(12) **BẢN MÔ TẢ GIẢI PHÁP HỮU ÍCH THUỘC BẰNG ĐỘC QUYỀN**
**GIẢI PHÁP HỮU ÍCH**

(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ

(11) **2-0004532**

(51) **H04W 12/12**
2022.01

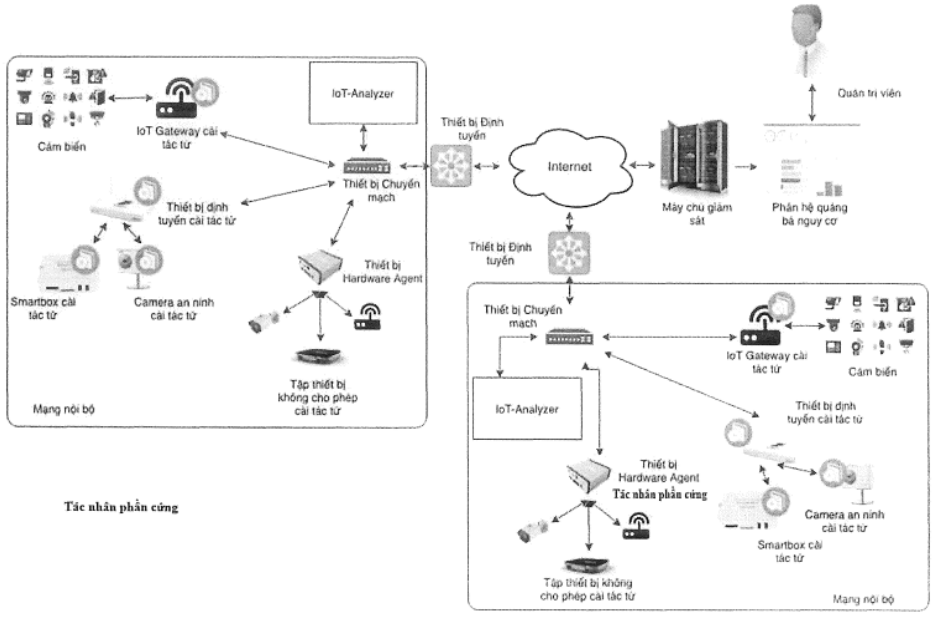
(13) **Y**

(21) 2-2022-00501
(22) 16/11/2022
(45) 25/11/2025 452
(43) 27/05/2024 434
(73) Học viện Công nghệ Bưu chính Viễn thông (VN)
Số 122 Hoàng Quốc Việt, Quận Cầu Giấy, Thành Phố Hà Nội
(72) NGÔ QUỐC DŨNG (VN); NGUYỄN HUY TRUNG (VN).

(54) QUY TRÌNH PHÁT HIỆN TẤN CÔNG MẠNG CHO THIẾT BỊ INTERNET KẾT NỐI VẠN VẬT (IOT) HẠN CHẾ TÀI NGUYÊN

(21) 2-2022-00501

(57) Giải pháp hữu ích đề cập đến quy trình phát hiện tấn công mạng cho thiết bị IoT hạn chế tài nguyên, quy trình này bao gồm các công đoạn: (i) cài đặt tác tử phần mềm trên các thiết bị IoT hạn chế tài nguyên, tác tử có khả năng cài đặt trên các thiết bị IoT đa nền tảng, có khả năng thu thập dữ liệu hoạt động trên thiết bị IoT (gồm System-call, Memory usage, Cpu usage, PiD, Process hash, Pcap, Opening port, Bandwidth, System message), có cơ chế lược bỏ dữ liệu không có hành vi bất thường của thiết bị IoT; (ii) cài đặt tác tử phần cứng trong cùng hệ thống mạng thiết bị IoT hạn chế tài nguyên; (iii) thu thập dữ liệu từ tác tử phần mềm và tác tử phần cứng để xử lý và phát hiện tấn công mạng. Giải pháp đưa ra có khả năng thu thập dữ liệu hoạt động trên thiết bị IoT hạn chế tài nguyên ở mức hệ thống và mức mạng, giúp cho việc phát hiện tấn công mạng một cách toàn diện, giảm đang kể nguy cơ tấn công mạng xảy ra đối với thiết bị IoT hạn chế tài nguyên.




**Hình 1**

**Lĩnh vực kỹ thuật được đề cập**

Giải pháp hữu ích thuộc lĩnh vực công nghệ thông tin, cụ thể là đề cập đến quy trình triển khai giải pháp bảo đảm an toàn thông tin cho thiết bị internet kết nối vạn vật (IoT) hạn chế tài nguyên, giải pháp tạo ra có khả năng nâng cao tính an toàn thông tin cho thiết bị IoT hạn chế tài nguyên và hệ thống mạng thiết bị IoT hạn chế tài nguyên, bằng cách phối hợp giữa thiết bị tác tử phần cứng và cài đặt tác tử phần mềm trên thiết bị IoT hạn chế tài nguyên nhằm tăng khả năng kiểm tra, giám sát mạng cho thiết bị IoT hạn chế tài nguyên.

