CẢI TIẾN BẢN ĐỒ TỔ CHỨC TỰ ĐỘNG (SOM) CHO HỆ THỐNG PHÁT HIỆN XÂM NHẬP

Lê Diên Tâm*, Nguyễn Xuân Vinh[+], Trần Công Hùng[@]
*Trường Cao đẳng Công nghệ Thủ Đức
[+]Đại học Nông lâm TP.HCM
[@]Học viện Công Nghệ Bưu Chính Viễn thông

Tóm tắt: Ngày nay, các cuộc tấn công rất đa dạng, các doanh nghiệp thường sử dụng hệ thống phát hiện xâm nhập (IDS) để phát hiện các cuộc tấn công. Có hai cách tiếp cận để thực hiện IDS: một cách phát hiện các cuộc tấn công dựa trên chữ ký và một cách dựa trên hành vi. Bài viết này theo cách tiếp cận thứ hai dựa trên hành vi. Trong giai đoạn đào tạo, được xử lý bởi ứng dụng SOM (Self-organizing map) (Bản đồ tự tổ chức), hệ thống tạo ra một số vectơ xác định trạng thái bình thường của hệ thống. Cụm các vectơ này sẽ được đặc trưng bởi một nơron (lõi lượng tử) với bán kính r (r: bán kính lượng tử). Một hình học của nơ ron (có bán kính r) được coi là một hình cầu có bán kính r. Dựa trên việc xây dựng các vectơ mô tả trạng thái của hệ thống trong thời gian thực, chúng ta có thể phát hiện một hoạt động bất thường mới bằng cách so sánh giữa khoảng cách d (từ các vectơ trên với tất cả các nơ-ron) và ngưỡng r (bán kính lượng tử). Nếu khoảng cách nhỏ hơn ngưỡng, hệ thống IDS sẽ coi hoạt động mới này là trạng thái bình thường và không đưa ra bất kỳ cảnh báo nào. Nếu khoảng cách lớn hơn ngưỡng r, hệ thống IDS sẽ coi hoạt động mới này là trạng thái bất thường và tạo cảnh báo. Vấn đề của bài báo xảy ra khi hai hoặc nhiều hơn bán kính hình cầu chồng lên nhau. Vấn đề này làm cho hệ thống IDS khó xác định. Mục tiêu nghiên cứu của bài báo là phát triển một thuật toán mô hình hóa làm cho tất cả các bán kính hình cầu không bị chồng chéo lẫn nhau. Từ đó, hệ thống phát hiện xâm nhập được xác định và tăng độ chính xác cho hệ thống.

Từ khóa: Hệ thống phát hiện xâm nhập IDS, bản đồ tự tổ chức SOM

I. GIỚI THIỆU

Hệ thống phát hiện xâm nhập (IDS) là một thiết bị hoặc ứng dụng phần mềm giám sát các hoạt động của mạng hoặc hệ thống đối với các hoạt động gây hại hoặc vi phạm chính sách và đưa ra báo cáo cho các trạm quản lý. Hai cách tiếp cận chính của IDS là: I) IDS dựa trên dấu hiệu vi phạm: phát hiện các cuộc tấn công thông qua các đặc điểm dấu hiệu vi phạm có sẵn. Những đặc điểm này được lưu trữ trong tập cơ sở dữ liệu của IDS. II) IDS dựa trên hành vi: phát hiện thông qua các hành vi bất thường. IDS phát hiện một hành vi là bất thường bởi vì đã được học trong các dữ liệu mẫu trước đó. Những hành vi bình thường này được mô tả thông qua hai vectơ: Activity vector: mô tả hoạt động của một luồng trong thời gian thực. Status vector: mô tả trạng thái của hệ thống.

