(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

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

(11) **1-0031187**

(51)[7] **H04L 63/00**

(13) **B**

(21) 1-2019-05256

(22) 26/09/2019

(45) 25/02/2022 407

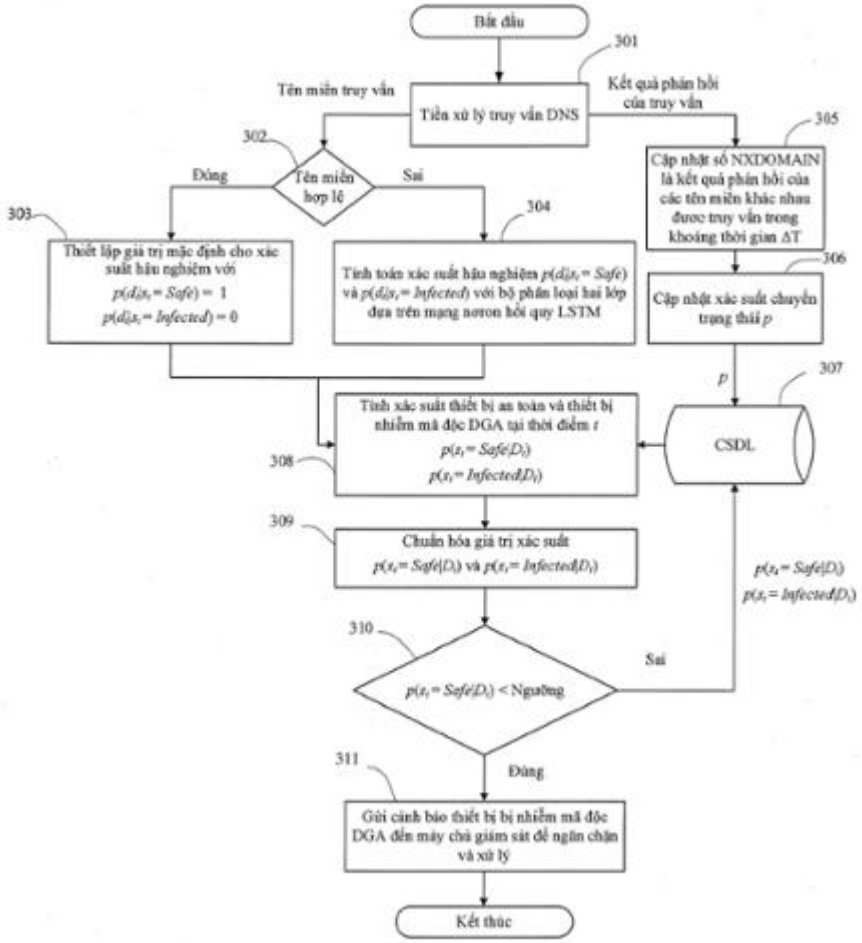
(43) 25/12/2019 381A

(73) Trường Đại học Bách khoa Hà Nội (VN)
Số 1, Đại Cồ Việt, quận Hai Bà Trưng, thành phố Hà Nội

(72) Trần Quang Đức (VN); Mạc Đình Hiếu (VN); Nguyễn Linh Giang (VN).

(54) PHƯƠNG PHÁP PHÁT HIỆN THIẾT BỊ BỊ NHIỄM MÃ ĐỘC DGA

(57) Sáng chế đề cập đến phương pháp phát hiện thiết bị bị nhiễm mã độc thuật toán sinh tên miền tự động (Domain Generation Algorithm - DGA), một trong những giải pháp cho phép ngăn chặn sự phát tán của Botnet. Phương pháp dựa trên định lý Bayes, mô hình Markov ẩn (Hidden Markov Model - HMM) và giả định Markov, trong đó sử dụng kết hợp xác suất chuyển trạng thái, xác suất hậu nghiệm và tình trạng thiết bị ở thời điểm thực hiện truy vấn tên miền trước đó. Xác suất chuyển trạng thái có thể tính toán trên cơ sở số lượng NXDOMAIN là kết quả phản hồi của nhiều tên miền không tồn tại khác nhau được truy vấn trong một khoảng thời gian. Xác suất hậu nghiệm được thiết lập mặc định để giảm khối lượng tính toán nếu tên miền thuộc danh sách tên miền hợp lệ. Trong trường hợp tên miền không nằm trong danh sách, xác suất hậu nghiệm là kết quả của mạng nơron hồi quy bộ nhớ dài ngắn hạn (Long Short-Term Memory - LSTM) với đầu vào là một vectơ số, biểu diễn chuỗi ký tự của tên miền đầy đủ bao gồm cả tên miền cấp cao nhất (Top Level Domain - TLD) và tên miền cấp hai (Second Level Domain - SLD). Ưu điểm của phương pháp này là không đòi hỏi nhiều bộ nhớ lưu trữ, khối lượng tính toán nhỏ và phù hợp để cài đặt, triển khai và hoạt động trên nhiều dạng máy tính hoặc máy chủ dịch vụ theo thời gian thực.


