điển hình là qua các tệp log), thu thập dữ liệu trao đổi trên mạng Fog (điển hình là qua giao diện hệ giám sát Fog). Thu thập dữ liệu trên mạng có ưu điểm trong trường hợp không thể thu được trực tiếp dữ liệu từ các thiết bị. Trung tâm giám sát đặt ở lớp Cloud, ví dụ trong miền Private Cloud của một nhà cung cấp dịch vụ mạng. Để bảo đảm an toàn, có thể đặt các thiết bị bảo vệ như tường lửa (Firewall), hệ thống phát hiện và chống xâm nhập (Intrusion Detection and Prevention System – IDPS) và tạo thành một miền phân cách bảo vệ (ví dụ Demilitarized Zone - DMZ). Ngoài ra, có thể thiết lập mạng riêng ảo (Virtual Private Networks – VPN) hoặc sử dụng kênh truyền có bảo mật giữa các hệ giám sát ở lớp Fog và hệ thống trung tâm. Trong khuôn khổ bài báo, chúng tôi không trình bày sâu hơn về những chi tiết này.

Dữ liệu sự kiện thu thập từ các thiết bị IoT được lưu giữ ở hai cấp phục vụ cho phân tích, xử lý. Cấp 1 là hệ giám sát sơ cấp (Hệ GSSC) ở lớp Fog và cấp 2 là hệ giám sát thứ cấp (Hệ GSTC) ở hệ thống trung tâm.

Các tham số được quan tâm nhất ở hệ giám sát các cấp là: dung lượng lưu trữ sự kiện, bộ đệm xử lý sự kiện, kích cỡ sự kiện, số lượng đặc trưng cần thiết cho

phân tích và phát hiện sự cố an toàn mạng, năng lực phân tích và phát hiện sự cố của hệ giám sát. Trong phần sau đây, bài báo trình bày cụ thể hơn về các tham số này.

B. Dung lượng lưu giữ sự kiện

Để xác định dung lượng lưu trữ sự kiện, cần xác định số lượng thiết bị IoT cần giám sát và tần suất sự kiện của mỗi thiết bị IoT. Tần suất sự kiện thường được mô tả theo số sự kiện trên một giây (Events per Second – EPS). Về mặt lý thuyết, EPS có thể nhận giá trị từ Min đến Max (Peak EPS). Mặt khác, EPS phụ thuộc vào kiểu thiết bị IoT, vị trí của chúng trên mạng, mức độ cần bảo vệ. Tuy nhiên, giá trị EPS tối đa (Peak EPS) thường dùng để tính toán cho hệ giám sát. Một thiết bị IoT có thể có tần suất sự kiện từ 0,5 đến 10 EPS, tùy theo vị trí thiết bị trên mạng Fog và tính chất quan trọng của thiết bị cần giám sát. Điều đó nghĩa là Peak EPS chọn để tính toán là 10 sự kiện / giây.

Dung lượng tối thiểu để lưu trữ sự kiện trên một giây tại hệ giám sát sơ cấp ở lớp Fog được tính như sau:

$$B = n\ E\ L \quad (1)$$

Với B là dung lượng tối thiểu tính theo Bytes, n là số thiết bị IoT cần giám sát, E là tần suất EPS tối đa của mỗi thiết bị IoT, L là số bytes của mỗi sự kiện.

Giả thiết hệ GSSC ở một cụm Fog cần giám sát 500 thiết bị IoT ($n = 500$), kích thước mỗi sự kiện là $L=200$ Bytes, tần suất sự kiện của mỗi thiết bị IoT là $E=10$ EPS, ta tính được tổng số sự kiện thu được tại mỗi hệ GSSC là:

$$S = 500\ x\ 10\ EPS = 5{,}000\ EPS \quad (2)$$

Dung lượng lưu trữ tối thiểu cho 5,000 sự kiện trong một giây là:

$$B_1 = S\ x\ 200\ Bytes = 1{,}0\ MBytes \quad (3)$$

Dung lượng đĩa cứng lưu trữ tối thiểu cho mỗi hệ GSSC trong một ngày là:

$$B_2 = B_1\ x\ 24\ x\ 60\ x\ 60 = 86{,}4\ GBytes \quad (4)$$

Hệ thống giám sát thường được thiết kế cho lưu trữ nóng (Warm) trong thời gian 3 ngày, lưu trữ nguội (Cold) trong thời gian 7 ngày và lưu trữ nén (compressed) trong thời gian 6 tháng.

