DOI: 10.15625/vap.2016.00061

MỘT TIẾP CẬN MÁY HỌC ĐỂ PHÂN LỚP CÁC KIỂU TẤN CÔNG TRONG HỆ THỐNG PHÁT HIỆN XÂM NHẬP MẠNG

Hoàng Ngọc Thanh[1, 3], Trần Văn Lăng[2, *], Hoàng Tùng[4]

[1]Trường Đại học Lạc Hồng
[2]Viện Cơ học và Tin học ứng dụng, VAST
[3]Khoa Công nghệ thông tin, Trường Đại học Bà Rịa - Vũng Tàu
[4]Trung tâm Tin học, Trường Đại học Nguyễn Tất Thành

thanhhn@bvu.edu.vn, langtv@vast.vn, htung@ntt.edu.vn

TÓM TẮT *— Chức năng chính của hệ thống phát hiện xâm nhập mạng (Intrusion Detection System: IDS) là để bảo vệ hệ thống, phân tích và dự báo hành vi truy cập mạng của người sử dụng. Những hành vi này được xem xét là bình thường hoặc một cuộc tấn công. Các IDS ngoài việc xác định một hành vi là bình thường hoặc một cuộc tấn công dựa trên các mẫu đã lưu trữ, còn có khả năng học để nhận dạng các cuộc tấn công mới. Với mỗi kiểu tấn công cụ thể là DoS, Probe, R2L hoặc U2R, tập dữ liệu mẫu có các tính chất đặc thù. Bài viết này đề cập đến việc tìm kiếm kỹ thuật máy học tối ưu phù hợp với mỗi kiểu tấn công dựa trên các thuật toán máy học đã biết như: cây quyết định, K láng giềng gần nhất, máy vectơ hỗ trợ (SVM), mạng nơron nhân tạo,... Từ đó, xây dựng một bộ phân lớp lai đa tầng trên cơ sở sử dụng các kỹ thuật máy học tối ưu phù hợp với mỗi kiểu tấn công ở mỗi tầng. Kết quả thí nghiệm trên tập dữ liệu KDD99 sử dụng đánh giá chéo 5-fold cho thấy, bộ phân lớp lai đa tầng kết hợp các kỹ thuật máy học: cây quyết định, mạng nơron nhân tạo và SVM có độ chính xác dự báo cao nhất: 99.83% khi phân lớp các truy cập bình thường và 99.58% khi phân lớp các kiểu tấn công.*

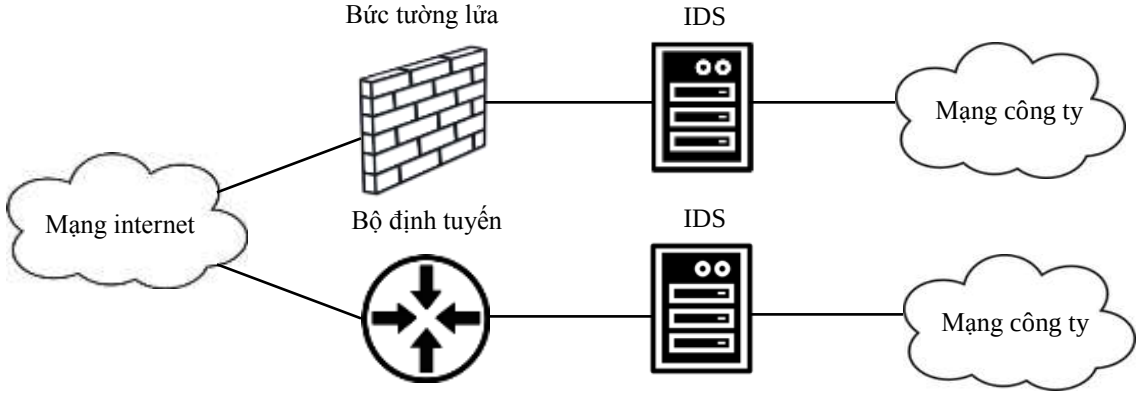
Từ khóa *— Máy học, IDS, an ninh mạng.*

I. GIỚI THIỆU

Trong cuộc sống hiện đại, internet là một trong những yếu tố quan trọng thúc đẩy sự phát triển của các tổ chức, doanh nghiệp. Tuy nhiên, có khá nhiều rủi ro khi sử dụng internet xuất phát từ các cuộc tấn công mạng. Vì vậy, các hệ thống phát hiện xâm nhập (Intrusion Detection System - IDS) khác nhau đã được thiết kế và xây dựng nhằm ngăn chặn các cuộc tấn công này. Mục tiêu của IDS là để cung cấp một bức tường bảo vệ, giúp các hệ thống mạng có khả năng chống lại các cuộc tấn công từ internet. Các IDS có thể được sử dụng để phát hiện việc sử dụng các loại truyền thông mạng và hệ thống máy tính độc hại, nhiệm vụ mà các bức tường lửa quy ước không thể thực hiện được. Việc phát hiện xâm nhập dựa trên giả thiết là hành vi của kẻ xâm nhập khác với người sử dụng hợp lệ [1]. Hình 1 mô tả các vị trí điển hình của IDS trong một hệ thống mạng. Ở đó, các bít dữ liệu vào ra giữa internet và mạng của tổ chức, doanh nghiệp được các IDS bắt, xử lý và phân lớp để xác định đó là một truy cập bình thường hoặc một cuộc tấn công; từ đó có các cảnh báo, hành động phù hợp.