Bản đồ tự tổ chức (SOM) là một loại mạng nơron nhân tạo (artificial neural network - ANN) được tạo ra bằng cách sử dụng học không giám sát (unsupervised learning) để tạo ra một bản đồ hai chiều của không gian đầu vào của các mẫu đào tạo. SOM khác với các mạng nơron nhân tạo khác nghĩa là được sử dụng hàm lân cận để bảo toàn các thuộc tính ban đầu của không gian đầu vào. Giống như hầu hết các mạng nơron khác, SOM hoạt động theo hai chế độ: I) Đào tạo: xây dựng bản đồ bằng các dữ liệu đầu vào (một quá trình cạnh tranh, còn gọi là lượng tử hóa vectơ), II) Ánh xạ: tự động phân loại một vectơ đầu vào mới. Mục tiêu của việc học trong SOM là làm cho các phần khác nhau của mạng phản ứng tương tự với các mẫu đầu vào nhất định.

Trong bài báo này, chúng tôi cố gắng giải quyết một hai vấn đề: thứ nhất là làm cho ứng dụng SOM mang tính chính xác cao hơn (các nơ-ron không chồng chéo lẫn nhau), thứ hai là cải thiện phát hiện các cuộc tấn công bằng cách giảm Sai âm (False Negative) và Sai dương (False Positive) để đảm bảo sự cân bằng giữa các nơ-ron. Trong bài báo này, phần 1 giới thiệu các kiến thức căn bản về IDS và ứng dụng SOM, phần 2 giới thiệu về các thuật toán phân cụm và các đề xuất về IDS hoạt động với bản đồ SOM, phần 3, 4 bài báo nói về phương pháp thực hiện và trình bày các kết quả mô phỏng và phần 5 kết luận.

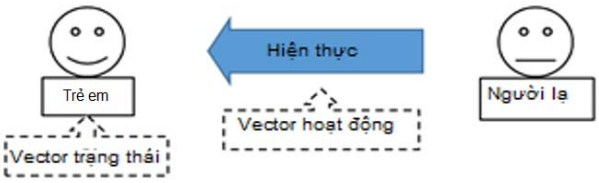
II. ĐỀ XUẤT VỀ IDS

Khi phát triển IDS dựa trên hành vi, chúng ta phải đối mặt với một số khó khăn sai âm và sai dương. Trong hệ thống máy tính, Sai dương: báo động khi không có cuộc tấn công. Vấn đề này không nghiêm trọng, nhưng hệ

Tác giả liên hệ: Lê Diên Tâm
Email: *tamld@tdc.edu.vn*
Đến tòa soạn: 8/2019, chỉnh sửa 11/2019, chấp nhận đăng 12/2019

thống IDS không nên đưa ra báo động trong khi không có cuộc tấn công nào. IDS dựa trên hành vi hoàn toàn không thể tránh được vấn đề này. Nhưng có thể học hỏi thêm kiến thức để loại bỏ dần sai dương giả. Âm tính giả: không có báo động khi bị tấn công. Vấn đề này rất nghiêm trọng và nguy hiểm. IDS trở nên vô dụng khi nó không đưa ra bất kỳ báo động nào khi bị tấn công. Những lỗi này có liên quan đến việc có quá nhiều kiến thức về sự hiểu biết mà IDS được học trong quá trình vận hành bình thường của hệ thống và mức độ lớn hay nhỏ để xem xét hai trạng thái vận hành là giống nhau hoặc khác nhau.

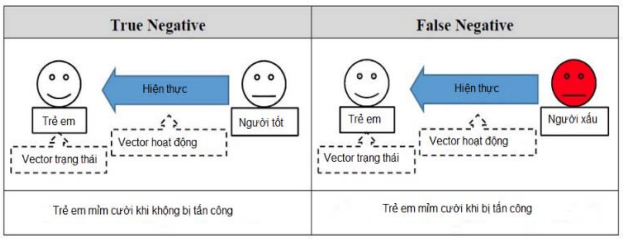
Ở ngoài đời, khi một đứa trẻ nhìn vào một người lạ mà nó đã thấy trước đó. Đứa trẻ có thể có một trong hai hành vi như sau:



Hình 1: Phản ứng của trẻ em trong thực tế

Trường hợp 1: Nếu người lạ là người tốt, đứa trẻ nghĩ rằng người lạ không phải là đối tượng nguy hiểm.