Dung lượng đĩa cứng lưu trữ nóng tối thiểu cho một hệ GSSC là:

$$B_3 = B_2\ x\ 3\ ngày = 259{,}2\ GBytes \quad (5)$$

Dung lượng đĩa cứng lưu trữ nguội tối thiểu cho một hệ GSSC là:

$$B_4 = B_2\ x\ 7\ ngày = 604{,}8\ GBytes \quad (6)$$

Với tỉ lệ nén 10:1, dung lượng đĩa cứng lưu trữ nén tối thiểu cho một hệ GSSC là:

$$B_5 = B_2\ x\ 180\ ngày = 15{,}5\ TBytes \quad (7)$$

Với m là số cụm Fog (số hệ GSSC) và giả thiết số sự kiện của mỗi cụm như nhau, ta tính được dung lượng tối thiểu để lưu trữ sự kiện trên một giây tại hệ giám sát thứ cấp ở trung tâm như sau:

$$C = m\ B_1 \quad (8)$$

Giả sử có 03 hệ GSSC trong hệ thống giám sát an toàn mạng IoT. Dung lượng đĩa cứng lưu trữ tối thiểu cho hệ GSTC tại trung tâm trong một ngày là:

$$C_2 = 3\ x\ B_1\ x\ 24\ x\ 60\ x\ 60 = 259{,}2\ GBytes \quad (9)$$

Dung lượng đĩa cứng lưu trữ nóng tối thiểu cho một hệ GSTC tại trung tâm là:

$$C_3 = C_2\ x\ 3\ ngày = 777{,}6\ GBytes \quad (10)$$

Dung lượng đĩa cứng lưu trữ nguội tối thiểu cho một hệ GSTC tại trung tâm là:

$$C_4 = C_2\ x\ 7\ ngày = 1{,}8\ Tbytes \quad (11)$$

Với tỉ lệ nén 10:1, dung lượng đĩa cứng lưu trữ nén tối thiểu cho một hệ GSTC tại trung tâm là:

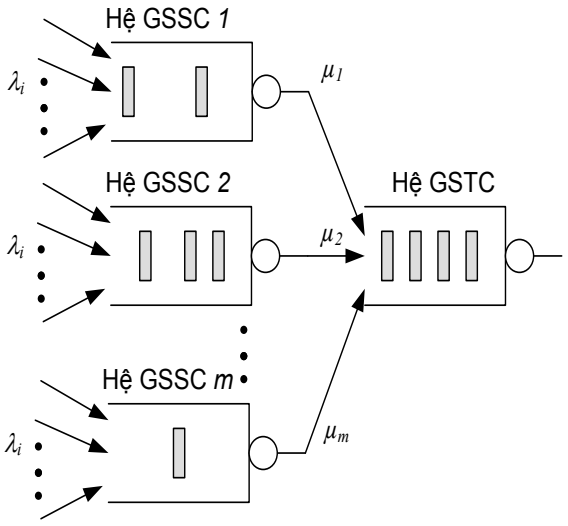
$$C_5 = C_2\ x\ 180\ ngày = 46{,}7\ TBytes \quad (12)$$

Trong thực tế, có thể chỉ cần lưu trữ các sự kiện tối thiểu trong một ngày tại mỗi hệ GSSC, nghĩa là với dung lượng đĩa cứng lưu giữ B_2. Lưu trữ nóng, lưu trữ nguội và lưu trữ nén chỉ cần thực hiện tại hệ thống trung tâm.

Ngoài ra, để bảo đảm lưu trữ an toàn, dung lượng đĩa cứng lưu trữ B_2, C_2 cần được dự phòng nóng 1+1. Các dung lượng đĩa cứng lưu trữ khác cũng có thể được dự phòng nóng tùy theo nhu cầu và tính cần thiết.