**Tình trạng kỹ thuật của giải pháp hữu ích**

Theo báo cáo dự báo, tổ chức dữ liệu quốc tế (International Data Group - IDC) ước tính sẽ có 41,6 tỷ thiết bị IoT được kết nối và có thể sinh ra 79,4 zettabyte (ZB) dữ liệu vào năm 2025. Trong năm 2020, khoảng 30% các thiết bị kết nối trong hệ thống mạng doanh nghiệp có quy mô vừa là thiết bị IoT và con số này sẽ tiếp tục gia tăng qua các năm tiếp theo. Dự án Bảo mật Ứng dụng Web Mở (Open Web Application Security Project - OWASP) nhận định 75% thiết bị IoT có nguy cơ bị tin tặc tấn công và xâm hại. Các thiết bị IoT có hai loại chính gồm (1) nhiều tài nguyên (máy chủ, máy tính cá nhân, máy tính bảng,…) và (2) hạn chế tài nguyên (thiết bị định tuyến, IP Camera, TV thông minh …). Loại thiết bị hạn chế tài nguyên (hay còn gọi là IoT cỡ nhỏ) là phạm vi nghiên cứu trong báo cáo giải pháp hữu ích này. Trong các năm 2017-2018 ở Việt Nam, có hơn 316.712 IP Camera cho phép tin tặc tấn công chiếm quyền điều khiển, 1.000 thiết bị định tuyến/thiết bị chuyển mạch của Cisco cho phép tin tặc thực hiện tấn công từ chối dịch vụ, v.v.. Qua đây có thể thấy rằng bảo mật được xác định là thách thức trong việc đẩy mạnh ứng dụng thiết bị IoT. Hai vấn đề kỹ thuật tối thiểu đối với bảo mật thiết bị IoT gồm: (1) các thiết bị IoT (tủ lạnh, lò vi sóng, IP camera giám sát, thiết bị định tuyến, …) có thể được quản lý bởi những người dùng không có chuyên môn trong bảo mật mạng. Một vài thiết bị IoT không có giao diện người dùng, vì vậy việc quản lý (bao gồm cập nhật chính sách bảo mật, cập nhật phần mềm để vá lỗ hổng bảo mật, …) không được thực hiện thường xuyên hoặc không được thực hiện; (2) thiết bị IoT chủ yếu là thiết bị mạng và do đó hạn chế về tính toán hoặc những lý do khác khiến khó triển khai các giải pháp bảo mật hạ tầng phức tạp (ví dụ khả năng tường lửa, phát hiện bất thường, …).

Imran Makhdoom và các đồng tác giả đã trình bày toàn diện các khía cạnh bảo mật đối với thiết bị IoT. Trong đó, xu hướng tấn công mạng phổ biến đối với thiết bị IoT là dựa trên phần mềm độc hại botnet nhằm khởi động các cuộc tấn công, chủ yếu là tấn công từ chối dịch vụ phân tán (Xem tài liệu: Imran Makhdoom, Mehran Abolhasan, Justin Lipman, Ren Ping Liu, Wei Ni. 2018. "Anatomy of threats to the internet of things". IEEE communications surveys & tutorials, 21(2), pp 1636-1675.

Trong công bố đơn đăng ký sáng chế số US 2017/0279620 A1, David W. Kravitz và các đồng tác giả đưa ra giải pháp quản lý và bảo mật cho thiết bị IoT, trong đó chứng minh việc thiết lập kết nối bảo mật giữa các thiết bị IoT bằng cách đưa ra một định danh duy nhất (sử dụng token nhận dạng kỹ thuật số và khóa mật mã) giữa hai thiết bị IoT, các thiết bị IoT được kết nối với nhau thì thiết bị sau sẽ được thiết bị trước đó xác thực và cấp chứng thư số, từ đó ngăn chặn kết nối độc hại từ kẻ tấn công. Tuy nhiên giải pháp ở đây không tập trung vào thiết bị IoT hạn chế tài nguyên, chỉ tập trung vào ngăn chặn và phòng ngừa tấn công mạng chứ không giải quyết vấn đề phát hiện tấn công mạng. (Xem tài liệu: David W . Kravitz, Donald Houston Graham, Josselyn L . Boudett, Russell S . Dietz. 2017. "System and method for Internet of Things (IoT) security and management". U.S. Patent No. 9,716,595).

Trong công bố đơn đăng ký sáng chế số WO 2018/206965 A1, Kaushik Anil và các đồng tác giả đã đưa ra giải pháp phát hiện tấn công mạng vào hệ thống mạng thiết bị IoT dựa trên các đặc trưng của lớp truyền thông vật lý của thiết bị IoT, cụ thể là Radio Frequency (RF). Hay nói cách khác, các tác giả chỉ sử dụng dữ liệu luồng mạng trong phát hiện tấn công mạng nhằm vào thiết bị IoT. Trong khi đó nhiều thiết bị IoT đã bị tin tặc khai thác, chiếm đoạt quyền điều khiển cho các cuộc tấn công mạng, nhưng do tin tặc chưa ra lệnh tấn công mạng nên việc chỉ dựa trên dữ liệu luồng mạng sẽ khó kịp thời phát hiện; bên cạnh đó giải pháp các tác giả đưa ra được triển khai, lắp đặt trong cùng hệ thống mạng các thiết bị IoT, chứ không thể triển khai trực tiếp trên các thiết bị IoT hạn chế tài nguyên. Do đó, giải pháp được đưa ra chưa bảo đảm phát hiện tấn công mạng một cách toàn diện đối với thiết bị IoT hạn chế tài nguyên. (Xem tài liệu: Kaushik Anil, Stutz Daniel. 2018. "Detecting IoT security attack using physical communication layer characteristics". WIPO Patent No. WO 2018/206965 A1).

Trong công bố đơn đăng ký sáng chế số US số 17/070,667, Nima Sharifi Mehr đưa ra giải pháp để thu thập dữ liệu liên quan đến bảo mật từ các thiết bị Internet of Things (IoT), và các thành phần liên quan khác, sử dụng tác tử phần

mềm cài đặt trên thiết bị IoT và các bộ giám sát mạng đặt trong hệ thống mạng thiết bị IoT. Tiếp đó phân tích dữ liệu thu thập được để phát hiện có hay không các giai đoạn tiến triển của các cuộc tấn công mạng nhằm vào thiết bị IoT. Tuy nhiên giải pháp ở đây không tập trung vào thiết bị IoT hạn chế tài nguyên, không nêu rõ cách thức triển khai tác tử phần mềm để có thể cài đặt thành công trên các thiết bị IoT hạn chế tài nguyên, đồng thời không sử dụng tác tử phần cứng. (Xem tài liệu: Nima Sharifi Mehr. 2020. "Security monitoring system for internet of things (IOT) device environments". U.S. Patent No. 10,812,521).