Các IDS được chia thành hai loại: IDS dựa trên dấu hiệu (misuse-based) và IDS dựa trên sự bất thường (anomaly-based) [2]. Việc phân lớp căn cứ vào cách tiếp cận phát hiện xâm nhập.

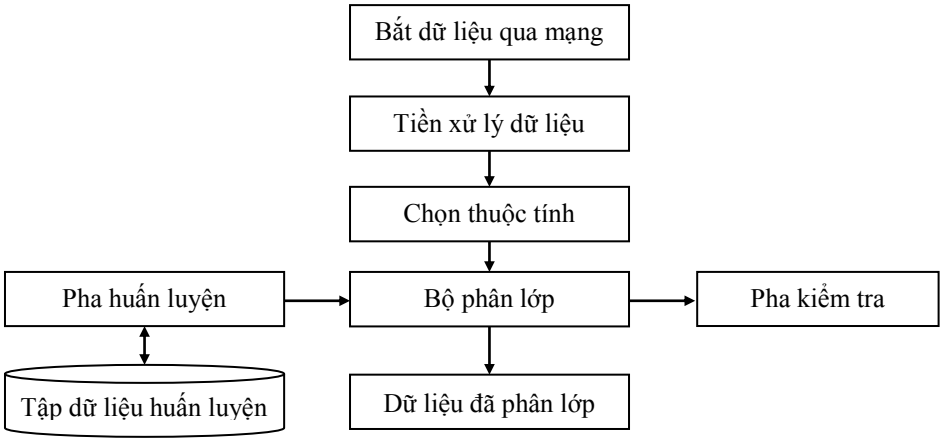
IDS dựa trên dấu hiệu sử dụng mẫu của các cuộc tấn công đã biết hoặc điểm yếu của hệ thống để xác định xâm nhập, tương tự như các phần mềm chống virus sử dụng mẫu để phát hiện virus. Yếu điểm của kỹ thuật này là không thể phát hiện các mẫu tấn công mới, nên nó cần phải cập nhật liên tục các dấu hiệu tấn công để nhận dạng các cuộc tấn công mới.



Hình 1. Vị trí của IDS trong một hệ thống mạng

IDS dựa trên sự bất thường cố gắng xác định độ lệch so với các mẫu sử dụng thông thường đã được thiết lập trước để đánh dấu các xâm nhập. Vì vậy, các IDS dựa trên sự bất thường cần quen với các mẫu sử dụng thông thường thông qua việc học. Các kỹ thuật máy học khác nhau đã được sử dụng rộng rãi để phục vụ cho mục đích này. Hình 2 mô tả kiến trúc của một IDS sử dụng kỹ thuật máy học [3]. Ở đó, chuỗi bít bắt được, sau khi qua các công đoạn tiền xử

lý, chọn lựa thuộc tính sẽ được phân lớp bởi các bộ phân lớp (classifier) đã được huấn luyện. Việc huấn luyện các bộ phân lớp được thực hiện qua pha huấn luyện và kiểm tra với tập dữ liệu huấn luyện đã lưu trữ.



Hình 2. Kiến trúc của một IDS

Có nhiều kỹ thuật học khác nhau đã được các học giả đề xuất sử dụng khi xây dựng các bộ phân lớp. Bài viết này đề cập đến việc xây dựng một bộ phân lớp lai đa tầng, trên cơ sở sử dụng các bộ phân lớp thành phần tối ưu phù hợp nhất với từng kiểu tấn công ở mỗi tầng. Nội dung bài viết gồm 6 phần: phần I giới thiệu, phần III trình bày chi tiết về các kiểu tấn công mạng. Do tính chất đặc thù của mỗi kiểu tấn công, các kỹ thuật máy học tối ưu phù hợp nhất trình bày ở phần II được lựa chọn khi xây dựng các bộ phân lớp thành phần theo các tiêu chí đánh giá được trình bày ở phần IV. Từ đó, kiến trúc một bộ phân lớp lai đa tầng được đề nghị, cũng như các kết quả thí nghiệm được trình bày ở phần V. Phần VI tóm tắt những kết quả đạt được, đồng thời cũng đưa ra các tồn tại cần được tiếp tục nghiên cứu trong thời gian tới.

II. CÁC KỸ THUẬT MÁY HỌC DÙNG TRONG BỘ PHÂN LỚP LAI ĐA TẦNG

Phần dưới đây mô tả tóm tắt các kỹ thuật máy học tối ưu phù hợp nhất với mỗi kiểu tấn công, được lựa chọn khi xây dựng các bộ phân lớp thành phần trong kiến trúc bộ phân lớp lai đa tầng, được đề xuất sử dụng để phân lớp các kiểu tấn công trong IDS.