Bắt đầu
301
Tiền xử lý truy vấn DNS
Tên miền truy vấn
Kết quả phản hồi của truy vấn
302
Tên miền hợp lệ
Đúng
Sai
303
Thiết lập giá trị mặc định cho xác suất hậu nghiệm với
$p(d_i|s_t = Safe) = 1$
$p(d_i|s_t = Infected) = 0$
304
Tính toán xác suất hậu nghiệm $p(d_i|s_t = Safe)$ và $p(d_i|s_t = Infected)$ với bộ phân loại hai lớp dựa trên mạng nơron hồi quy LSTM
305
Cập nhật số NXDOMAIN là kết quả phản hồi của các tên miền khác nhau được truy vấn trong khoảng thời gian ΔT
306
Cập nhật xác suất chuyển trạng thái p
p
307
CSDL
308
Tính xác suất thiết bị an toàn và thiết bị nhiễm mã độc DGA tại thời điểm t
$p(s_t = Safe|D_t)$
$p(s_t = Infected|D_t)$
309
Chuẩn hóa giá trị xác suất
$p(s_t = Safe|D_t)$ và $p(s_t = Infected|D_t)$
$p(s_t = Safe|D_t)$
$p(s_t = Infected|D_t)$
310
$p(s_t = Safe|D_t) <$ Ngưỡng
Sai
Đúng
311
Gửi cảnh báo thiết bị bị nhiễm mã độc DGA đến máy chủ giám sát để ngăn chặn và xử lý
Kết thúc

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực an ninh mạng. Cụ thể, sáng chế đề cập đến phương pháp xác định một thiết bị bị nhiễm mã độc thuật toán sinh tên miền tự động (Domain Generation Algorithm- DGA).

Tình trạng kỹ thuật của sáng chế

Mã độc trong hầu hết các mạng Botnet ngày nay đều sử dụng cơ chế thuật toán sinh tên miền tự động (Domain Generation Algorithm - DGA) để tạo ra một tập tên miền cho việc kết nối với máy chủ điều khiển C&C (Command and Control) nhằm tránh bị phát hiện, ngăn chặn và loại bỏ bởi các hệ thống phát hiện xâm nhập (Intrusion Detection System –IDS)/hệ thống ngăn ngừa xâm nhập (Intrusion Prevention System –IPS).

DGA (Domain Generation Algorithm) là thuật toán sinh tên miền tự động thường được mã độc sử dụng để tạo ngẫu nhiên một số lượng lớn tên miền cho việc kết nối với máy chủ điều khiển C&C nhằm tránh bị phát hiện, ngăn chặn và loại bỏ bởi các hệ thống IDS/IPS. Cụ thể, tập tên miền thay đổi theo thời gian khiến các kỹ thuật như lập danh sách đen (Blacklist) hoặc hệ thống tên miền (Domain Name System – DNS) Sinkhole trở nên kém hiệu quả. Việc dịch ngược mã nguồn cho phép xác định chính xác thuật toán sinh tên miền. Tuy nhiên, việc dịch ngược không phải lúc nào cũng khả thi vì cần mẫu mã độc, trong khi chỉ một thay đổi nhỏ trong mã nguồn cũng có thể khiến quá trình phân tích phải thực hiện lại từ đầu.

Xu hướng hiện nay là xây dựng giải pháp phát hiện tấn công mạng dựa trên dấu hiệu bất thường. Công bố đơn sáng chế Hoa Kỳ số US 2013/0191915 A1 bộc lộ phương pháp phân cụm tên miền sinh bởi mã độc và đề xuất cơ chế phát hiện trên cơ sở đánh giá mức độ tương quan giữa tên miền đầu vào và cụm tên miền đã được tạo ra ở pha huấn luyện. Một số nghiên cứu tiến hành xác định mã độc DGA bằng cách trích chọn đặc trưng thống kê, đặc trưng ngữ nghĩa, đặc trưng cấu trúc hoặc ứng dụng mạng nơron tích chập (Convolutional Neural Networks - CNN), mạng nơron hồi quy bộ nhớ dài ngắn hạn (Long Short-term Memory networks - LSTM) để tìm ra đặc trưng nội hàm, thể hiện mối liên hệ giữa các ký tự trong cùng một tên miền. Mặc dù được tiếp cận theo nhiều hướng khác nhau, nhưng những giải pháp đã đề cập đều chỉ tập trung vào việc phân loại tên miền và dạng mã độc tạo ra tên miền.

Bằng độc quyền sáng chế Hoa Kỳ số US 9,654,484 B2 bộc lộ cơ chế phát hiện thiết bị bị nhiễm mã độc DGA dựa trên thông tin về luồng dữ liệu, sử dụng tỷ số giữa số lượng truy vấn DNS và số lượng địa chỉ IP mà thiết bị kết nối đến thay vì khai thác đặc điểm tên miền sinh ra bởi thuật toán. Công bố đơn sáng chế Hoa Kỳ số US 2016/0057165 A1 đề cập đến việc tính toán đặc trưng độ dài và độ phức tạp về mặt từ vựng của tên miền không tồn tại (Non-Existent Domain - NXDOMAIN). Hệ thống sau đó tìm kiếm tên miền có đặc điểm tương đồng để khoanh vùng và ngăn chặn máy chủ điều khiển C&C. Thiết bị bị nhiễm mã độc được xác định thông qua số lượng NXDOMAIN trả về và khoảng thời gian giữa các NXDOMAIN. Nhược điểm của giải pháp nêu trên là sự phụ thuộc vào đặc trưng cấu trúc và ngữ nghĩa. Việc xác định tên miền độc hại với đặc trưng cấu trúc và ngữ nghĩa thường có độ chính xác không cao, trong khi chúng cũng rất dễ bị tin tặc lợi dụng để vượt qua sự kiểm soát của thiết bị giám sát an ninh mạng.