C. Kích thước bộ đệm xử lý sự kiện

Bộ đệm xử lý sự kiện trong mỗi hệ GSSC và hệ GSTC có thể được tính như sau. Ta có thể giả định quá trình sinh sự kiện an toàn mạng là ngẫu nhiên theo phân bố Poisson. Giả thiết này thường được áp dụng cho mạng máy tính và sử dụng với mô hình Markov để phân tích hiệu năng mạng. Có thể mô hình hóa hệ GSSC và hệ GSTC với lý thuyết hàng chờ (Queueing Theory) như trên hình 2.



Hình 2. Mô hình hàng chờ cho hệ thống giám sát an toàn mạng IoT

Gọi số sự kiện trung bình trong hàng chờ của từng hệ GSSC là W_i, thời gian xử lý trung bình cho mỗi sự kiện trong mỗi hệ GSSC là T_{pi}. Áp dụng định luật Little, ta tính được kích thước bộ đệm xử lý sự kiện theo công thức sau.

$$W_i = \lambda T_{pi} \quad (13)$$

Với λ là tổng tần suất các sự kiện của các tiến trình con λ_i đến mỗi hệ GSSC, nghĩa là:

$$\lambda = \sum_{i=1}^{n} \lambda_i \quad (14)$$

Trong thực tế, để đơn giản hóa việc tính toán, ta có thể giả thiết tần suất sự kiện của mỗi thiết bị IoT là như nhau, nghĩa là $\lambda_1 = \lambda_2 = \ldots \lambda_n$. Theo dữ kiện đã nêu ở phần trên, mỗi hệ GSSC ở một cụm Fog giám sát 500 thiết bị IoT ($n = 500$), tần suất sự kiện của mỗi thiết bị IoT là *10* EPS, ta tính được tổng tần suất sự kiện tại mỗi hệ GSSC là:

$$\lambda = n\ \lambda_1 = 500 \text{ x } 10 \text{ EPS} = 5{,}000 \text{ EPS} \quad (15)$$

Nếu dùng một bộ xử lý Intel Xeon 2 core tốc độ 2.5 GHz cho một hệ GSSC, khả năng xử lý có thể đạt được 20 EPS. Thời gian xử lý cho mỗi sự kiện trong hệ GSSC sẽ là:

$$T_{pi} = 1 / 20 = 0.05 \text{ s} \quad (16)$$

Với kích thước mỗi sự kiện là 200 Bytes, kích thước bộ đệm xử lý sự kiện của mỗi hệ GSSC tối thiểu là:

$$W_i = \lambda T_{pi} = 50 \text{ MBytes} \quad (17)$$

Theo cách tương tự, ta tính được tổng tần suất sự kiện đến hệ GSTC với giả thiết có 03 hệ GSSC là:

$$\mu = m\ \lambda = 3 \text{ x } 5000 \text{ EPS} = 15{,}000 \text{ EPS} \quad (18)$$

Kích thước bộ đệm xử lý sự kiện W tối thiểu của hệ GSTC là:

$$W = \mu T_p = 150 \text{ MBytes} \quad (19)$$

D. Số lượng đặc trưng cần cho phân tích, phát hiện sự cố an toàn mạng

Theo các công trình nghiên cứu [18, 19], các thuộc tính lưu lượng mạng có thể phục vụ cho việc phân tích và phát hiện sự cố an toàn mạng. Số lượng thuộc tính có thể khá nhiều, song nếu chọn quá nhiều thuộc tính, độ phức tạp tính toán sẽ rất cao. Do vậy cần chọn một số lượng thuộc tính điển hình nhất (nghĩa là đặc trưng) của lưu lượng mạng phù hợp cho hệ thống giám sát. Bảng I là ví dụ về một số thuộc tính điển hình.