A. Máy vectơ hỗ trợ

Máy vectơ hỗ trợ (SVM) là một giải thuật máy học dựa trên lý thuyết học thống kê do Vapnik (1998) đề xuất. Bài toán cơ bản của SVM là bài toán phân lớp loại 2 lớp: Cho trước n điểm trong không gian d chiều (mỗi điểm thuộc vào một lớp ký hiệu là +1 hoặc -1, mục đích của giải thuật SVM là tìm một siêu phẳng (hyperplane) phân hoạch tối ưu cho phép chia các điểm này thành hai phần sao cho các điểm cùng một lớp nằm về một phía với siêu phẳng này.

Xét tập dữ liệu mẫu có thể tách rời tuyến tính $\{(x_1, y_1), (x_2, y_2), ..., (x_n, y_n)\}$ với $x_i \in R^d$ và $y_i \in \{\pm 1\}$. Siêu phẳng tối ưu phân tập dữ liệu này thành hai lớp là siêu phẳng có thể tách rời dữ liệu thành hai lớp riêng biệt với lề (margin) lớn nhất. Tức là, cần tìm siêu phẳng H: $y = w.x + b = 0$ và hai siêu phẳng H_1, H_2 hỗ trợ song song với H và có cùng khoảng cách đến H. Với điều kiện không có phần tử nào của tập mẫu nằm giữa H_1 và H_2, khi đó:

$w.x + b \geq +1$ với y = +1 và $w.x + b \leq -1$ với $y = -1$, kết hợp ta có $y(w.x + b) \geq 1$.

Khoảng cách của siêu phẳng H_1 và H_2 đến H là: $||w|| = \sqrt{w_1^2 + w_2^2 + \cdots + w_n^2}$

Ta cần tìm siêu phẳng H với lề lớn nhất, tức là giải bài toán tối ưu tìm $\min_{w,b} ||w||$ với ràng buộc $y(w.x + b) \geq 1$. Từ đó giải để tìm được các giá trị tối ưu cho w, b. Về sau, việc phân loại một mẫu mới chỉ là việc kiểm tra hàm dấu $\text{sign}(w.x + b)$.

Lời giải tìm siêu phẳng tối ưu trên có thể mở rộng trong trường hợp dữ liệu không thể tách rời tuyến tính bằng cách ánh xạ dữ liệu vào một không gian có số chiều lớn hơn, qua việc sử dụng một hàm nhân (kernel) như: Polynomial, Laplacian, Sigmoid, Gaussian (GRBF),…

Cho đến nay đã có nhiều cải tiến, biến thể của SVM với mục đích nâng cao hiệu quả phân lớp của các IDS [7, 8, 9, 10, 11, 12, 13, 14].

B. Mạng nơron nhân tạo

Là mô hình xử lý thông tin mô phỏng hoạt động của hệ thống thần kinh sinh vật, bao gồm số lượng lớn các nơron được gắn kết để xử lý thông tin. ANN giống như bộ não con người, được học bởi kinh nghiệm (qua huấn luyện), có khả năng lưu giữ những kinh nghiệm hiểu biết (tri thức) và sử dụng những tri thức đó trong việc dự đoán các dữ liệu chưa biết.

ANN được huấn luyện hay được học theo 2 kỹ thuật cơ bản là học có giám sát và học không giám sát.

- Học có giám sát: quá trình huấn luyện được lặp lại cho đến khi kết quả (output) của ANN đạt được giá trị mong muốn đã biết. Điển hình cho kỹ thuật này là mạng nơron lan truyền ngược (back-propagation).

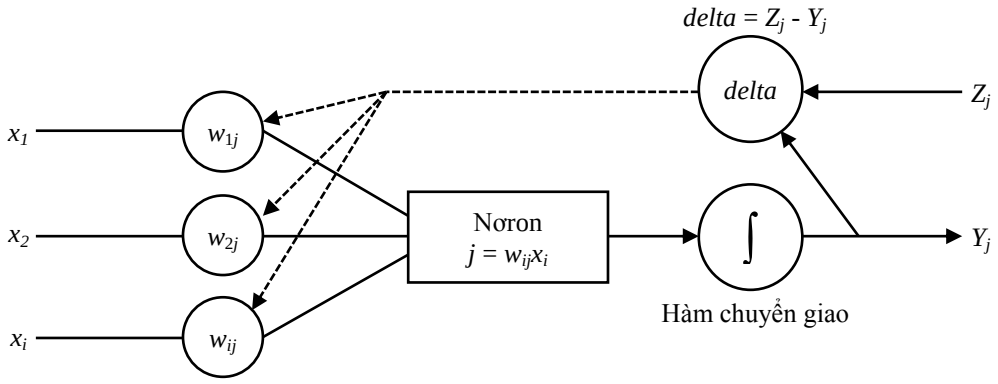
- Học không giám sát: không sử dụng tri thức bên ngoài trong quá trình học, nên còn gọi là tự tổ chức (Self - Organizing). Mạng nơron điển hình được huấn luyện theo kiểu không giám sát là SOM.