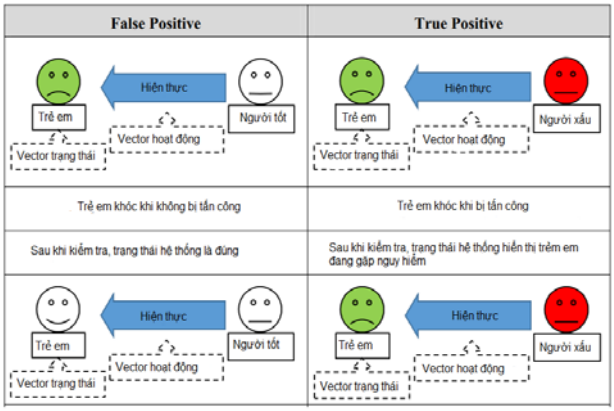
- Nếu người này tốt: không có vấn đề gì. Được gọi là đúng (**True negative**)
- Nếu người này xấu: có một vấn đề lớn, đứa trẻ đã nhận ra sai. Và điều này có thể dẫn đến tổn hại cho đứa trẻ. Được gọi là Sai âm (**False negative**)



- ➢ Vấn đề sai âm khiến trẻ không phản ứng khi bị tấn công
- ➢ Sai dương thực sự không có tác động gì đến đứa trẻ

Trường hợp 2: Coi người lạ là người xấu, trẻ sẽ khóc để báo cho bố mẹ.

- Người này là tốt: báo động này là vô ích. Nhưng, sau đó, trẻ nhận ra rằng mình đã sai, và trẻ sẽ coi hoạt động của người lạ này là hoạt động bình thường. Sau đó, nếu đứa trẻ gặp lại những hoạt động bình thường này, nó sẽ không báo cho bố mẹ. (Sai dương (False Positive) + Học mới bình thường -> Tiêu cực thực sự (True negative))
- Nếu người này xấu: trẻ khóc là cần thiết để cha mẹ chú ý đến mối nguy hiểm mới từ người lạ (Đúng tích cực (True positive))



- ➢ **True positive** Sự tích cực thực sự là một trạng thái tốt khi trẻ phát hiện ra cuộc tấn công nó trẻ tìm cách trú ẩn người lạ trước.
- ➢ **True Negative** Tiêu cực thực sự là một trạng thái bình thường học được mà vô hại với trẻ.
- ➢ **False positive** Việc dương tính giả không gây ra bất kỳ tác động nào đến trẻ, nhưng nó chỉ xảy ra một lần. Sau đó trẻ sẽ được học các hoạt động mới của người lạ.
- ➢ **False negative** Âm tính giả được coi là trạng thái bình thường. Trạng thái này báo động sai rất nghiêm trọng.

Kết luận: Sai tiêu cực là tác động gây ảnh hưởng nhiều hơn sai tích cực. Sai tích cực sẽ được loại bỏ khi IDS có nhiều kiến thức về về các trạng thái bình thường.

Đối mặt với những khó khăn đã đề cập ở trên, chúng tôi đã phát triển một thuật toán để giải quyết các vấn đề về sai âm và sai dương. Đồng thời, làm cho bản đồ trở nên chính xác hơn bằng cách loại bỏ sự chồng chéo giữa nhóm bản đồ cũ và bản đồ mới. Đầu tiên, chúng tôi nhắc lại về các quy trình mà SOM đã sử dụng để học và quản lý kiến thức. Bao gồm các bước sau:

- ➢ Giai đoạn 0. Zero knowledge - Không có kiến thức

Lúc đầu, hệ thống IDS không có kiến thức về trạng thái bình thường và trạng thái bất thường.

- ➢ Giai đoạn 1. Tạo tế bào nơ ron ngẫu nhiên

Một mảng S (n x m) của k-dimensional-vector được tạo bởi lệnh randinit. Mỗi vectơ sẽ được gọi là nơ ron để phân biệt chúng với vectơ huấn luyện. Mỗi nơ ron có 1 trung tâm
k-dimension được tạo ngẫu nhiên.