Bảng I: Các thuộc tính lưu lượng mạng điển hình

Thuộc tính	Ý nghĩa
# Byte	Số byte trong luồng tin
# Packet	Số gói tin trong luồng tin
SRC IP ADR	Địa chỉ IP nguồn
DST IP ADR	Địa chỉ IP đích
SRC port	Cổng nguồn
DST port	Cổng đích
Protocol	Giao thức
Flags	Bit cờ của gói tin
Count-dest	Số luồng tin đến 1 đích duy nhất từ cùng một nguồn
Count-src	Số luồng tin từ 1 nguồn đến cùng một đích
Count-serv-src	Số luồng tin từ 1 IP đến cùng cổng đích trong T giây
Count-serv-dest	Số luồng tin đến 1 IP từ cùng 1 cổng nguồn trong T giây
Count-dest-conn	Số luồng tin đến 1 IP duy nhất từ cùng một nguồn
Count-src-conn	Số luồng tin từ 1 IP duy nhất đến cùng một đích
Count-serv-src-conn	Số luồng tin từ 1 IP đến cùng cổng đích
Count-serv-dest-conn	Số luồng đến 1 IP từ cùng một cổng nguồn

Đối với mạng IoT, ta có thể chọn một số đặc trưng lưu lượng điển hình nhất như trên Bảng II.

Bảng II: Các đặc trưng lưu lượng mạng IoT

Thuộc tính	Ý nghĩa
SRC IP ADR	Địa chỉ IP nguồn
DST IP ADR	Địa chỉ IP đích
SRC port	Cổng nguồn
DST port	Cổng đích
Protocol Flags	Các cờ SYN, RST, FIN,…
Received PKT	Số gói tin nhận tại thiết bị
Sent PKT	Số gói tin gửi tới thiết bị
Duration	Thời gian kết nối

Việc lựa chọn này phù hợp với các đề xuất trong [20, 21] và đủ để phân tích, phát hiện các dấu hiệu bất thường nổi bật trên mạng IoT. Quản trị mạng có thể tăng số lượng đặc trưng (ví dụ tối đa 40 như đã chỉ ra trong [19]). Tuy nhiên, khi đó sẽ phải áp dụng các phương pháp giảm chiều dữ liệu để giảm độ phức tạp tính toán, tăng tốc độ phân tích và phát hiện của hệ thống giám sát.

E. Phân tích, phát hiện sự cố an toàn mạng

Có hai cách cơ bản để phát hiện sự cố an toàn mạng là phát hiện theo dấu hiệu và phát hiện hành vi bất thường như đã nêu trong các tài liệu (ví dụ [18, 19]. Tuy nhiên, phát hiện theo dấu hiệu có nhược điểm lớn là phải biết trước mẫu (dấu hiệu) tấn công, do đó không thể phát hiện các tấn công mạng kiểu mới. Phát hiện hành vi bất thường có ưu điểm hơn là có khả năng phát hiện được các tấn công mới, chưa biết trước dấu hiệu. Tuy nhiên, phương pháp này đòi hỏi phải tạo ra một tập các hành vi bình thường của mạng (tạo baseline), thiết lập mức ngưỡng so sánh giữa bình thường và bất thường. Trong quá trình phân tích, hệ thống giám sát thu thập lưu lượng mạng, so sánh với baseline và kiểm tra theo mức ngưỡng để phát hiện bất thường (nghĩa là dấu hiệu có sự cố an toàn mạng).

Phương pháp phân tích và phát hiện có thể được thực hiện theo hai cách phổ biến như đã chỉ ra trong [19, 20, 21] như sau:

- Phát hiện dựa theo phân tích các thành phần chính (Principal Component Analysis) [19]. Tập các

đặc trưng của lưu lượng mạng được chuyển đổi sang miền PCA để giảm độ phức tạp. Việc kiểm tra, so sánh với tập bình thường sử dụng công thức tính khoảng cách (ví dụ Euclidean, Mahalanobis, Mahattan,…).

- Phát hiện dựa theo hàm Entropy [20, 21]. Hàm Entropy được tính dựa theo mức Entropy thống kê của tập dữ liệu đặc trưng của lưu lượng mạng hoặc theo mức Entropy thống kê của từng đặc trưng. Hệ thống giám sát thực hiện tính Entropy của dữ liệu lưu lượng mạng thu thập được, so sánh với giá trị Entropy của tập bình thường đã tính trước đó để tìm ra dấu hiệu bất thường.