Quá trình học có giám sát của ANN được mô tả như ở Hình 3, gồm các bước:

1. Tính giá trị output *Y*.

2. So sánh *Y* với giá trị mong muốn *Z*.

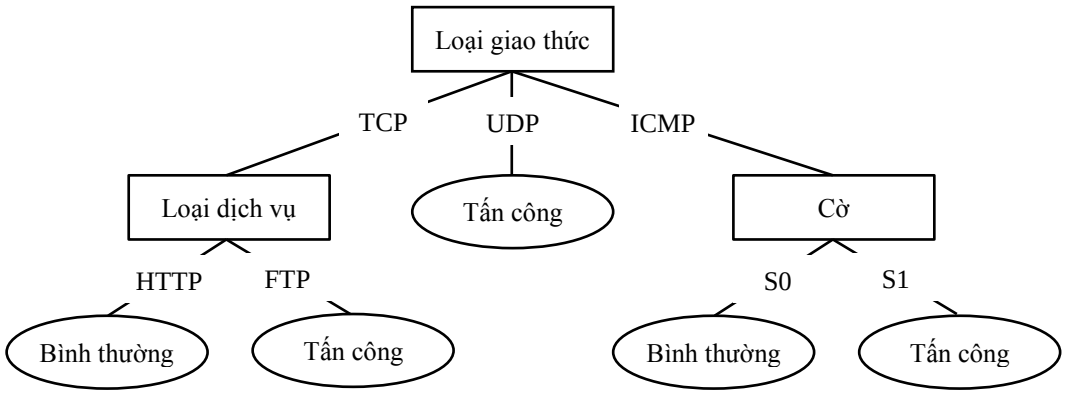
3. Nếu chưa đạt giá trị mong muốn (*delta* = *Z* - *Y* lớn) thì chỉnh trọng số (weights) và tính lại output cho đến khi *delta* = 0 hoặc nhỏ đến mức chấp nhận được.



Hình 3. Giảm thiểu *delta* bằng cách chỉnh trọng số

C. Cây quyết định

Với những ưu điểm của mình, DT được đánh giá là một công cụ mạnh, phổ biến và đặc biệt thích hợp cho data mining nói chung và phân lớp dữ liệu nói riêng [10]. Ngoài những ưu điểm như: xây dựng tương đối nhanh, đơn giản. DT dễ dàng được chuyển đổi sang các câu lệnh SQL được sử dụng để truy nhập cơ sở dữ liệu một cách hiệu quả. Cuối cùng, việc phân lớp dựa trên DT đạt được sự tương tự, đôi khi là chính xác hơn so với các phương pháp phân lớp khác.



Hình 4. Cây quyết định

Biểu đồ phát triển hình cây của DT được minh họa như ở Hình 4, gồm:

- Gốc: là node trên cùng của cây;

- Node trong: biểu diễn một kiểm tra trên một thuộc tính đơn;

- Nhánh: biểu diễn các kết quả của kiểm tra trên node trong;

- Node lá: biểu diễn lớp.

Để phân lớp mẫu dữ liệu chưa biết, giá trị các thuộc tính của mẫu được đưa vào kiểm tra trên DT. Mỗi mẫu tương ứng có một đường đi từ gốc đến lá và lá biểu diễn dự đoán giá trị phân lớp của mẫu đó.

III. TẬP DỮ LIỆU (DATA SET)

Trước khi các bộ phân lớp được đưa vào sử dụng để phát hiện xâm nhập mạng, các bộ phân lớp phải trải qua quá trình huấn luyện và kiểm tra, việc huấn luyện và kiểm tra được thực hiện trên tập dữ liệu đã được gán nhãn trước.

Theo thống kê [16], tập dữ liệu được sử dụng phổ biến nhất trong các thí nghiệm cho đến nay là KDD99, được tạo ra bằng cách xử lý phần dữ liệu TCPDUMP lấy được trong 7 tuần từ hệ thống phát hiện xâm nhập DARPA 1998. KDD99 gồm các tập dữ liệu huấn luyện và kiểm tra. Tập dữ liệu huấn luyện có 4.898.431 vectơ kết nối đơn, mỗi vectơ có 41 thuộc tính (loại giao thức, dịch vụ và cờ) và được dán nhãn là bình thường hoặc một cuộc tấn công một cách chính xác với một kiểu tấn công cụ thể [17]. Tập dữ liệu huấn luyện chứa 22 kiểu tấn công và thêm 17 kiểu trong tập dữ liệu kiểm tra, được phân thành 4 nhóm:

(1) Denial of Service (DoS), gồm các kiểu tấn công như: Neptune, Smurf, Pod, Teardrop. Ở đó, kẻ tấn công làm cho các tài nguyên tính toán hoặc bộ nhớ quá tải để xử lý các yêu cầu hợp lệ, hoặc từ chối người dùng hợp lệ truy cập máy.

(2) Remote to Local (R2L), gồm các kiểu tấn công như: Guess-password, Ftp-write, Imap và Phf. Ở đó, kẻ tấn công tuy không có tài khoản nhưng có khả năng gửi các gói tin đến một máy qua mạng, sẽ khai thác một số lỗ hổng để đạt được quyền truy cập cục bộ như là người sử dụng của máy đó.