- ➢ Giai đoạn 2. Thu thập trạng thái Vector

Khi một sự kiện bình thường xảy ra, sự kiện này hoạt động theo một số hoạt động và làm cho hệ thống mạng

tạo ra các trạng thái. Các hoạt động này được mô hình hóa như Vector hoạt động **Activity Vector**, vector hoạt động này có kích thước x-dimension (Đại diện cho x thông tin). Các trạng thái hệ thống này được mô hình hóa như vector trạng thái **Status Vector**, có kích thước k-dimension (Đại diện cho k thông tin).

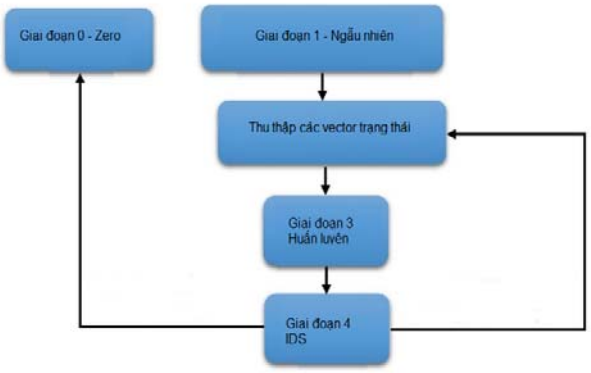
- Giai đoạn 3. Huấn luyện

Sau quá trình training dựa trên phương pháp SOM, vị trí của các nơron trong mảng S sẽ được thiết lập để có các tính năng tốt nhất, gần nhất với sự phân bố của các Vector training.

Hoạt động bình thường của hệ thống sẽ được đại diện bởi một cụm các vectơ huấn luyện và mỗi cụm vectơ huấn luyện sẽ được đặc trưng bởi một nơron. Mỗi tế bào thần kinh có trung tâm đại diện cho chiều k-dimension thông tin và bán kính biểu thị bằng lỗi lượng tử hóa (Lỗi lượng tử hóa được tính bằng lệnh lỗi).

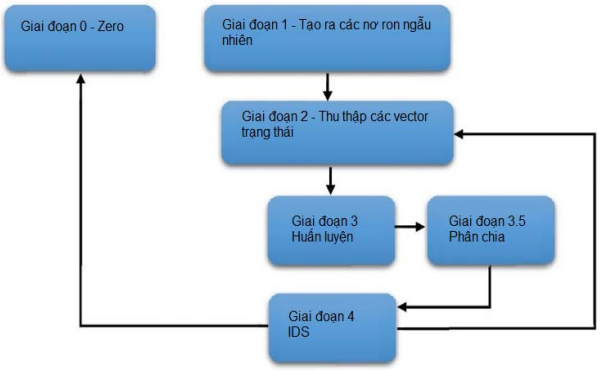
- Giai đoạn 4. IDS

Trong giai đoạn phát hiện, IDS sẽ xác định trạng thái bất thường của hệ thống bằng cách so sánh với các tế bào nơron hiện tại trong bản đồ SOM. Nếu khoảng cách đến bất kỳ tế bào nơron nào nhỏ hơn ngưỡng, thì hệ thống IDS sẽ xử lý một cách ngẫu nhiên và không có cảnh báo nào được nêu ra. Ngược lại, nếu khoảng cách đến mỗi nơron trong mảng S lớn hơn ngưỡng, được gọi là bán kính IDS, thì hệ thống IDS sẽ coi đó là trạng thái bất thường và tạo ra báo động. Bán kính IDS đóng vai trò là độ nhạy của từng nơron trong hệ thống IDS. Bán kính nhỏ hơn khiến hệ thống IDS trở nên dễ bị ảnh hưởng hơn, đây được gọi là IDS dương tính giả vì IDS sẽ tạo ra báo động sai. Ngược lại, bán kính lớn hơn làm cho IDS ít tạo ra cảnh báo, điều này sẽ gây ra âm tính giả.