Hàm Entropy của tập dữ liệu lưu lượng mạng có thể tính theo công thức sau:

$$H = \sum_i p(x_i).log_2 p(x_i) \quad (20)$$

Trong đó $p(x_i)$ là xác suất xuất hiện đặc trưng x_i trong tập dữ liệu. Giá trị trung bình của $p(x_i)$ được tính theo công thức:

$$p(x_i) = \frac{n(x_i)}{\sum_i P_i} \quad (21)$$

Trong đó, $n(x_i)$ là số sự kiện có chứa đặc trưng x_i, P_i là sự kiện thứ i thu được trong khoảng thời gian giữa hai lần lấy mẫu.

Nếu như tập lấy mẫu chứa n sự kiện có phân bố giống nhau và độc lập với nhau (independent identical distributed – idd), ta có $H = log_2(n)$. Hàm H biểu thị lượng thông tin kỳ vọng có trong mỗi sự kiện trong tập lấy mẫu về lưu lượng mạng.

Đối với tập dữ liệu có hành vi bình thường, hàm Entropy của tập dữ liệu mạng thu thập được có giá trị thống kê ổn định. Bất kỳ một thay đổi bất thường nào trong lưu lượng mạng sẽ tạo ra một sự sai lệch đáng kể trong giá trị thống kê của hàm Entropy. Thông qua một giá trị ngưỡng cho sự khác biệt đó, ta có thể xác định được hành vi bất thường trong lưu lượng mạng thu được, nghĩa là có một sự cố tấn công mạng. Qua phân tích cụ thể hơn các đặc trưng lưu lượng bất thường và so sánh với các mẫu tấn công đã biết, ta có thể xác định được các loại tấn công.

IV. KẾT LUẬN

Bảo đảm an toàn mạng IoT đang đặt ra những thách thức mới do những đặc thù của mạng IoT và các thiết bị IoT. Các thiết bị IoT thường bị hạn chế về tài nguyên (bộ nhớ, băng thông, dung lượng lưu trữ) và năng lực xử lý. Vì vậy, một hệ thống giám sát an toàn mạng IoT cần xem xét các vấn đề này.

Qua khảo sát, bài báo đã chỉ ra một số vấn đề trong hệ thống giám sát an toàn mạng vẫn chưa được xem xét cụ thể, điển hình như: kiến trúc phân lớp, tính toán kích cỡ hệ thống giám sát, lựa chọn đặc trưng sự kiện. Trên cơ sở đó, bài báo đã đề xuất một mô hình kiến trúc hệ thống giám sát an toàn mạng IoT phù hợp với kiến trúc phân lớp. Ngoài ra, bài báo đã đưa ra cách thức tính toán thực tế cho thiết kế hệ thống giám sát đối với một số yêu cầu cụ thể về kích cỡ bộ đệm xử lý sự kiện, dung lượng lưu trữ sự kiện, lựa chọn đặc trưng của sự kiện. Một số ví dụ tính toán cụ thể giúp minh chứng cho tính khả thi của kiến trúc và phương pháp tính toán đã đề xuất trong bài.

TÀI LIỆU THAM KHẢO

[1] https://www.idc.com/getdoc.jsp?containerId=US43087717.

[2] Securing the Internet of Things, Sept 2017. https://www.gartner.com/doc/3316617.

[3] R. Bejtlich, The Tao of Network Security Monitoring Beyond Intrusion Detection, Addison Wesley, 2004.

[4] L. Heberlein, G. Dias, K. Levitt, B. Mukherjee, J. Wood, and D. Wolber, "A Network Security Monitor," Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy, pp. 296–304 (May 1990).

[5] P. Bhattacharya, J.C. Lawrence. Network security monitoring system, US Patent No. 7,483,972. US Patents 2009.

[6] K.Alhamazani, etal., An overview of the commercial cloud monitoring tools: research dimensions, design issues, and state-of-the-art, Journal Computing, Vol 97, Issue 4, Apr.2015, pp.357-377.

[7] M. Kolomeec, A. Chechulin, A. Pronoza, I. Kotenkom, Technique of Data Visualization: Example of Network Topology Display for Security Monitoring, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 7:1 (Mar. 2016), pp. 58-78.

[8] Q.Jing, A.V. Vasilakos, J.Wan, J.Lu, D.Qiu. "Security of the Internet of Things: Perspectives and Challenges". Wireless Networks, Vol 20, Issue 8, Nov. 2014, pp.2481-2501.