Nhiều nghiên cứu thực hiện kết luận thiết bị bị nhiễm mã độc DGA dựa trên phân loại tên miền. Ví dụ, cụ thể trong LSTM, ứng với mỗi tên miền đầu vào, LSTM

sẽ đưa ra giá trị xác suất hậu nghiệm là kết quả của quá trình phân loại. Xác suất hậu nghiệm sẽ gồm xác suất tên miền là tên miền bình thường và xác suất tên miền là tên miền do thuật toán sinh ra. Nếu xác suất tên miền là tên miền do thuật toán sinh ra lớn hơn một ngưỡng thì có thể kết luận thiết bị bị nhiễm mã độc DGA. Mặc dù hướng tiếp cận này cho độ chính xác lớn hơn 98%, nhưng khi thử nghiệm thực tế trên dữ liệu lịch sử truy vấn DNS gửi đi từ một thiết bị, hướng tiếp cận này lại không thực sự hiệu quả. Nguyên nhân là do truy vấn DNS từ một thiết bị gửi đi rất đa dạng và chỉ cần một tên miền trong đó bị kết luận sai thì thiết bị sẽ kết luận sai là đã nhiễm mã độc DGA. Vì thế hệ thống thường đưa ra rất nhiều cảnh báo giả.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là đề xuất phương pháp phát hiện thiết bị bị nhiễm mã độc DGA với độ chính xác cao, cụ thể sáng chế mô tả phương pháp phát hiện thiết bị bị nhiễm mã độc DGA, trong đó đề xuất kết hợp kết quả của mô hình phân loại hai lớp và thông tin lịch sử truy vấn tên miền trên cơ sở định lý Bayes, mô hình Markov ẩn (Hidden Markov Model - HMM) và giả định Markov để tăng cường độ chính xác khi đưa ra quyết định. Phương pháp không đòi hỏi nhiều bộ nhớ lưu trữ, có khối lượng tính toán nhỏ và phù hợp để hoạt động trên nhiều dạng máy tính hoặc máy chủ dịch vụ theo thời gian thực.

Để đạt được mục đích trên đây, theo khía cạnh chính, sáng chế đề cập đến phương pháp phát hiện thiết bị bị nhiễm mã độc thuật toán sinh tên miền tự động (Domain Generation Algorithm – DGA), bao gồm các bước sau đây:

thu thập tên miền và kết quả phản hồi của các truy vấn hệ thống tên miền (Domain Name System – DNS) thông qua theo dõi lưu lượng mạng của thiết bị;

xác định xác suất chuyển trạng thái trong mô hình Markov ẩn (Hidden Markov Model – HMM) dựa trên kết quả phản hồi của các truy vấn;

xác định xác suất hậu nghiệm của tên miền bao gồm các bước:

so khớp tên miền với danh sách tên miền hợp lệ,

trường hợp tên miền thuộc danh sách hợp lệ, thiết lập giá trị mặc định cho xác suất hậu nghiệm với $(d_t|s_t = Safe) = 1$ và $p(d_t|s_t = Infected) = 0$,

trường hợp tên miền không thuộc danh sách, giá trị xác suất hậu nghiệm là kết quả đầu ra của bộ phân loại hai lớp dựa trên mạng nơron hồi quy bộ nhớ dài ngắn hạn (Long Short-Term Memory – LSTM) với đầu vào là một vectơ số, biểu diễn chuỗi ký tự của tên miền đầy đủ bao gồm cả tên miền cấp cao nhất (Top Level Domain-TLD) và tên miền cấp hai (Second Level Domain - SLD);

tính toán xác suất thiết bị an toàn và xác suất thiết bị bị nhiễm mã độc DGA trên cơ sở tình trạng của thiết bị ở thời điểm trước đó, xác suất hậu nghiệm và xác suất chuyển trạng thái;

chuẩn hóa sao cho tổng hai giá trị xác suất ở bước tính toán xác suất nêu trên bằng 1;

đưa ra kết luận:

nếu xác suất thiết bị an toàn nhỏ hơn giá trị ngưỡng cho trước, thiết bị được xác định bị nhiễm mã độc DGA; thì gửi cảnh báo đến máy chủ giám sát để ngăn chặn và xử lý,

nếu xác suất thiết bị an toàn lớn hơn hoặc bằng giá trị ngưỡng cho trước, thiết bị được xác định là an toàn, và lưu các giá trị xác suất

vào cơ sở dữ liệu để phục vụ cho quá trình tính toán tiếp theo theo đúng nguyên tắc của thuật toán đệ quy.

Tốt hơn là, danh sách tên miền hợp lệ có thể được định nghĩa dựa trên thống kê của Alexa Internet, Inc. hoặc dựa trên tập tên miền mà người dùng thường xuyên truy cập đến.

Tốt hơn là, xác suất chuyển trạng thái p trong mô hình HMM được xác định dựa trên hàm phân phối tích lũy Poisson hoặc một hàm khác thỏa mãn điều kiện giá trị p tăng cùng với số tên miền không tồn tại (Non-Existent Domain - NXDOMAIN) là kết quả phản hồi của nhiều tên miền không tồn tại khác nhau được truy vấn trong khoảng thời gian ΔT.

Tốt hơn là, ΔT mặc định là 60 phút và có thể thay đổi tùy theo tần suất truy vấn DNS của thiết bị.