Brasilino và đồng tác giả đã chứng minh về việc sử dụng giao thức ứng dụng bị ràng buộc CoAP trong hệ thống trên vi mạch (System-on-Chip) mảng phần tử logic có thể tái lập trình (Field-programmable Gate Array), đem lại hiệu quả khả quan trọng là giảm thiểu ảnh hưởng của tấn công từ chối dịch vụ phân tán (DdoS - Distributed Denial of Service) nhằm vào các thiết bị IoT. Giải pháp này chỉ tập trung xử lý khi tấn công DDoS nhằm vào tiêu tốn tài nguyên tính toán của thiết bị IoT (CPU), nếu tấn công DDoS nhằm vào băng thông mạng thì không có khả năng xử lý. (Xem tài liệu Brasilino Lucas RB, Swany Martin.2019. "Mitigating ddos flooding attacks against iot using custom hardware modules". In Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS). IEEE. p. 58-64). Faik Kerem Örs đã chứng minh về việc pháp hiện và phân loại tấn công mạng nhằm vào thiết bị IoT dựa trên giao thức 6LoWPANs và RPL có hiệu quả rất tốt. Với dữ liệu lưu lượng mạng thu thập từ hệ thống mạng các thiết bị IoT và từ trực tiếp các thiết bị IoT (trong một khoảng thời gian nhất định), ứng dụng học máy được sử dụng để huấn luyện và phân loại 06 loại tấn công mạng gồm sinkhole, blackhole, selective forwarding, DIS flood, version number, Mirai botnet UDP flood), trong đó tập trung vào tấn công mạng botnet IPv4 nhắm mục tiêu vào mạng 6LoWPAN. Nghiên cứu này chưa đưa ra mô hình quy trình hệ thống, không tập trung vào các thiết bị IoT hạn chế tài nguyên cũng như dữ liệu sử dụng chỉ ở mức mạng, không thu thập thông tin mức hệ thống trên các thiết bị IoT. (Xem tài liệu Faik Kerem Örs.2021. "Data driven intrusion detection for 6LoWPAN based IoT systems". Doctoral dissertation. Sabanci University, Turkish).

Trong khi đó, các mối đe dọa chính mà tầng mạng phải đối mặt bao gồm chứng thực tính toàn vẹn của dữ liệu, truy cập trái phép thiết bị, tấn công từ chối dịch vụ phân tán. Do việc hạn chế tài nguyên như bộ nhớ, năng lực xử lý và không có khả năng triển khai các giải pháp bảo mật nhằm phát hiện các cuộc tấn công mạng nhằm vào thiết bị IoT hạn chế tài nguyên. Do đó, cần có giải pháp tiếp cận

toàn diện để hỗ các thiết bị IoT hạn chế tài nguyên để phát hiện các tấn công mạng.

Về giải pháp này (các) tác giả đã có công bố trên tạp chí khoa học, thông tin cụ thể như sau:

Nguyen, H. T., & Ngo, Q. D. (2022). Cyberattack detection and prevention on resource-constrained IoT devices based on intelligent agents. Emerging Real-World Applications of Internet of Things, pp. 41-68. CRC Press, Boca Raton, United State. https://doi.org/10.1201/9781003304203.

**Bản chất kỹ thuật của giải pháp hữu ích**

Mục đích của giải pháp hữu ích là khắc phục những nhược điểm và giải quyết những vấn đề nêu trên. Để đạt được mục đích đó, giải pháp hữu ích đề xuất giải pháp triển khai tác tử phần mềm có khả năng cài đặt trên thiết bị IoT hạn chế tài nguyên và tác tử phần cứng đặt trong cùng hệ thống mạng thiết bị IoT hạn chế tài nguyên để phát hiện tấn công mạng nhằm vào thiết bị IoT hạn chế tài nguyên.

Theo một phương án ưu tiên, giải pháp hữu ích đề xuất quy trình phát hiện tấn công mạng cho thiết bị internet kết nối vạn vật (IoT) hạn chế tài nguyên, bằng cách phối hợp giữa các thiết bị tác tử phần cứng (hardware agent) và các tác tử phần mềm (software agent) được cài đặt trên các thiết bị IoT hạn chế tài nguyên có phần sụn mở (cho phép cài đặt) nhằm tăng khả năng kiểm tra, giám sát mạng cho thiết bị IoT hạn chế tài nguyên. Quy trình theo giải pháp hữu ích gồm các công đoạn sau:

a. Cài đặt tác tử phần mềm trên thiết bị IoT hạn chế tài nguyên

b. Triển khai tác tử phần cứng trong hệ thống mạng thiết bị IoT hạn chế tài nguyên

c. Tổng hợp dữ liệu thu thập từ tác tử phần mềm và tác tử phần cứng để phát hiện tấn công mạng nhằm vào thiết bị IoT

Quy trình triển khai giải pháp phát hiện tấn công mạng cho thiết bị IoT hạn chế tài nguyên có các đặc trưng sau:

- Tác tử phần mềm có kích thước nhỏ gọn (dưới 1 MB) vừa có khả năng cài đặt tích hợp trên các thiết bị IoT hạn chế tài nguyên (với các nền tảng kiến truc vi xử lý đa dạng gồm MIPS, ARM, x86, PowerPC, Sparc), vừa thu thập thông tin hoạt động của thiết bị IoT gồm: System-call, Memory usage, Cpu usage, PiD, Process hash, PCAP, Opening port, Bandwidth, System message.

- Quy trình kết hợp với tác tử phần cứng được triển khai trong hệ thống mạng thiết bị IoT hạn chế tài nguyên, cho phép thu thập dữ liệu và quản trị các thiết bị IoT không cho phép cài đặt tác tử phần mềm, trong đó dữ liệu tấn công mạng được thu thập thông tin ở mức hệ thống trên nhiều thiết bị IoT.

- Thông tin được thu thập từ tác tử phần mềm và tác tử phần cứng được truyền tải và xử lý tại các phân hệ xử lý trung tâm (IoT-Analyzer) nhằm đảm bảo tốc độ xử lý, do đó, đảm bảo hiệu quả cao trong phát hiện tấn công mạng.

Với những đặc trưng nêu trên, quy trình này có thể khắc phục được những điểm hạn chế của các quy trình đã biết, tạo ra một giải pháp phát hiện tấn công mạng nhằm vào các thiết bị IoT hạn chế tài nguyên có hiệu quả kép, vừa làm gia tăng khả năng giám sát an ninh, an toàn thông tin thiết bị IoT hạn chế tài nguyên, vừa làm tăng khả năng thu thập dữ liệu đối với thiết bị IoT không hỗ trợ giao thức SNMP (Simple Network Management Protocol).