(3) User to Root (U2R), gồm các kiểu tấn công như: Buffer-overflow, Load-module, Perl và Spy. Ở đó, kẻ tấn công bắt đầu với một quyền truy cập bình thường và sau đó khai thác một số lỗ hổng để đạt được quyền truy cập root trên hệ thống.

(4) Probe, gồm các kiểu tấn công như: Port-sweep, IP-sweep và Nmap. Ở đó, kẻ tấn công nỗ lực thu thập thông tin về mạng máy tính nhằm phá vỡ khả năng kiểm soát an ninh của nó.

Thông tin chi tiết về mỗi kiểu tấn công trong tập dữ liệu KDD99 được mô tả trong Bảng 1.

Bảng 1. Thông tin chi tiết các tập dữ liệu huấn luyện và kiểm tra trong KDD99

Tập dữ liệu huấn luyện		
Kiểu tấn công	**Số mẫu**	**Tỷ lệ %**
Normal	972.781	19,860
DoS	3.883.370	79,280
Probe	41.102	0,840
R2L	1.126	0,023
U2R	52	0,001

Tập dữ liệu kiểm tra		
Kiểu tấn công	**Số mẫu**	**Tỷ lệ %**
Normal	60.593	19,48
DoS	229.853	73,90
Probe	4.166	1,34
R2L	16.374	5,26
U2R	70	0,02

IV. CÁC CHỈ SỐ ĐÁNH GIÁ

Nếu **FP** là số mẫu bị phân lớp sai là dương tính; **TP** là số mẫu được phân lớp đúng là dương tính; **FN** là số mẫu bị phân lớp sai là âm tính; **TN** là số mẫu được phân lớp đúng là âm tính. Việc đánh giá hiệu năng của các IDS được thực hiện qua việc đo và so sánh các chỉ số:

- Accuracy = (TP + TN) / (TP + FP + TN + FN)

- Sensitivity = R = TPR = TP / (TP + FN)

- Specificity = TNR = TN / (TN + FP)

- Efficiency = (Sensitivity + Specificity) / 2

- Độ chính xác cảnh báo: Precise = P = TP / (TP + FP)

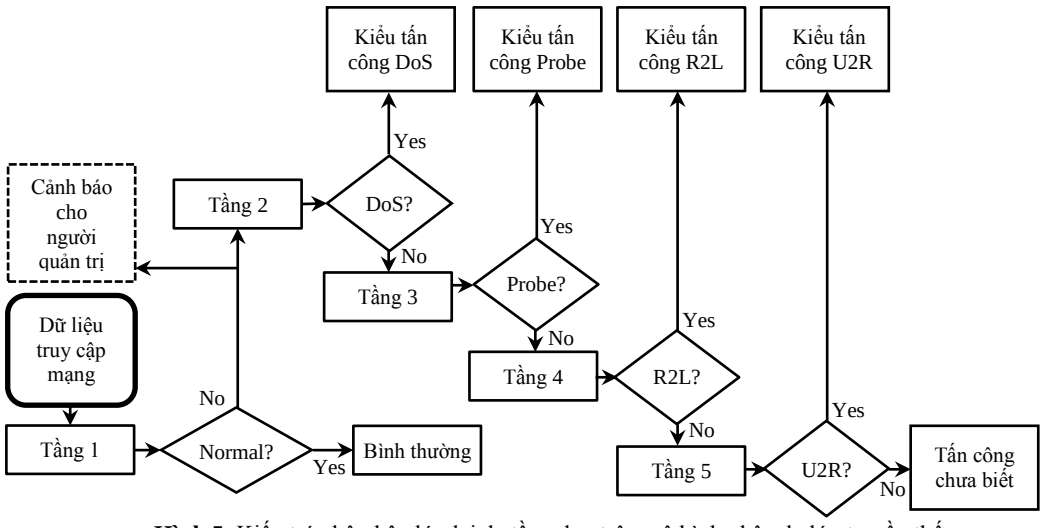
- Thời gian huấn luyện và kiểm tra.

Có nhiều kỹ thuật đánh giá độ chính xác dự báo như: đánh giá chéo K-fold, Holdout, Re-substitution và Leave-one-out [11]. Trong đó, đánh giá chéo K-fold được xem là hiệu quả, phù hợp với các IDS. Theo đó, các bản ghi được phân ngẫu nhiên thành *k* tập con; một tập con được chỉ định là tập dữ liệu kiểm tra và các tập con còn lại được xử lý như tập dữ liệu huấn luyện. Sau đó, quá trình đánh giá chéo lặp lại *k* lần, cũng như độ chính xác phân lớp có thể được kiểm tra thông qua các độ chính xác phân lớp trung bình từ *k* lần đánh giá. Đánh giá chéo K-fold đặc biệt phù hợp với nguồn dữ liệu huấn luyện lớn, trái với đánh giá Leave-one-out, tốn nhiều thời gian để thực hiện, gây trở ngại do thời gian đào tạo lớn.