Tốt hơn là, bước tính toán xác suất thiết bị an toàn và xác suất thiết bị bị nhiễm mã độc DGA sau khi đã thực hiện t truy vấn trên cơ sở tình trạng của thiết bị ở thời điểm trước đó, xác suất hậu nghiệm và xác suất chuyển trạng thái. Tốt hơn nữa là, quá trình tính toán được thực hiện dựa trên định lý Bayes, mô hình HMM và giả định Markov.

Tốt hơn là, giá trị ngưỡng mặc định là 10^{-5} và có thể thay đổi tùy theo yêu cầu an ninh đối với hệ thống mà phương pháp phát hiện thiết bị bị nhiễm mã độc DGA đã cài đặt, triển khai.

Hiệu quả có lợi của sáng chế

Phương pháp phát hiện thiết bị bị nhiễm mã độc DGA theo sáng chế dựa trên định lý Bayes, mô hình HMM và giả định Markov, trong đó sử dụng kết hợp xác suất chuyển trạng thái, xác suất hậu nghiệm và tình trạng thiết bị ở thời điểm thực

hiện truy vấn tên miền trước đó theo nguyên tắc của thuật toán đệ quy. Xác suất chuyển trạng thái có thể tính toán trên cơ sở số lượng NXDOMAIN là kết quả phản hồi của nhiều tên miền không tồn tại khác nhau được truy vấn trong một khoảng thời gian. Xác suất hậu nghiệm được thiết lập mặc định để giảm khối lượng tính toán nếu tên miền thuộc danh sách tên miền hợp lệ. Trong trường hợp tên miền không nằm trong danh sách, xác suất hậu nghiệm là kết quả của mạng nơron hồi quy LSTM với đầu vào là một vectơ số, biểu diễn chuỗi ký tự của tên miền đầy đủ bao gồm cả tên miền cấp cao nhất (Top Level Domain - TLD) và tên miền cấp hai (Second Level Domain - SLD). Ưu điểm của phương pháp đề xuất là khối lượng tính toán nhỏ, không đòi hỏi nhiều bộ nhớ lưu trữ và phù hợp để cài đặt, triển khai và hoạt động trên nhiều dạng máy tính hoặc máy chủ dịch vụ theo thời gian thực.

Mô tả vắn tắt các hình vẽ

Hình 1 là ví dụ minh họa kiến trúc hệ thống mạng của một cơ quan tổ chức, trong đó phương pháp phát hiện thiết bị bị nhiễm mã độc DGA được tích hợp và triển khai.

Hình 2A và Hình 2B là mô hình HMM (Hidden Markov Model) và mô hình chuyển trạng thái.

Hình 3 là lưu đồ phương pháp phát hiện thiết bị bị nhiễm mã độc DGA.

Mô tả chi tiết sáng chế

Trong bản mô tả sáng chế, thuật ngữ "mã độc DGA" được hiểu là mã độc sử dụng cơ chế thuật toán sinh tên miền tự động (Domain Generation Algorithm - DGA) để tạo ra một tập các chuỗi ký tự có cấu trúc của một tên miền. Mã độc thực hiện

truy vấn đến từng tên miền để tìm ra địa chỉ IP, kết nối và nhận lệnh từ máy chủ điều khiển C&C.

Trong bản mô tả sáng chế, thuật ngữ "thiết bị" được hiểu là máy tính cá nhân của người sử dụng hoặc máy chủ cung cấp dịch vụ trong hệ thống mạng của tổ chức và doanh nghiệp.

Trong bản mô tả sáng chế, thuật ngữ "danh sách tên miền hợp lệ" là tập tên miền do con người tạo ra và được kiểm chứng bởi các tổ chức có uy tín hoặc quản trị viên hệ thống.

Trong bản mô tả sáng chế, thuật ngữ "máy chủ giám sát" được hiểu là máy chủ trên đó cài đặt phần mềm cho phép giám sát, quản lý, đảm bảo an toàn cho hệ thống mạng và hoạt động của các thiết bị trong mạng.

Hình 1 là ví dụ minh họa kiến trúc hệ thống mạng của một cơ quan tổ chức, trong đó phương pháp phát hiện thiết bị bị nhiễm mã độc DGA được tích hợp và triển khai. Máy tính, máy chủ cung cấp dịch vụ (gọi chung là thiết bị) 101 và máy chủ giám sát 105 được kết nối với nhau trong mạng LAN với thiết bị chuyển mạch 107, 108, bộ định tuyến 109 và kết nối mạng Internet thông qua thiết bị modem 111. Tường lửa 110 được dùng để ngăn chặn hệ thống khỏi các nguy cơ tấn công từ bên ngoài.

Trên mỗi thiết bị 101, phương pháp đề xuất có thể được tích hợp dưới dạng phần mềm hoặc phân hệ trong hệ thống ngăn ngừa xâm nhập mạng (Intrusion Prevention System – IPS) 102. Tại đây, toàn bộ lưu lượng DNS được thu thập, phân tích và xử lý. Lưu lượng DNS có thể chia thành một số dạng: (1) truy vấn được gửi đi từ hệ điều hành, trình duyệt và các ứng dụng khác 103, (2) truy vấn sinh ra bởi mã độc DGA 104 (nếu có), và (3) kết quả phản hồi truy vấn nhận được từ hệ thống phân giải tên miền 112. Trên cơ sở định lý Bayes, mô hình HMM và giả định

Markov, phương pháp cho phép phát hiện thiết bị đã bị lây nhiễm mã độc DGA. Trong trường hợp đó, nhiệm vụ của hệ thống IPS 102 là gửi cảnh báo đến máy chủ giám sát 105 để ngăn chặn mã độc phát tán trong mạng. Giải pháp ngăn chặn có thể thực hiện trên tường lửa 110 hoặc trực tiếp đóng cổng kết nối trên thiết bị chuyển mạch 107.