Tác tử phần mềm được phát triển có hỗ trợ khả năng lược bỏ dữ liệu không có hành vi bất thường của thiết bị IoT hạn chế tài nguyên. Tác tử phần mềm hoạt động tiêu tốn ít tài nguyên của thiết bị.

**Mô tả vắn tắt các hình vẽ**

Hình 1 là Sơ đồ quy trình giải pháp phát hiện tấn công mạng cho thiết bị IoT hạn chế tài nguyên;

Hình 2 là hình vẽ mô hình hoạt động của trình biên dịch chéo;

Hình 3 là hình vẽ mô hình tiếp nhận, tiền xử lý dữ liệu được đề xuất.

**Mô tả chi tiết giải pháp hữu ích**

Sau đây quy trình phát hiện tấn công mạng cho thiết bị IoT hạn chế tài nguyên được đề xuất sẽ được mô tả chi tiết như sau:

Các thiết bị IoT hạn chế tài nguyên (như IoT Gateway, IP Camera, Router, Smartbox) được sản xuất tại Việt Nam cũng như nhập khẩu từ nước ngoài được chia làm hai loại:

- Loại 1 là các thiết bị có phần sụn (firmware) mở và cho phép cài đặt phần mềm tác tử trực tiếp bộ nhớ Flash hoặc lên bộ nhớ RAM của thiết bị;

- Loại 2 là các thiết bị có phần sụn đóng và không cho phép cài đặt phần mềm tác tử lên thiết bị.

Như được thể hiện trên hình 1, trong phạm vi giải pháp hữu ích này, tác tử phần cứng (Hardware-Agent) là một thiết bị mạng nằm trong mạng LAN, được

thiết kế, chế tạo và hoạt động một cách trong suốt đối với hệ thống mạng thiết bị IoT hạn chế tài nguyên với nhiệm vụ chính là thu thập thông tin/giám sát thiết bị IoT. Vị trí, chức năng của Hardware-Agent cụ thể trong các trường hợp sau:

+ Đối với các mô hình mạng nhỏ như mạng Small Office – Home Office (SOHO) thì Hardware-Agent sẽ được dùng thay thế trực tiếp cho các Router/IoT Gateway và cho phép kết nối, giám sát hoạt động của các thiết bị IoT hạn chế tài nguyên với Internet.

+ Đối với các mô hình mạng lớn hơn thì Hardware-Agent đóng vai trò như một thiết bị mạng đứng giữa các thiết bị IoT hạn chế tài nguyên và thiết bị chuyển mạch như trên hình 1.

Đối với các thiết bị loại 2, hệ thống sử dụng thiết bị Hardware-Agent cho phép kết nối, thu thập dữ liệu, giám sát các cuộc tấn công mạng nhằm vào các thiết bị IoT này. Đối với các thiết bị loại 1, hệ thống sẽ thực hiện cài đặt các tác tử lên thiết bị để thu thập dữ liệu, tiền xử lý và phân tích. Hệ thống bao gồm 03 phân hệ chính như sau:

a. Phân hệ thu thập dữ liệu

Phân hệ này bao gồm mạng lưới các tác tử được cài đặt trên các thiết bị IoT (IoT gateway, Router, Smartbox và IP Camera) và các thiết bị Hardware-Agent được thiết lập trong hệ thống có nhiệm vụ là thu thập dữ liệu thông tin có chọn lọc liên quan đến quá trình vận hành của thiết bị, trong đó dữ liệu tấn công mạng được thu thập thông tin ở mức hệ thống trên nhiều thiết bị IoT. Các thông tin này bao gồm: dữ liệu luồng mạng (PCAP) và dữ liệu hệ thống của thiết bị (syscalls, PiD…). Thông thường, các thiết bị IoT hạn chế tài nguyên có cấu trúc gồm các thành phần chính như sau:

- CPU: điều khiển mọi hoạt động của thiết bị trên cơ sở các hệ thống chương trình thực thi của hệ điều hành.

- ROM: chứa các chương trình tự động kiểm tra và có thể có thành phần cơ bản nhất sao cho thiết bị có thể thực thi được một số hoạt động tối thiểu ngay cả khi không có hệ điều hành hay hệ điều hành bị hỏng.

- RAM: cấp phát vùng nhớ cho các quá trình như: các vùng đệm, tập tin cấu hình khi chạy, các thông số đảm bảo hoạt động của thiết bị.

- FLASH: là bộ nhớ có khả năng ghi và xóa, không mất dữ liệu khi mất nguồn.

Thông thường, phần sụn của thiết bị được lưu trữ ở đây. Tùy thuộc các thiết bị khác nhau mà hệ điều hành sẽ được chạy trực tiếp từ Flash hay được tải lên RAM trước khi chạy. Tập tin cấu hình cũng có thể được lưu trữ trong Flash.

- NVRAM (None-Volatile RAM): có chức năng tương tự như FLASH nhưng với khả năng lưu trữ ít hơn. NVRAM thường chứa tập tin cấu hình của thiết bị để đảm bảo khi khởi động, cấu hình mặc định của thiết bị sẽ được tự động nạp về đúng trạng thái đã lưu giữ.

Thành phần quan trọng nhất đảm bảo cho mọi hoạt động của các thiết bị IoT chính là phần sụn. Cấu trúc của phần sụn rất đa dạng, phụ thuộc vào chức năng và thiết kế của từng nhà sản xuất. Phần sụn có thể được chia thành các kiểu như sau:

- ***Full-blown*** (full-OS/kernel + bootloader + libs + apps): đây thường là một Linux hoặc Windows firmware vì chúng chứa một hệ điều hành hoàn chỉnh nhưng tối giản. Các ứng dụng có thể chạy trong chế độ người dùng, kernel modules, drivers.

- ***Integrated*** (apps + OS-as-a-lib): đây là một bản firmware không đầy đủ, các chức năng và hệ điều hành được xây dựng như một thư viện chứ không có đầy đủ các thành phần cần thiết như trong bản Full-blown.