V. KIẾN TRÚC BỘ PHÂN LỚP LAI ĐA TẦNG VÀ KẾT QUẢ THÍ NGHIỆM

Để phân lớp dữ liệu mạng bắt được thành các lớp ứng với từng kiểu tấn công cụ thể. Kiến trúc của bộ phân lớp lai đa tầng dựa trên mô hình phân đa lớp truyền thống One-Versus-Rest (OVR) được đề xuất như mô tả ở Hình 5.

Theo đó, dữ liệu truy cập mạng được đưa vào tầng 1 để phân lớp là bình thường hoặc một cuộc tấn công, nếu truy cập là một cuộc tấn công, hệ thống sẽ cảnh báo cho người quản trị, đồng thời dữ liệu sẽ được chuyển sang tầng 2 để xác định đó có phải là kiểu tấn công DoS hay không? nếu không, dữ liệu sẽ được chuyển sang các tầng kế tiếp để xác định chính xác kiểu tấn công cụ thể, trường hợp không xác định được, thì đó là kiểu tấn công mới chưa được biết đến.



Hình 5. Kiến trúc bộ phân lớp lai đa tầng dựa trên mô hình phân đa lớp truyền thống

Việc lựa chọn thứ tự phân lớp kiểu tấn công dựa vào xác suất xuất hiện thực tế của mỗi kiểu tấn công nhằm tối ưu thời gian phân lớp, các kiểu tấn công có xác suất xuất hiện thấp hơn sẽ nằm ở các tầng cao hơn do thời gian phân lớp lớn hơn.

Do tính chất đặc thù dữ liệu của mỗi kiểu tấn công, các bộ phân loại được sử dụng tại mỗi tầng sẽ khác nhau, để xác định chính xác kỹ thuật máy học nào là tối ưu tại mỗi tầng, chúng tôi sử dụng nhiều kỹ thuật máy học khác nhau để huấn luyện, kiểm tra và so sánh kết quả dựa trên các chỉ số đánh giá.

Các tập dữ liệu dùng trong thí nghiệm được tạo ra bằng cách rút trích một cách ngẫu nhiên các mẫu tin từ tập dữ liệu KDD99, số mẫu tin cụ thể cho từng kiểu tấn công trong mỗi tập dữ liệu thí nghiệm được thống kê như Bảng 2.

Bảng 2. Thông tin chi tiết 6 tập dữ liệu con được sử dụng trong thí nghiệm

TT	Tập dữ liệu	Số mẫu tin ứng với từng kiểu tấn công					Tổng số mẫu tin
		Normal	DoS	Probe	R2L	U2R	
1	Tập dữ liệu 1	9.623	38.891	462	9	0	48.985
2	Tập dữ liệu 2	9.622	38.937	407	18	1	48.985
3	Tập dữ liệu 3	9.903	38.629	437	13	3	48.985
4	Tập dữ liệu 4	9.743	38.830	400	12	0	48.985
5	Tập dữ liệu 5	9.706	38.856	416	7	0	48.985
6	Tập dữ liệu 6	0	0	41.102	1.126	52	42.280

Các tập dữ liệu 1-5 được sử dụng cho các phân lớp Normal và DoS. Tập dữ liệu 6, gồm tất cả các mẫu tin của các kiểu tấn công Probe, R2L và U2R rút trích từ tập dữ liệu KDD99, được sử dụng cho các phân lớp còn lại: Probe, R2L và U2R. Đó là do số lượng mẫu tin của các kiểu tấn công Probe, R2L và U2R ở các tập dữ liệu 1-5 ít, không đảm bảo độ chính xác phân lớp khi đánh giá hiệu quả của thuật toán.

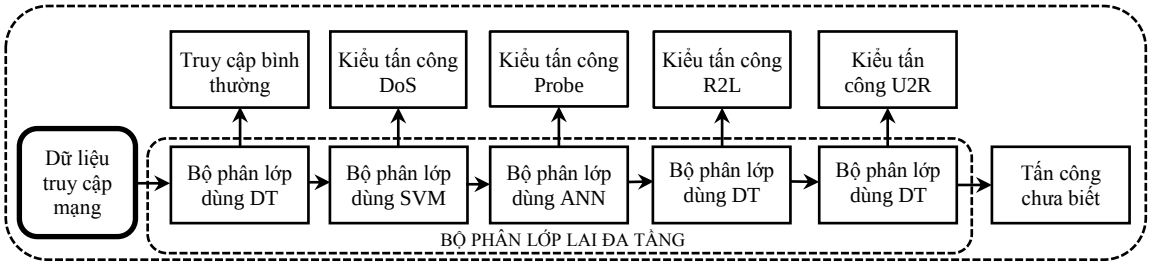
Kết quả, độ chính xác phân lớp (Accuracy) trung bình dựa trên đánh giá chéo 5-fold chạy trên cả 6 tập dữ liệu sử dụng các thuật toán: Naïve Bayes, SVM, mạng nơron, cây quyết định, hồi quy luận lý (Logistic Regression) và k láng giềng gần nhất được trình bày như ở Bảng 3.