Cũng theo sơ đồ trên Hình 1, truy vấn DNS của các thiết bị trong LAN cũng được phân hệ 106 tại máy chủ giám sát 105 thu thập. Nhiệm vụ của phân hệ 106 là xây dựng mô hình phân loại hai lớp tên miền dựa trên mạng nơron hồi quy LSTM với đầu vào là các vectơ số, biểu diễn chuỗi ký tự của tập tên miền đầy đủ được sử dụng cho mục đích huấn luyện. Tập huấn luyện gồm danh sách tên miền hợp lệ và danh sách tên miền thu thập trong thực tế của mã độc DGA. Danh sách tên miền hợp lệ có thể được định nghĩa dựa trên thống kê của Alexa Internet, Inc. hoặc dựa trên tập tên miền mà người dùng thường xuyên truy cập đến. Cuối cùng, danh sách này cùng với mô hình phân loại hai lớp sẽ được cập nhật về hệ thống IPS 102 để phát hiện thiết bị bị nhiễm mã độc DGA, sẽ được đề cập cụ thể sau đây.

Hình 2A là mô hình HMM (Hidden Markov Model), trong đó $s_t = \{Safe, Infected\}$ minh họa trạng thái của thiết bị tại thời điểm t. $D_t = \{d_1, d_2, \dots, d_t\}$ là chuỗi tên miền thu thập sau mỗi lần truy vấn DNS được gửi đi. Dựa trên định lý Bayes, giả định Markov và một số bước biến đổi đơn giản, xác suất thiết bị an toàn $p(s_t = Safe|D_t)$ và xác suất thiết bị bị nhiễm mã độc DGA $p(s_t = Infected|D_t)$ tại thời điểm t có thể viết dưới dạng:

$$p(s_t = Safe|D_t) \propto p(d_t|s_t = Safe).(1-p).p(s_{t-1} = Safe|D_{t-1}) \quad (1)$$

$$p(s_t = Infected|D_t) \propto p(d_t|s_t = Infected).\{p.p(s_{t-1} = Safe|D_{t-1}) + p(s_{t-1} = Infected|D_{t-1})\} \quad (2)$$

Trong đó, $p(d_t|s_t = Safe)$ và $p(d_t|s_t = Infected)$ là xác suất hậu nghiệm của tên miền d_t, $p(s_{t-1} = Safe|D_{t-1})$ và $p(s_{t-1} = Infected|D_{t-1})$ mô tả tình trạng của thiết bị sau khi đã thực hiện $t-1$ truy vấn DNS, p theo Hình 2B được hiểu là xác suất chuyển trạng thái từ $s_{t-1} = Safe$ sang $s_t = Infected$. Có thể thấy, việc tính toán thực hiện theo nguyên tắc của thuật toán đệ quy trong đó cần giả định thiết bị ở tình trạng an toàn tại thời điểm $t = 0$, có nghĩa $p(s_0 = Safe|D_0) = 1$ và $p(s_0 = Infected|D_0) = 0$.

Ý nghĩa ký hiệu $\propto$ trong biểu thức (1) và (2) là ký hiệu tỷ lệ thuận (proportional to). Biểu thức (1) và (2) sẽ được hiểu là xác suất một thiết bị là an toàn và xác suất thiết bị bị nhiễm mã độc DGA sau khi quan sát thiết bị thực hiện một chuỗi D_t các truy vấn DNS hay xác suất trạng thái của thiết bị tại thời điểm t tỷ lệ thuận với tích các xác suất bao gồm xác suất hậu nghiệm của tên miền d_t, xác suất chuyển trạng thái của thiết bị và xác suất tình trạng của thiết bị tại thời điểm $t-1$ trước đó.

Phát triển từ biểu thức (1) và (2), thu được phương pháp phát hiện thiết bị bị nhiễm mã độc DGA, bao gồm các bước sau đây:

Viện dẫn Hình 3 là lưu đồ chi tiết của phương pháp đề xuất, trong đó bước 301 tiến hành tiền xử lý, phân tích và trích xuất tên miền cũng như kết quả phản hồi truy vấn từ lưu lượng DNS thu thập được trên thiết bị. Dữ liệu tên miền sẽ được lần lượt đưa qua các bước 302, 303 và 304 để xác định giá trị xác suất hậu nghiệm. Cụ thể, bước 302 thực hiện so khớp tên miền với danh sách tên miền hợp lệ nhằm giảm khối lượng tính toán và tăng độ chính xác của phương pháp đề xuất. Trong thực tế,

danh sách tên miền hợp lệ có thể được định nghĩa dựa trên thống kê của Alexa Internet, Inc. hoặc dựa trên tập tên miền mà người dùng thường xuyên truy cập đến. Trường hợp tên miền thuộc danh sách hợp lệ, bước 303 thiết lập giá trị mặc định cho xác suất hậu nghiệm với $(d_t|s_t = Safe) = 1$ và $p(d_t|s_t = Infected) = 0$. Trường hợp tên miền không thuộc danh sách, giá trị xác suất hậu nghiệm là kết quả đầu ra của bộ phân loại hai lớp dựa trên mạng nơron hồi quy LSTM với đầu vào là một vectơ số, biểu diễn chuỗi ký tự của tên miền đầy đủ bao gồm cả tên miền cấp cao nhất TLD và tên miền cấp hai SLD (bước 304).