- ***Partial updates*** (apps or libs or resources or support): Loại firmware này chỉ chứa các tập tin dùng trong việc cập nhật cho bản firmware cần nâng cấp

Trong phạm vi giải pháp hữu ích này, để có thể thu thập thông tin có chọn lọc liên quan đến quá trình vận hành của thiết bị như dữ liệu luồng mạng (pcap), dữ liệu hoạt động mức hệ thống của thiết bị (syscalls, PiD…), tập trung nghiên cứu các loại thiết bị IoT hạn chế tài nguyên được trang bị phần sụn Full-blown. Phần sụn Full-Blown thông thường chứa các tập tin hệ thống như sau:

- ***Bootloader***: là một đoạn mã được thực thi trước khi hệ điều hành bắt đầu chạy và nó cho phép nhà sản xuất thiết bị quyết định những tính năng nào người sử dụng được phép dùng hoặc bị hạn chế.

- ***Kernel***: được hiểu là hạt nhân, là thành phần trung tâm của thiết bị, có trách nhiệm giúp cho phần cứng và phần mềm của thiết bị có thể giao tiếp được với nhau. Kernel là thành phần quan trọng nhất trong thiết bị, nếu kernel bị hỏng thì thiết bị sẽ dừng hoạt động. Kernel thường được lưu trữ trong bộ nhớ Flash của thiết bị.

- ***File–system images***: chứa các tập tin hệ thống có chức năng tổ chức và kiểm soát quá trình hoạt động của thiết bị nhúng.

- ***Web–server/web–interface***: đây chính là thành phần quan trọng giúp cho người dùng có thể tương tác được với thiết bị một cách dễ dàng. Tất cả các thông tin và cấu hình thiết bị phần lớn được thao tác thông qua Web–server và Web–interface. Do đó, đối với yêu cầu cài đặt tác tử phần mềm và các thiết bị IoT hạn chế tài nguyên, giải pháp hữu ích thông qua 3 hình thức như sau:

+ Đối với các thiết bị cho phép cập nhật phần sụn thông qua kênh Webserver/web-Interface: Chỉnh sửa firmware của thiết bị bằng cách đóng gói thêm tác tử vào Kernel, sau đó sẽ cập nhật trực tiếp vào bộ nhớ Flash của thiết bị. Cách này sẽ đảm bảo mỗi lần khởi động thiết bị thì tác tử cũng mặc định được kích hoạt.

+ Đối với các thiết bị không cho phép can thiệp, chỉnh sửa Kernel: Cài đặt gián tiếp tác tử thông qua các cổng dịch vụ mạng như Ssh, Telnet...Cách này đảm bảo tác tử được cài đặt trên bộ nhớ RAM và sẽ bị mất đi khi thiết bị khởi động lại. Do đó, cần có cơ chế định danh, xác định một thiết bị đã được cài tác tử hay chưa để từ đó có biện pháp cài đặt.

+ Đối với các thiết bị không cho phép can thiệp, cài đặt tác tử phần mềm thì tác tử phần cứng là biện pháp cần thiết giúp cho việc thu thập thông tin được thực hiện. Tác tử phần cứng được thiết kế, chế tạo và hoạt động một cách trong suốt nằm trong mạng LAN và là bước đệm kết nối giữa các thiết bị IoT hạn chế tài nguyên và thiết bị chuyển mạch trung tâm. Do không thể can thiệp vào mức hệ thống các thiết bị nên dữ liệu thu thập của tác tử phần cứng sẽ từ lưu lượng mạng.

Khác với các thiết bị máy tính cá nhân với bộ vi xử lý đa phần dùng nền tảng i386 và hệ điều hành Windows, thì thiết bị IoT hạn chế tài nguyên sử dụng đa dạng các bộ vi xử lý khác nhau như MIPS32, MIPS64, ARM, PowerPC, SPARC. Do đó, một trong những yêu cầu quan trọng trong xây dựng các tác tử phần mềm đó chính là việc phát triển một trình biên dịch chéo cho phép biên dịch từ một ngôn ngữ bậc cao thành tệp tin thực thi cho nền tảng Linux. Dữ liệu đầu vào là mã nguồn của một ngôn ngữ lập trình (ở đây là C) và các thư viện cần thiết của mã nguồn. Dữ liệu đầu ra là một tệp thực thi với nền tảng vi xử lý mong muốn (x86, Arm, Mips, Sparc, PowerPC, …), như tại hình 2.

Sau quá trình thu thập, dữ liệu thô sẽ được gửi về và xử lý tại phân hệ xử lý và phân tích dữ liệu, như tại hình 3.

b. Phân hệ xử lý và phân tích dữ liệu

Phân hệ này được phát triển theo hướng phân tán với mỗi điểm phân tích (IoT-Analyzer) quản trị độc lập một tập các thiết bị IoT. Từ những dữ liệu thu được, phân hệ tiến hành phân tích và cảnh báo các nguy cơ an ninh mạng trước khi gửi về máy chủ giám sát tập trung. Mỗi điểm phân tích này gồm 2 môđun chính:

+ Môđun tiền xử lý và chuẩn hoá dữ liệu thu thập được từ các thiết bị dưới sự quản lý của từng điểm trong hệ thống,

+ Môđun áp dụng mô hình học máy trong việc phân tích và phát hiện các nguy cơ tấn công mạng.