Bảng 3. Độ chính xác phân lớp trung bình ứng với mỗi thuật toán phân lớp

TT	Bộ phân lớp	Normal	DoS	Probe	R2L	U2R
1	Cây quyết định	99,83%	99,94%	99,81%	99,85%	99,90%
2	K láng giềng gần nhất	99,79%	99,90%	99,88%	99,78%	99,85%
3	Hồi quy luận lý	99,14%	99,39%	99,26%	99,17%	99,81%
4	Hồi quy luận lý đa thức	99,33%	99,64%	99,53%	99,52%	99,80%
5	Naïve Bayes	98,36%	99,57%	99,56%	99,36%	86,76%
6	Mạng nơ ron	99,76%	99,90%	99,88%	99,83%	99,82%
7	SVM tuyến tính	98,65%	99,45%	99,18%	98,93%	99,73%
8	SVM với nhân dùng GRBF	99,63%	99,95%	99,87%	99,77%	99,87%

Theo đó, số liệu ở cột Normal thể hiện độ chính xác phân lớp một truy cập là bình thường hay một cuộc tấn công, số liệu ở các cột còn lại thể hiện độ chính xác phân lớp với từng kiểu tấn công cụ thể là DoS, Probe, R2L hoặc U2R. Theo đó, bộ phân lớp sử dụng cây quyết định đạt độ chính xác cao nhất ở các tầng 1, 4 và 5; bộ phân lớp sử dụng mạng nơron đạt độ chính xác cao nhất ở tầng 3 và bộ phân lớp sử dụng SVM với nhân dùng GRBF đạt độ chính xác

cao nhất ở tầng 2. Để thực hiện SVM với nhân dùng GRBF, một thuật toán tìm kiếm lưới được sử dụng trên tập huấn luyện để có được tham số tối ưu dùng cho GRBF, tham số này sau đó được SVM sử dụng cho việc phân lớp. Kiến trúc bộ phân lớp lai đa tầng được hình thành từ các bộ phân lớp đơn tối ưu phù hợp với mỗi kiểu tấn công tại mỗi tầng được trình bày ở Hình 6.



Hình 6. Kiến trúc bộ phân lớp lai đa tầng

Theo kết quả thí nghiệm, độ chính xác dự báo tổng thể của bộ phân lớp lai đa tầng đạt 99.83% khi phân lớp các truy cập bình thường và 99.58% khi phân lớp các kiểu tấn công, tốt hơn so với việc áp dụng chỉ một kỹ thuật máy học đơn trong các IDS [15].

VI. KẾT LUẬN

Từ kết quả thí nghiệm, ta nhận thấy: do tính chất đặc thù dữ liệu của mỗi kiểu tấn công, các kỹ thuật máy học tối ưu phù hợp đã được lựa chọn khi xây dựng các bộ phân lớp loại 2 lớp. Từ đó, kiến trúc một bộ phân lớp lai đa tầng dùng kỹ thuật OVR, trên cơ sở sử dụng các bộ phân lớp loại 2 lớp tối ưu đã chọn ở mỗi tầng để phân lớp các kiểu tấn công trong IDS. Đồng thời, kết quả thí nghiệm cũng đặt ra các vấn đề cần được tiếp tục nghiên cứu, đặc biệt là các nội dung:

(1) Việc nghiên cứu tìm ra các bộ phân lớp phức tạp hơn so với các bộ phân lớp đơn ở mỗi tầng cần được xem xét. Xuất phát từ ý tưởng kết hợp nhiều bộ phân lớp để hợp tác thay vì cạnh tranh trong việc thực hiện nhiệm vụ, có thể sẽ đem lại hiệu năng cao hơn khi kết hợp các bộ phân lớp để phát triển các IDS.

(2) Các bộ phân lớp cơ sở: việc lựa chọn các bộ phân lớp đơn như một bộ phân lớp cơ sở để so sánh và đánh giá các bộ phân lớp có vẻ không phải là lựa chọn tốt, sẽ tốt hơn nếu các bộ phân lớp lai hoặc kết hợp được sử dụng để so sánh độ chính xác dự báo.

(3) Việc lựa chọn thuộc tính và phân cụm dữ liệu đã có nhiều hướng tiếp cận [7, 18, 19, 20]. Tuy nhiên, cần nghiên cứu tìm kiếm một thuật toán lựa chọn thuộc tính và phân cụm dữ liệu tối ưu, phù hợp nhất với kỹ thuật máy học, cũng như đặc thù dữ liệu của mỗi kiểu tấn công.

(4) Năng lực xử lý dữ liệu cũng như tính toán của hệ thống máy đóng vai trò quan trọng trong việc khai thác thuật toán cũng như kỹ thuật máy học. Từ đó nâng cao hiệu quả xử lý, tiếp cận theo hướng trí tuệ nhân tạo.