Hình 2: Tiến trình hoạt động của SOM

Trong quá trình thực hiện, hệ thống IDS sẽ được cập nhật liên tục với các dữ liệu đầu vào mới và thực hiện lại giai đoạn 3 (giai đoạn training), sẽ tạo ra một bản đồ mới. SOM cần kết hợp và so sánh bản đồ cũ và bản đồ mới thành một. Sự kết hợp này gây ra một số tế bào nơron có thể được chồng chéo với nhau. Vì vậy chúng tôi chèn một bước giữa sau giai đoạn đào tạo, bước này có trách nhiệm thu hẹp từng nơron. Quá trình thu hẹp phải đảm bảo chất lượng của IDS. Chất lượng này của quá trình này thể hiện thông qua việc giảm sai âm và sai dương.



Hình 3: Cải tiến quá trình SOM

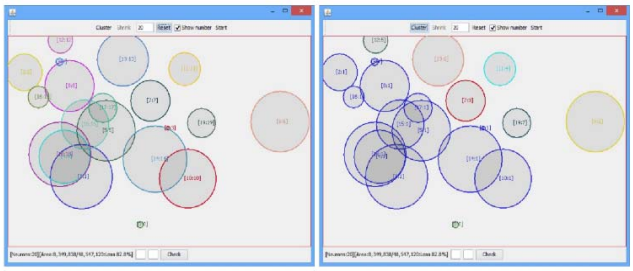
Thuật toán thu nhỏ của chúng tôi có hai giai đoạn: giai đoạn nhóm cụm (cluster) và giai đoạn phân chia. Giai đoạn nhóm cụm lại là giai đoạn tùy chọn để tăng tốc độ khi thu hẹp. Nếu các tế bào nơron là riêng biệt, giai đoạn nhóm cụm sẽ trở nên vô ích. Nhưng, nếu các nơ-ron được nhóm lại với nhau, giai đoạn nhóm cụm sẽ tạo thuận tiện cho việc tính toán khoảng cách Euclide bằng cách tính khoảng cách Euclide giữa các nơ-ron trong cùng một cụm. Bước này làm tăng tốc độ thu nhỏ các nơron lại bởi các nơron nhóm liền kề nhau với nhau sẽ tạo thành một cụm. Nó làm cho thời gian để tính khoảng cách Euclide giữa mỗi cặp nơ ron giảm đi đáng kể.

Bước này là một bước tùy chọn. Nếu các tế bào thần kinh là riêng biệt, giai đoạn phân chia cụm sẽ không có ý nghĩa. Nhưng, nếu các tế bào thần kinh gần nhau và tạo thành nhiều cụm. Việc phân chia cụm sẽ làm giảm số lượng tính toán khoảng cách Euclide. Các nơron trong một cụm không cần phải so sánh khoảng cách với nơron trong một cụm khác.

```
Method void clustering(Model model) {
  // Initialize cluster flag for each neuron: neuron i-th is belong to cluster i-th
  Neuron[] neurons = model.getNeurons()
  int[] clusters = model.getClusters()
  int[] neighbors = model.getNeighbors()
  for each i IN flag
    SET clusters[i] = i;
  for each neuron ni IN neurons (i begin = 0) {
    for each neuron nj IN neurons (j begin = i+1) {
      if (ni is overlapped nj) {
        neighbors[i]++
        if (flag[j] != j) {
          if (flag[i] != i) {
            if (i < j) {
              replace all where flag[j] = flag[i]
            } else {
              replace all where flag[i] = flag[j]
            }
          } else {
            replace all where flag[i] = flag[j]
          }
        } else {
          flag[j] = flag[i]
        }
      }
    }
  }
}
```

Hình 4: Mô phỏng Pseudo code

Kết quả phân cụm:



Hình 5: Kết quả Trước và sau khi phân cụm

Sau khi phân cụm (tùy chọn), chúng tôi tiếp tục thu nhỏ bán kính nơron để làm cho các nơron trong bản đồ tạo được sự chồng chéo với nhau. Nơron lớn hơn sẽ co lại nhiều hơn nơron nhỏ hơn

Tối ưu thuật toán phân cụm

Bằng cách kết hợp thuật toán phân cụm và thuật toán rút gọn. Chúng tôi đã sửa đổi thuật toán đó để giảm bớt sai số với các nơ-ron nhóm thành các mảng. Trong bài báo trước, họ sử dụng một ràng buộc khi nhóm nhóm nơ-ron thành một mảng bằng cách so sánh khoảng cách giữa nơ-ron với bán kính của IDS.