Theo một khía cạnh, giải pháp hữu ích cũng đề xuất việc sử dụng Kafka như một bộ đệm giúp tránh tình huống thắt nút cổ chai khi lượng dữ liệu xử lý quá lớn và làm ảnh hưởng đến tài nguyên của thiết bị. Cũng tại phân hệ IoT-Analyzer này, giải pháp hữu ích đề xuất sử dụng GPU có tối thiểu 3500 cores Cuda cho phép áp dụng các thuật toán học máy/học sâu trong việc xây dựng mô hình và phát hiện các cuộc tấn công mạng nhằm vào các thiết bị IoT hạn chế tài nguyên.

c. Phân hệ giám sát tập trung, cảnh báo và ngăn chặn tấn công

Để nâng cao khả năng phân tích, cảnh báo các nguy cơ của tấn công mạng của hệ thống, máy chủ tập trung giám sát có nhiệm vụ cập nhật các hành vi mạng/hệ thống bất thường, mẫu mã độc mới, địa chỉ IP độc hại… từ các nguồn mã nguồn mở tin cậy. Các nguồn dữ liệu này được sử dụng để huấn luyện mô hình trước khi cập nhật cho các điểm phân tích. Ngoài ra, máy chủ giám sát cũng là cầu nối cập nhật các mẫu tác tử phần mềm mới và giúp cho quản trị viên theo dõi và giám sát các thiết bị hệ thống đang quản lý, trạng thái giám sát của tác tử với thiết bị, các cảnh báo tấn công mạng nhằm vào thiết bị IoT. Trong khuôn khổ giải pháp hữu ích, các hình thức tấn công mạng nhằm vào hệ thống mạng thiết bị IoT hạn chế tài nguyên được phát hiện gồm: tấn công từ chối dịch vụ, tấn công bằng mã độc.

**Ví dụ thực hiện giải pháp hữu ích**

Ví dụ 1: Sử dụng hệ thống nhằm phát hiện tấn công từ chối dịch vụ (DDoS) nhằm vào thiết bị định tuyến VNPT GPON ONT iGate GW040-H.

Thực hiện phát hiện tấn công DDoS được thực hiện như sau:

- Chuẩn bị một máy tính có cài đặt phần mềm hỗ trợ tấn công DDoS tiến hành tấn công mạng vào thiết bị định tuyến VNPT iGate GW040-H được quản lý

bởi giải pháp hữu ích, theo các hình thức tấn công phổ biến như (TCP flood, SYN flood, Slowloris) với lưu lượng băng thông lớn.

- Thiết bị VNPT iGate GW040-H có cài tác tử phần mềm và trong cùng hệ thống mạng có Hardware-Agent nhằm tiến hành thu thập các thông tin của thiết bị VNPT iGate GW040-H và gửi dữ liệu về IoT-Analyzer.

Ví dụ 2: Sử dụng hệ thống nhằm phát hiện mã độc Botnet chạy trong thiết bị định tuyến VNPT GPON ONT iGate GW040-H.

- Chuẩn bị một tệp thực thi của mã độc Botnet phổ biến trên các thiết bị IoT. Tiếp hành chạy tệp thực thi của mã độc Botnet trên thiết bị định tuyến VNPT iGate GW040-H có cài đặt tác tử phần mềm.

- Tác tử phần mềm được cài đặt trên thiết bị VNPT iGate GW040-H sẽ tiến hành quét, lấy thông tin của các tiến trình đang chạy trên thiết bị và gửi về IoT-Analyzer.

**Hiệu quả đạt được của giải pháp hữu ích**

Quy trình triển khai giải pháp phát hiện tấn công mạng cho thiết bị IoT hạn chế tài nguyên sử dụng dữ liệu được thu thập từ tác tử phần mềm trên thiết bị VNPT GPON ONT iGate GW040-H. Với dữ liệu thu thập được, phân hệ IoT-Analyzer tiến hành tiền xử lý, phân tích, trích chọn và đưa các dữ liệu được tiếp nhận qua mô hình học máy/học sâu để phân loại. Các hành vi tấn công DDoS được mô hình học máy/học sâu phát hiện và đưa ra cảnh báo cho quản trị viên hệ thống. Bằng các mô hình học máy/học sâu, giải pháp cho phép phát hiện các hành vi tấn công từ chối dịch vụ với độ chính xác cao lên tới hơn 90% với nhiều hình thức tấn công khác nhau nhằm vào thiết bị định tuyến VNPT GPON ONT iGate GW040-H.

Mặt khác, nhờ có dữ liệu hệ thống thu thập từ thiết bị định tuyến VNPT GPON ONT iGate GW040-H, phân hệ IoT-Analyzer tiến hành phân tích các thông tin tiến trình nhận được với cơ sở dữ liệu về mã độc đã biết và các cơ sở dữ liệu về mã độc công khai. Kết quả tiến trình của mã độc botnet được IoT-Analyzer phát hiện và đưa ra cảnh báo cho quản trị viên hệ thống. Do đó, việc sử dụng dữ liệu thu thập từ giải pháp hữu ích trong phát hiện tấn công mạng cho thiết bị IoT hạn chế tài nguyên được cải thiện rõ rệt, tăng khả năng phát hiện các hình thức tấn công mạng với dữ liệu thu thập được ở mức mạng và mức hệ thống của thiết bị IoT hạn chế tài nguyên

## YÊU CẦU BẢO HỘ

1. Quy trình phát hiện tấn công mạng cho thiết bị internet kết nối vạn vật (IoT) hạn chế tài nguyên, bằng cách phối hợp giữa các thiết bị tác tử phần cứng (hardware agent) và các tác tử phần mềm (software agent) được cài đặt trên các thiết bị IoT hạn chế tài nguyên có phần sụn mở (cho phép cài đặt) nhằm tăng khả năng kiểm tra, giám sát mạng cho thiết bị IoT hạn chế tài nguyên, trong đó mạng nêu trên là hệ thống bao gồm:

a. phân hệ thu thập dữ liệu

phân hệ này bao gồm mạng lưới các tác tử phần mềm được cài đặt trên các thiết bị IoT (gồm IoT gateway, Router, Smartbox và IP Camera) và các thiết bị tác tử phần cứng được thiết lập trong hệ thống, có nhiệm vụ thu thập dữ liệu thông tin có chọn lọc liên quan đến quá trình vận hành của các thiết bị, trong đó dữ liệu tấn công mạng được thu thập thông tin ở mức hệ thống trên nhiều thiết bị IoT, các thông tin này bao gồm: dữ liệu luồng mạng ít nhất gồm file dữ liệu PCAP (Packet Capture Data) và dữ liệu hệ thống của thiết bị ít nhất gồm syscalls, PiD, sau quá trình thu thập, dữ liệu thô sẽ được gửi về và xử lý tại phân hệ xử lý và phân tích dữ liệu;