TÀI LIỆU THAM KHẢO

1. Devarakonda, N., S. Pamidi, et al. - Intrusion Detection System using Bayesian Network and Hidden Markov Model. Procedia Technology, 2012, 4(0) 506-514.
2. Bhat A. H., Patra S., Jena D. - Machine learning approach for intrusion detection on cloud virtual machines. International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2013, 2(6) 56-66.
3. Gaidhane R., Vaidya C., Raghuwanshi M. - Survey: Learning Techniques for Intrusion Detection System (IDS), International Journal of Advance Foundation and Research in Computer (IJAFRC), 2014, 1(2) 21-28.
4. Omar S., Ngadi A., Jebur H. H. - Machine learning techniques for anomaly detection: an overview. International Journal of Computer Applications, 2013, 79(2) 33-41.
5. Singh J., Nene M. J. - A Survey on Machine Learning Techniques for Intrusion Detection Systems. International Journal of Advanced Research in Computer and Communication Engineering, 2013, 2(11) 4349-4355.
6. Wagh S. K., Pachghare V. K., Kolhe S. R. - Survey on intrusion detection system using machine learning techniques. International Journal of Computer Applications, 2013, 78(16) 30-37.
7. Calix R. A., Sankaran R. - Feature Ranking and Support Vector Machines Classification Analysis of the NSL-KDD Intrusion Detection Corpus. Proceedings of the Twenty-Sixth International Florida Artificial Intelligence Research Society Conference, 2013, 292-295.
8. Reddy R. R., Kavya B., Ramadevi Y. - A Survey on SVM Classifiers for Intrusion Detection. International Journal of Computer Applications, 2014, 98(19) 38-44.
9. Catania C.A., Bromberg F., et al. - An autonomous labeling approach to support vector machines algorithms for network traffic anomaly detection. Expert Systems with Applications, 2012, 39(2) 1822-1829.
10. Guanghui S., Jiankang G., et al. - An Intrusion Detection Method Based on Multiple Kernel Support Vector Machine. Network Computing and Information Security (NCIS), 2011 International Conference on, IEEE, 2011, 119-123.
11. Li W., Liu Z. - A method of SVM with Normalization in Intrusion Detection. Procedia Environmental Sciences 11, 2011, Part A(0) 256-262.

12. Mohammad M.N., Sulaiman N., et al. - A novel local network intrusion detection system based on support vector machine. Journal of Computer Science, 2011, 7(10) 1560-1564.
13. Xiaozhao F., Wei Z,, et al. - A Research on Intrusion Detection Based on Support Vector Machines. Communications and Intelligence Information Security (ICCIIS), 2010 International Conference on, IEEE, 2010, 109-112.
14. Xie Y., Zhang T., - An intelligent anomaly analysis for intrusion detection based on SVM. Computer Science and Information Processing (CSIP), 2012 International Conference on, IEEE, 2012, 739-742.
15. Altwaijry H., Algarny S. - Bayesian based intrusion detection system. Journal of King Saud University - Computer and Information Sciences, 2012, 24(1) 1-6.
16. Aburomma A. A., Reaz M. B. I. - Evolution of Intrusion Detection Systems Based on Machine Learning Methods. Australian Journal of Basic and Applied Sciences, 7(7) 799-813.
17. Sanjaya S. K. S. S. S., Jena K. - A Detail Analysis on Intrusion Detection Datasets. In 2014 IEEE International Advance Computing Conference (IACC), 2014, 1348-1353.
18. Al-Jarrah O. Y., Siddiqui A., et al. - Machine-Learning-Based Feature Selection Techniques for Large-Scale Network Intrusion Detection. In Distributed Computing Systems Workshops, 2014 IEEE 34th International Conference on, IEEE, 2014, 177-181.
19. Moradi Koupaie H., Ibrahim S., Hosseinkhani J. - Outlier detection in stream data by machine learning and feature selection methods. International Journal of Advanced Computer Science and Information Technology (IJACSIT), 2014, 2 17-24.
20. Patel S., Sondhi J. - A Review of Intrusion Detection Technique using Various Technique of Machine Learning and Feature Optimization Technique. International Journal of Computer Applications, 2014, 93(14) 43-47.

A MACHINE LEARNING APPROACH TO CLASSIFY TYPES OF ATTACKS IN NETWORK INTRUSION DETECTION SYSTEM

Hoang Ngoc Thanh, Tran Van Lang, Hoang Tung

ABSTRACT *— The main function of Network Intrusion Detection Systems (IDS) is to protect the system, analyze and predict network access behavior of users. This behavior is considered normal or an attack. IDS than to identify the behavior is normal or an attack based on the stored data, has the ability to learn to identify new attacks. For each specific type of attack is DoS, Probe, R2L or U2R, dataset have peculiar characteristics. This article refers to finding the optimum machine learning techniques for each type of attack is based on known machine learning algorithms as: Decision Tree (DT), K Nearest Neighbor, Support Vector Machine (SVM), Artificial Neural Network (ANN),... Since then, built a multi-layer hybrid classifier based on the use of optimal machine learning techniques, best suited to type of attack on each layer. Results of experiments on the KDD99 dataset using 5-fold Cross Validation showed that the multi-layer hybrid classifier integrated machine learning techniques: DT, ANN and SVM have highest predicted accuracy: 99.83% when the classification of normal access and 99.58% when the classification of types of attacks.*