Dữ liệu kết quả truy vấn được lần lượt đưa qua bước 305, 306 để xác định xác suất chuyển trạng thái p trong mô hình HMM như minh họa trên Hình 2B. Bản chất của mã độc DGA khi hoạt động sẽ tạo ra số lượng lớn NXDOMAIN. Vì vậy, trong bản mô tả sáng chế, xác suất chuyển trạng thái được xác định dựa trên hàm phân phối tích lũy Poisson hoặc một hàm khác thỏa mãn điều kiện giá trị p tăng cùng với số NXDOMAIN là kết quả phản hồi của nhiều tên miền không tồn tại khác nhau được truy vấn trong khoảng thời gian ΔT. ΔT mặc định là 60 phút và có thể thay đổi tùy theo tần suất truy vấn DNS của thiết bị. Theo lưu đồ trên Hình 3, xác suất chuyển trạng thái được cập nhật vào cơ sở dữ liệu (bước 307).

Bước 308 tính toán xác suất thiết bị an toàn và xác suất thiết bị bị nhiễm mã độc sau khi đã thực hiện t truy vấn trên cơ sở tình trạng của thiết bị ở thời điểm trước đó, xác suất hậu nghiệm và xác suất chuyển trạng thái, như được minh họa tại biểu thức (1) và (2). Như đã đề cập, quá trình tính toán dựa trên định lý Bayes, mô hình HMM và giả định Markov.

Sau đó, bước 309 tiến hành chuẩn hóa sao cho tổng hai giá trị xác suất thu được ở bước 308 bằng 1. Cuối cùng, giá trị này cũng được lưu vào cơ sở dữ liệu 307 để phục vụ cho quá trình tính toán tiếp theo theo đúng nguyên tắc của thuật toán đệ quy.

Tại bước 310, nếu xác suất thiết bị an toàn nhỏ hơn giá trị ngưỡng cho trước, thiết bị được xác định bị nhiễm mã độc DGA. Bước 311 thực hiện gửi cảnh báo đến máy chủ giám sát để ngăn chặn và xử lý. Giá trị ngưỡng mặc định là 10^{-5} và có thể thay đổi tùy theo yêu cầu an ninh đối với hệ thống mà phương pháp phát hiện thiết bị bị nhiễm mã độc DGA đã cài đặt, triển khai.

Trong khi sáng chế đã được mô tả chi tiết ở các phương án làm ví dụ, cần hiểu rằng sáng chế không bị giới hạn bởi các phương án đó. Đúng ra là, sáng chế được dự định để bao hàm các biến thể khác nhau được bao gồm trong phạm vi nội dung diễn dịch theo nghĩa rộng nhất của sáng chế để bao vây toàn bộ các biến thể tương đương như vậy.

YÊU CẦU BẢO HỘ

1. Phương pháp phát hiện thiết bị bị nhiễm mã độc thuật toán sinh tên miền tự động (Domain Generation Algorithm – DGA), bao gồm các bước sau đây:

bước (301): thu thập tên miền và kết quả phản hồi của các truy vấn hệ thống tên miền (Domain Name System – DNS) thông qua theo dõi lưu lượng mạng của thiết bị;

bước (306): xác định xác suất chuyển trạng thái trong mô hình Markov ẩn (Hidden Markov Model – HMM) dựa trên kết quả phản hồi của các truy vấn;

bước (304): xác định xác suất hậu nghiệm của tên miền bao gồm các bước:

so khớp tên miền với danh sách tên miền hợp lệ,

trường hợp tên miền thuộc danh sách hợp lệ, thiết lập giá trị mặc định cho xác suất hậu nghiệm với $(d_t|s_t = Safe) = 1$ và $p(d_t|s_t = Infected) = 0$,

trường hợp tên miền không thuộc danh sách, giá trị xác suất hậu nghiệm là kết quả đầu ra của bộ phân loại hai lớp dựa trên mạng nơron hồi quy bộ nhớ dài ngắn hạn (Long Short-Term Memory – LSTM) với đầu vào là một vectơ số, biểu diễn chuỗi ký tự của tên miền đầy đủ bao gồm cả tên miền cấp cao nhất (Top Level Domain-TLD) và tên miền cấp hai (Second Level Domain - SLD);

bước (308): tính toán xác suất thiết bị an toàn và xác suất thiết bị bị nhiễm mã độc DGA trên cơ sở tình trạng của thiết bị ở thời điểm trước đó, xác suất hậu nghiệm và xác suất chuyển trạng thái;

bước (309): chuẩn hóa sao cho tổng hai giá trị xác suất ở bước (308) bằng 1;

bước (310): đưa ra kết luận,

nếu xác suất thiết bị an toàn nhỏ hơn giá trị ngưỡng cho trước, thiết bị được xác định bị nhiễm mã độc DGA; thì gửi cảnh báo đến máy chủ giám sát để ngăn chặn và xử lý,

nếu xác suất thiết bị an toàn lớn hơn hoặc bằng giá trị ngưỡng cho trước, thiết bị được xác định là an toàn, và lưu các giá trị xác suất vào cơ sở dữ liệu để phục vụ cho quá trình tính toán tiếp theo theo đúng nguyên tắc của thuật toán đệ quy.

2. Phương pháp theo điểm 1, trong đó danh sách tên miền hợp lệ có thể được định nghĩa dựa trên thống kê của Alexa Internet, Inc. hoặc dựa trên tập tên miền mà người dùng thường xuyên truy cập đến.