b. phân hệ xử lý và phân tích dữ liệu

phân hệ này được phát triển theo hướng phân tán với mỗi điểm phân tích (IoT-Analyzer) quản trị độc lập một tập hợp các thiết bị IoT, từ những dữ liệu thu được, phân hệ này tiến hành phân tích và cảnh báo các nguy cơ an ninh mạng trước khi gửi về máy chủ giám sát tập trung, mỗi điểm phân tích này gồm hai môđun chính:

môđun tiền xử lý và chuẩn hoá dữ liệu thu thập được từ các thiết bị dưới sự quản lý của từng điểm phân tích trong hệ thống;

môđun áp dụng mô hình học máy trong việc phân tích và phát hiện các nguy cơ tấn công mạng;

c. phân hệ giám sát tập trung, cảnh báo và ngăn chặn tấn công

phân hệ này gồm máy chủ tập trung giám sát có nhiệm vụ cập nhật các hành vi mạng/hệ thống bất thường, mẫu mã độc mới, địa chỉ IP độc hại từ các nguồn mã nguồn mở tin cậy, các nguồn dữ liệu này được sử dụng để huấn luyện mô hình trước khi cập nhật cho các điểm phân tích,

ngoài ra, máy chủ giám sát cũng là cầu nối cập nhật các mẫu tác tử phần mềm mới và giúp cho quản trị viên quản lý các thiết bị của mình thông qua phân hệ quảng bá nguy cơ;

và quy trình phát hiện tấn công mạng này bao gồm các công đoạn:

cài đặt tác tử phần mềm trên thiết bị IoT hạn chế tài nguyên, tác tử phần mềm này có khả năng cài đặt trên các thiết bị IoT hạn chế tài nguyên (cho phép cài đặt) và thu thập dữ liệu mức hệ thống và mức mạng;

lắp đặt thiết bị tác tử phần cứng trong cùng hệ thống mạng thiết bị IoT hạn chế tài nguyên;

đưa dữ liệu thu thập được từ các tác tử phần mềm và các tác tử phần cứng tới các điểm phân tích (IoT-Analyzer);

tại mỗi điểm phân tích, thực hiện:

tiền xử lý và chuẩn hoá dữ liệu thu thập được từ các thiết bị dưới sự quản lý của từng điểm phân tích trong hệ thống,

áp dụng mô hình học máy trong việc phân tích và phát hiện các nguy cơ tấn công mạng;

cập nhật, bởi máy chủ tập trung giám sát, các hành vi mạng/hệ thống bất thường, mẫu mã độc mới, địa chỉ IP độc hại từ các nguồn mã nguồn mở tin cậy, các nguồn dữ liệu này được sử dụng để huấn luyện mô hình trước khi cập nhật cho các điểm phân tích, và ngoài ra, máy chủ giám sát cũng cập nhật các mẫu tác tử phần mềm mới và giúp cho quản trị viên quản lý các thiết bị của mình thông qua phân hệ quảng bá nguy cơ;

và trong đó tác tử phần mềm được tạo cấu hình để:

có khả năng thu thập thông tin hoạt động của các thiết bị IoT hạn chế tài nguyên, bao gồm: System-call, Memory usage, Cpu usage, PiD, Process hash, Pcap, Opening port, Bandwidth, System message,

có kích thước nhỏ gọn (< 1Mb), có khả năng tích hợp trên các thiết bị có tài nguyên hạn chế (Flash trên các thiết bị IoT có dung lượng tối thiểu là 4Mb),

có khả năng tích hợp trên các nền tảng kiến trúc vi xử lý gồm MIPS32, MIPS64, ARM, PowerPC, SPARC, bằng cách triển khai trên các tác tử phần mềm một trình biên dịch chéo cho phép biên dịch từ một ngôn ngữ bậc cao thành mã thực thi trên các nền tảng kiến trúc vi xử lý khác nhau (Mips32, Mips64, Arm, Intel X86, PowerPC, Sparc),

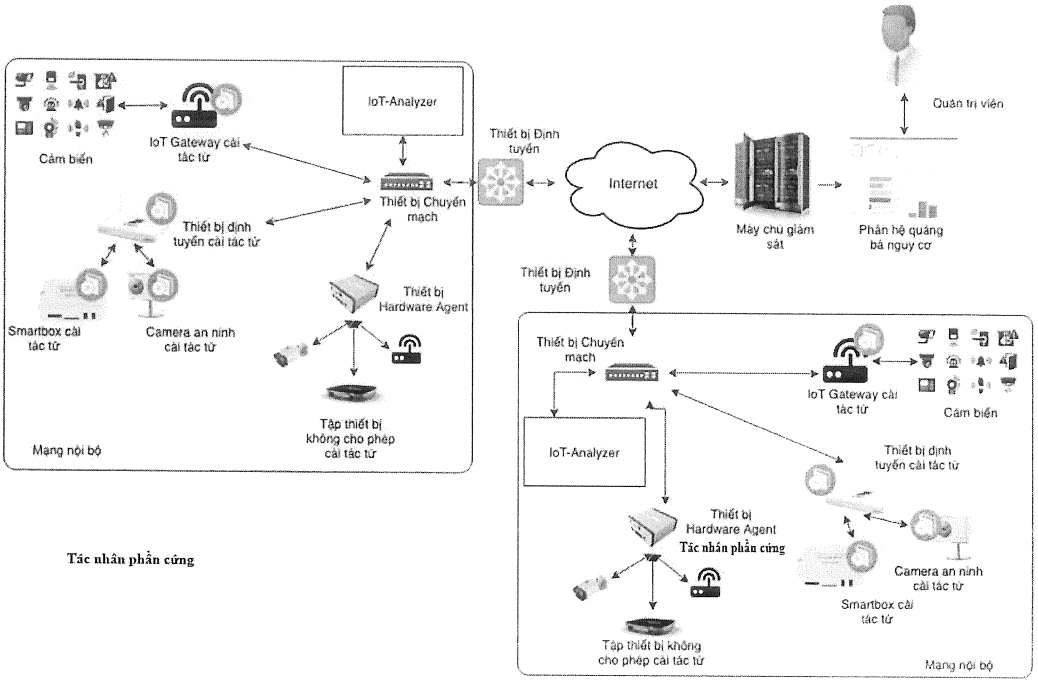
không sửa đổi, tuỳ biến nhân (Kernel) của thiết bị IoT được cài đặt;

có tích hợp cơ chế thu thập và lược bỏ dữ liệu không có hành vi bất thường của thiết bị IoT.