[9] C.Kolia, G.Kambourakis, A.Stavrou, J.Voas, "DDoS in the IoT: Mirai and Other Botnets", IEEE Computer Society, 2017, pp.80-85.

[10] J. Granjal, E. Monteiro, J.S. Silva, Security for the internet of things: a survey of existing protocols and open research issues. IEEE Communications Surveys and Tutorials, 17(3), 2015, 1294-1312.

[11] S. Chakrabarty, D.W. Engels, S. Member, A Secure IoT Architecture for Smart Cities, IEEE 13th CCNC, Mar. 2016.

[12] I.Bouij-Pasquier, A.A.El Kalam, A.A. Ouahman, M. De Montfort. "A Security Framework for Internet of Things". LNCS 9476, 2015, pp.19-31.

[13] J.Lin, W.Yu, N.Zhang, etal, A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications, IEEE Internet of Things journal, 2017.

[14] M. Pasha, S.M. Waqas Shah, U. Pasha, "Security Framework for IoT Systems". International Journal of Computer Science and Information Security (IJCSIS), Vol 14, No 11, Nov. 2016, pp.99-104.

[15] A.Chokshi, S.Patel, Internet of Things (IoT), IoT Architecture, Security Challenges in IoT & Role of IoT in Healthcare Industry, Intl. Journal of Engineering Technology Science & Research (IJETSR), Vol4,Iss 10, Oct 2017, pp.822-826.

[16] V. Chalee, R. Ekkachan, T. Phithak, D.H. Hoang, Recent Challenges, Trends, and Concerns Related to IoT Security: An Evolutionary Study, Proc of IEEE IACT 2018. Korea, Feb 2018.

[17] N.M. Tura, Internet of Things: A Survey of Existing architectural models and their security Protocols. IJCSNS International Journal of Computer Science and Network Security, Vol.17, No.5, May 2017. Pp. 198-205.

[18] Y.M. Pa pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, C. Rossow. "IoTPOT: A Novel Hoeypot for Revealing Current IoT Threats". Journal of Information Processing, Vol 24, No.3, May 2016, pp.522-533.

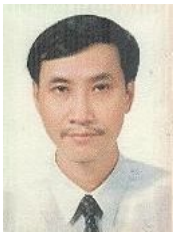
[19] D.H. Hoang, H.D Nguyen, A PCA-based Method for IoT Network Traffic Anomaly Detection, Proc of IEEE IACT 2018. Korea, Feb 2018.

[20] A. Altaher, S. Ramadass, A. Almomani, Real Time Netork Anomaly Detection Using Relative Entropy. Proceedings of High Capacity Optical Networks and Enabling Technologies (HONET), 2011.

[21] M. Marchetti, D. Stabili, A. Guido, M. Colajanni, Evaluation of anomaly detection for in-vehicle networks through information-theoretic algorithms. Proceedings of Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI), IEEE 11/2016.

SECURITY MONITORING FOR IoT NETWORKS

Abstract: Security in IoT networks is different from traditional networks due to the special properties of IoT networks. Models, mechanisms and techniques developed for network security in traditional networks could not be directly applied for IoT networks, calling for suitable modifications. Until now, several problems in network security monitoring systems have not been considered in details. Typical ones are such as the choice of the layer architecture, the calculation of the monitoring system, the selection of event characteristics. This paper proposes an architecture for an IoT network security monitoring system that is corresponding to the layer separation into Fog and Cloud. In addition, the paper proposes a practical suitable calculation method for the design of an IoT network security monitoring system, namely the necessary buffer for event processing, the capacity of event storage and the selection of suitable event characteristics. Some calculation examples are given for proving the feasibility of the proposed method in the practice.



Hoàng Đăng Hải, TS (1999), TSKH (2002) tại CHLB Đức, PGS (2009). Hiện đang đang công tác tại Học viện Công nghệ Bưu chính Viễn thông. Lĩnh vực nghiên cứu: Mạng và hệ thống thông tin, các giao thức truyền thông, chất lượng dịch vụ, mạng IoT, an toàn thông tin, an toàn mạng.