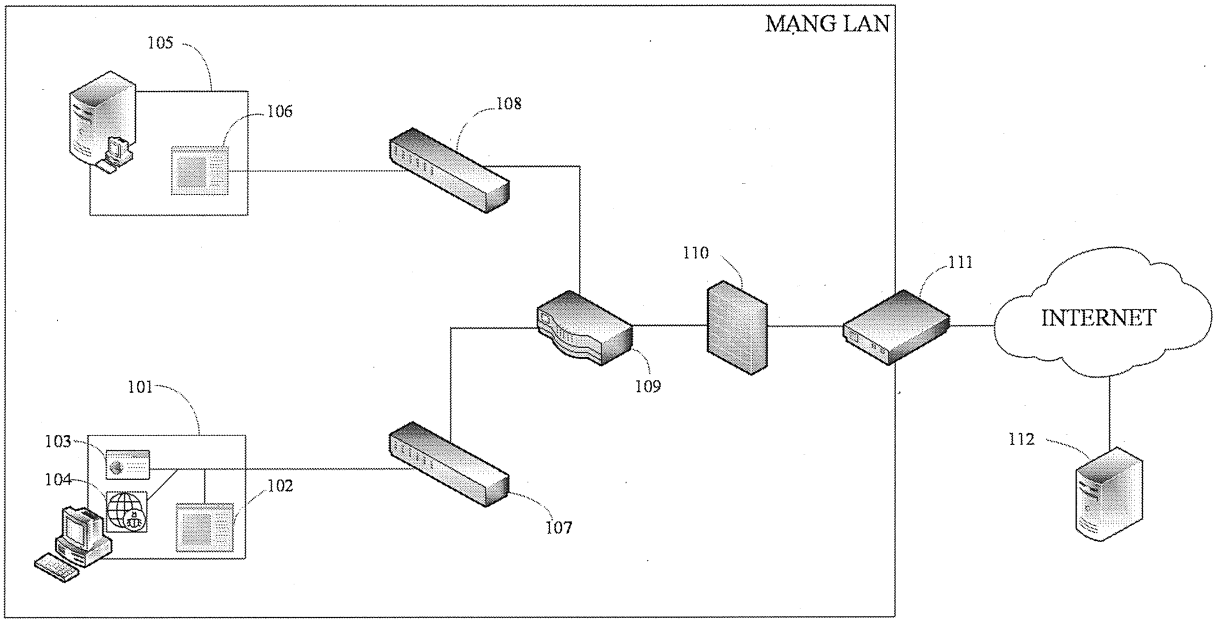
3. Phương pháp theo điểm 1 hoặc 2, trong đó xác suất chuyển trạng thái p trong mô hình HMM được xác định dựa trên hàm phân phối tích lũy Poisson hoặc một hàm khác thỏa mãn điều kiện giá trị p tăng cùng với số NXDOMAIN là kết quả phản hồi của nhiều tên miền không tồn tại khác nhau được truy vấn trong khoảng thời gian ΔT.

4. Phương pháp theo điểm 3, trong đó ΔT mặc định là 60 phút và có thể thay đổi tùy theo tần suất truy vấn DNS của thiết bị.

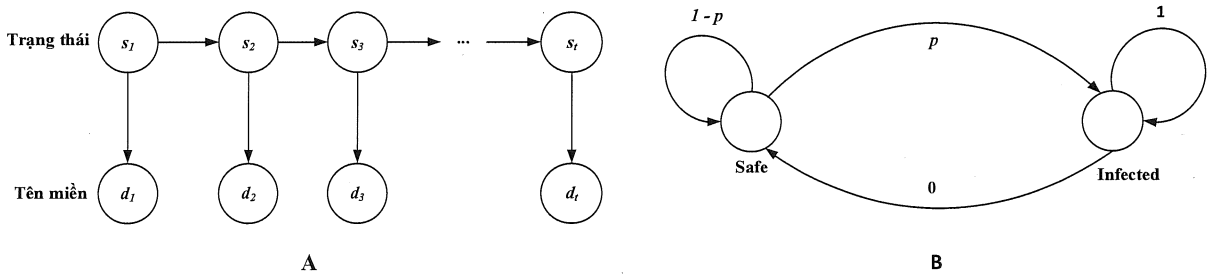
5. Phương pháp theo điểm 1, trong đó bước tính toán xác suất thiết bị an toàn và xác suất thiết bị bị nhiễm mã độc DGA được thực hiện sau khi đã thực hiện t truy vấn trên cơ sở tình trạng của thiết bị ở thời điểm trước đó, xác suất hậu nghiệm và xác suất chuyển trạng thái.

6. Phương pháp theo điểm 5, trong đó quá trình tính toán được thực hiện dựa trên định lý Bayes, mô hình HMM và giả định Markov.