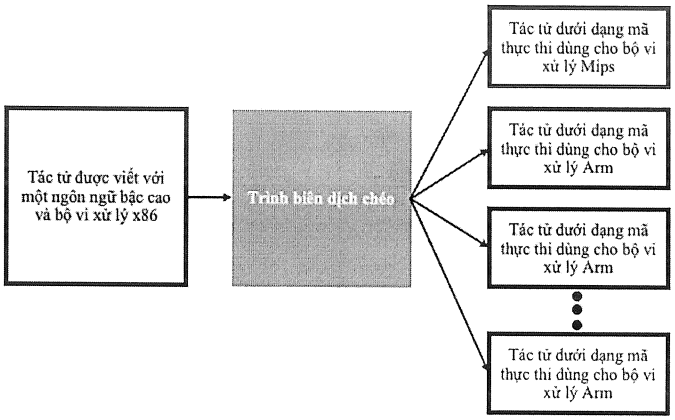
2. Quy trình theo điểm 1, trong đó:

phân hệ xử lý và phân tích dữ liệu sử dụng nền tảng Apache Kafka như một bộ đệm giúp tránh tình huống thắt nút cổ chai khi lượng dữ liệu xử lý quá lớn và làm ảnh hưởng đến tài nguyên của thiết bị.

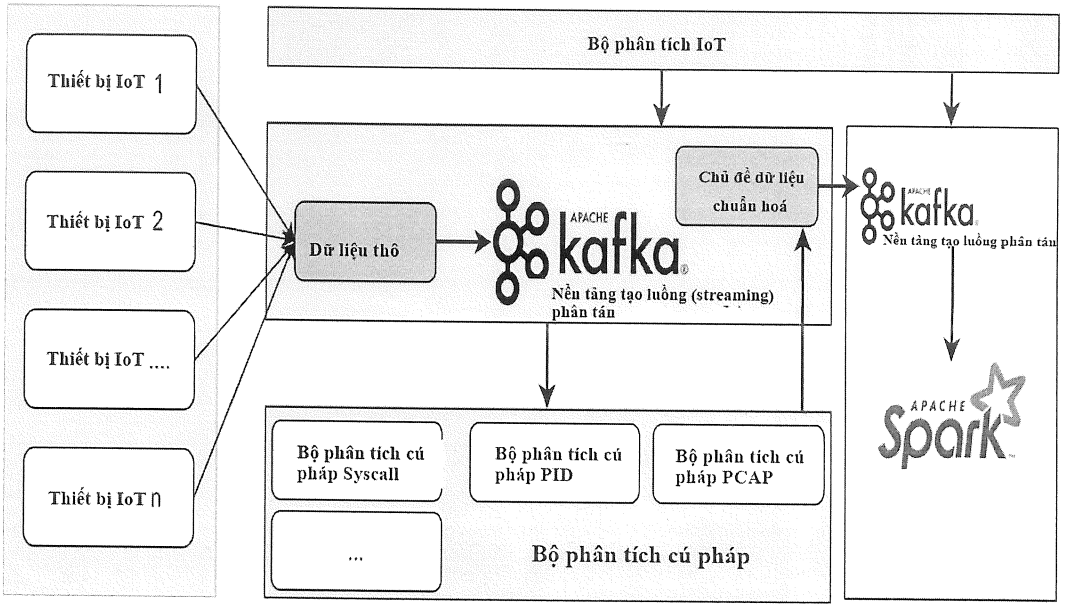
3. Quy trình theo một trong các điểm nêu trên, trong đó trong phân hệ xử lý và phân tích dữ liệu, điểm phân tích (IoT-Analyzer) sử dụng GPU có tối thiểu 3500 cores CUDA (Compute Unified Device Architecture) cho phép áp dụng các thuật toán học máy/học sâu trong việc xây dựng mô hình và phát hiện các cuộc tấn công mạng nhằm vào các thiết bị IoT hạn chế tài nguyên.


IoT-Analyzer
Cảm biến
IoT Gateway cài tác tử
Thiết bị Chuyển mạch
Thiết bị định tuyến cài tác tử
Smartbox cài tác tử
Camera an ninh cài tác tử
Thiết bị Hardware Agent
Tập thiết bị không cho phép cài tác tử
Mạng nội bộ
Tác nhân phần cứng
Thiết bị Định tuyến
Internet
Quản trị viên
Máy chủ giám sát
Phần hệ quản bá nguy cơ
Thiết bị Định tuyến
Thiết bị Chuyển mạch
IoT Gateway cài tác tử
Cảm biến
IoT-Analyzer
Thiết bị định tuyến cài tác tử
Thiết bị Hardware Agent
Tác nhân phần cứng
Camera an ninh cài tác tử
Smartbox cài tác tử
Tập thiết bị không cho phép cài tác tử
Mạng nội bộ

**Hình 1**


Tác tử được viết với một ngôn ngữ bậc cao và bộ vi xử lý x86
Trình biên dịch chéo
Tác tử dưới dạng mã thực thi dùng cho bộ vi xử lý Mips
Tác tử dưới dạng mã thực thi dùng cho bộ vi xử lý Arm
Tác tử dưới dạng mã thực thi dùng cho bộ vi xử lý Arm
Tác tử dưới dạng mã thực thi dùng cho bộ vi xử lý Arm

**Hình 2**


Thiết bị IoT 1
Thiết bị IoT 2
Thiết bị IoT ....
Thiết bị IoT n
Bộ phân tích IoT
Dữ liệu thô
APACHE kafka
Nền tảng tạo luồng (streaming) phân tán
Chủ đề dữ liệu chuẩn hoá
APACHE kafka
Nền tảng tạo luồng phân tán
APACHE Spark
Bộ phân tích cú pháp Syscall
Bộ phân tích cú pháp PID
Bộ phân tích cú pháp PCAP
...
Bộ phân tích cú pháp

**Hình 3**