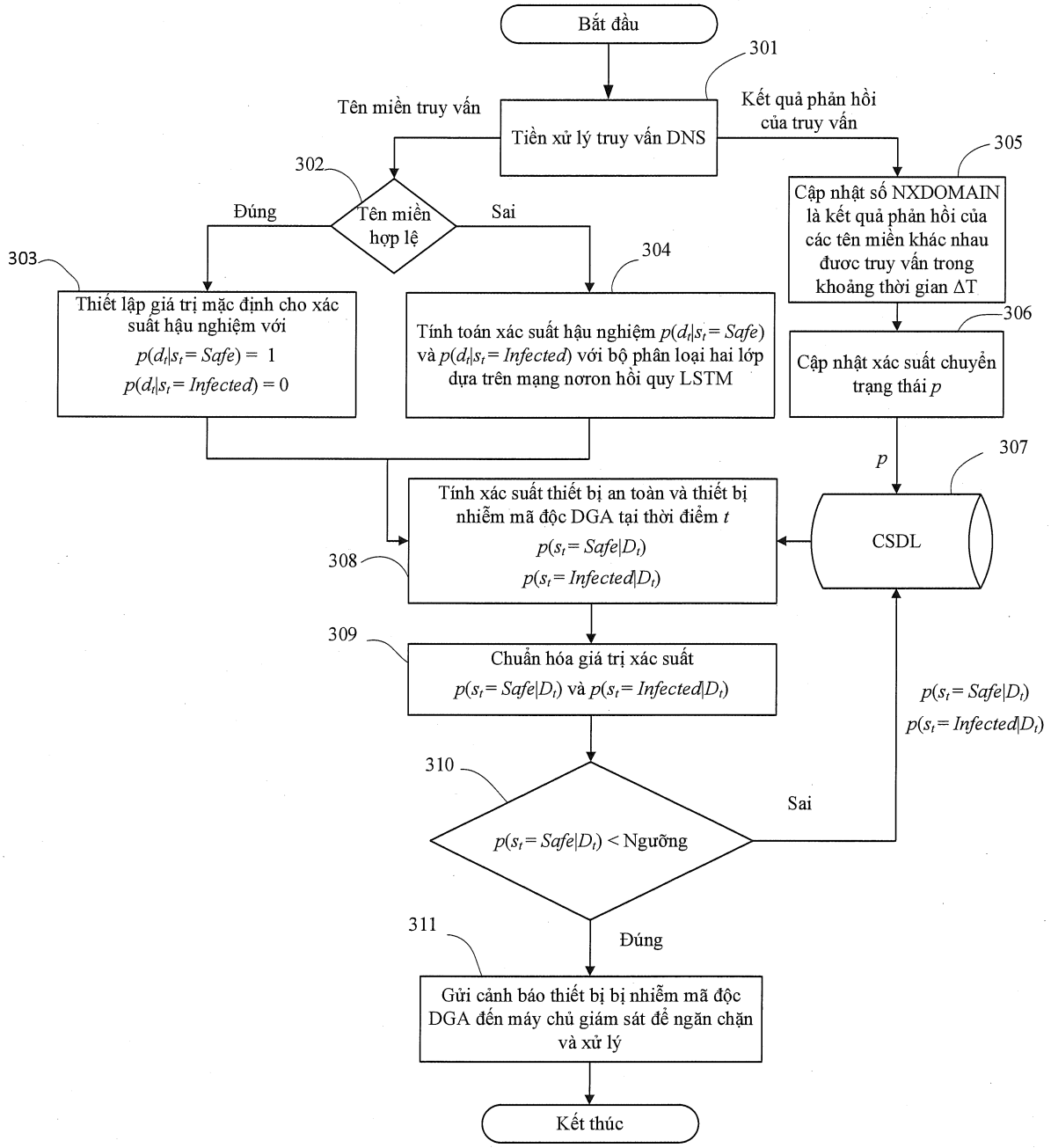
7. Phương pháp theo điểm 1, trong đó giá trị ngưỡng mặc định là 10^{-5} và có thể thay đổi tùy theo yêu cầu an ninh đối với hệ thống mà phương pháp phát hiện thiết bị bị nhiễm mã độc DGA đã cài đặt, triển khai.


MẠNG LAN
105
106
108
110
111
INTERNET
109
101
103
104
102
107
112

HÌNH 1


Trạng thái
s_1
s_2
s_3
...
s_t
Tên miền
d_1
d_2
d_3
d_t
A
1 - p
p
1
Safe
Infected
0
B

HÌNH 2


Bắt đầu
301
Tên miền truy vấn
Tiền xử lý truy vấn DNS
Kết quả phản hồi của truy vấn
305
302
Đúng
Tên miền hợp lệ
Sai
Cập nhật số NXDOMAIN là kết quả phản hồi của các tên miền khác nhau được truy vấn trong khoảng thời gian ΔT
303
304
306
Thiết lập giá trị mặc định cho xác suất hậu nghiệm với
$p(d_t|s_t = Safe) = 1$
$p(d_t|s_t = Infected) = 0$
Tính toán xác suất hậu nghiệm $p(d_t|s_t = Safe)$ và $p(d_t|s_t = Infected)$ với bộ phân loại hai lớp dựa trên mạng nơron hồi quy LSTM
Cập nhật xác suất chuyển trạng thái p
p
307
Tính xác suất thiết bị an toàn và thiết bị nhiễm mã độc DGA tại thời điểm t
$p(s_t = Safe|D_t)$
$p(s_t = Infected|D_t)$
CSDL
308
309
Chuẩn hóa giá trị xác suất
$p(s_t = Safe|D_t)$ và $p(s_t = Infected|D_t)$
$p(s_t = Safe|D_t)$
$p(s_t = Infected|D_t)$
310
Sai
$p(s_t = Safe|D_t) <$ Ngưỡng
311
Đúng
Gửi cảnh báo thiết bị bị nhiễm mã độc DGA đến máy chủ giám sát để ngăn chặn và xử lý
Kết thúc

HÌNH 3