Khoảng cách <= Bán kính của IDS

Chúng tôi đã sửa đổi cách tiếp cận trên bằng cách thêm một tham số tỷ lệ cho biết tỷ lệ trùng lặp..

Khoảng cách <= Tốc độ * Bán kính của IDS (Hiện tại, tốc độ này đang là 0.5)

Khi chạy thuật toán tối ưu hóa (giảm co lại), chúng tôi đánh giá mức giảm âm lượng dựa trên so sánh giữa âm lượng trước khi thu nhỏ và giảm âm lượng sau quá trình thu nhỏ.
Giá trị âm lượng được tính theo cách đệ quy như sau theo công thức:

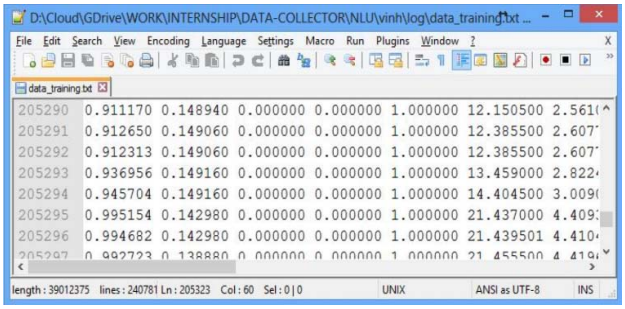
$$V_n(R) = \frac{2\pi R^2}{n} V_{n-2}(R)$$

1. Kết quả mô phỏng

Trong hệ thống của chúng tôi, chúng tôi có thể thu thập thông tin hệ thống thời gian thực. Để thử nghiệm, chúng tôi đã sử dụng hai bộ dữ liệu mẫu: 3840 trạng thái bình thường (do SOM cung cấp) và dữ liệu được thu thập từ một máy chủ vật lý đặt tại phòng thí nghiệm trường đại học của chúng tôi. Việc thu thập thông tin từ máy chủ vật lý bao gồm 2 dạng:

- Vecto trạng thái lượng tử (Quantized status vectors):

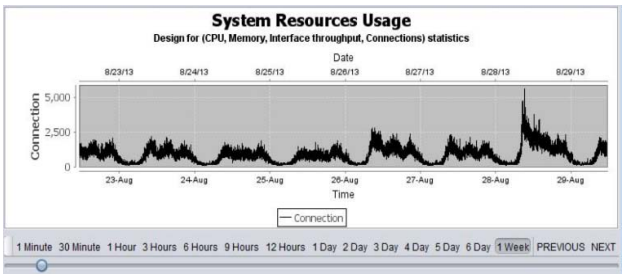
Các vectơ trạng thái được lượng tử hóa dùng để huấn luyện SOM. Số lượng các trường bằng kích thước k (hiện tại, k = 18)



Hình 6: Dữ liệu mẫu Vector trạng thái lượng tử

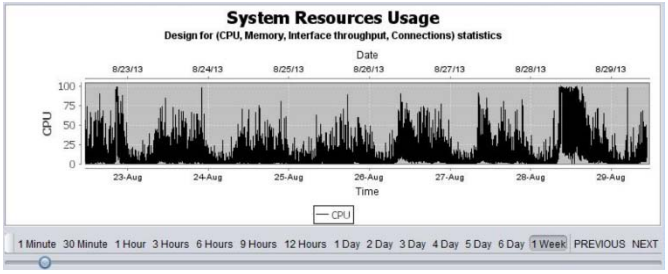
- Thông tin trạng thái ban đầu:

Thông tin này sẽ được đưa vào chương trình hệ thống để quan sát trạng thái bất thường trực quan. Sau đó, chúng tôi sẽ xóa thông tin khi hệ thống không tốt. Ví dụ, CPU được giữ ở mức 100% trong một khoảng thời gian
Kết nối:



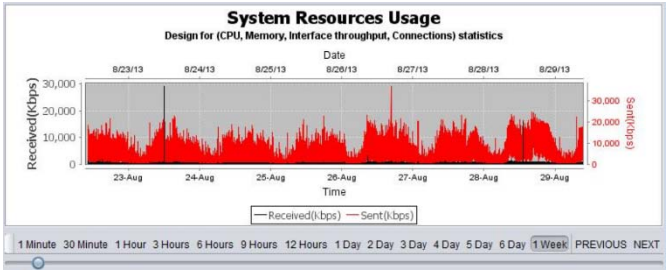
Hình 7: Số lượng kết nối TCP đang mở

CPU:



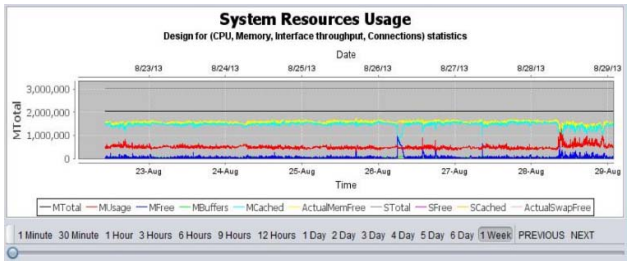
Hình 8: Phần trăm CPU được sử dụng

Băng thông mạng:



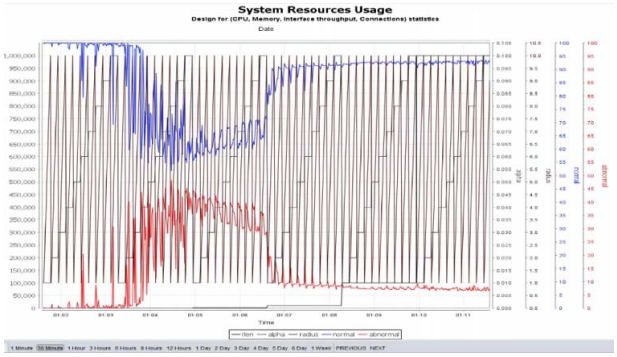
Hình 9: Băng thông mạng

Bộ nhớ được sử dụng:

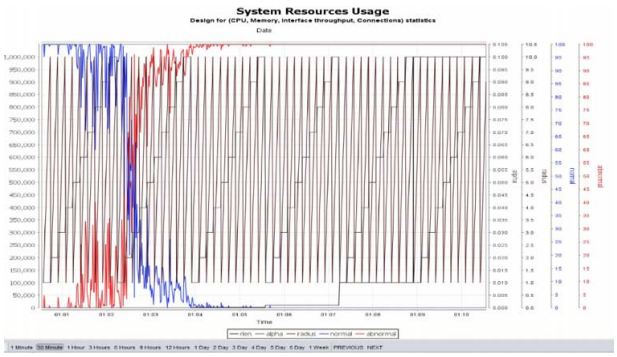


Hình 10: Bộ nhớ được sử dụng

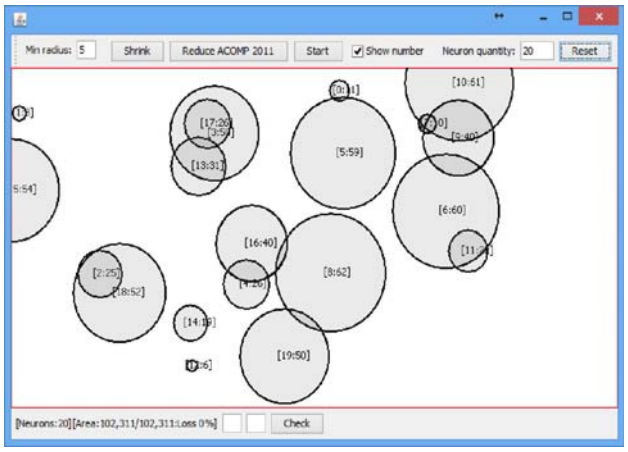
Sau khi chạy 600 trường hợp cho mỗi tham số cho mỗi trường hợp kiểm tra (3840 trạng thái SOM (máy chủ vật lý)), chúng tôi đã có kết quả như sau.



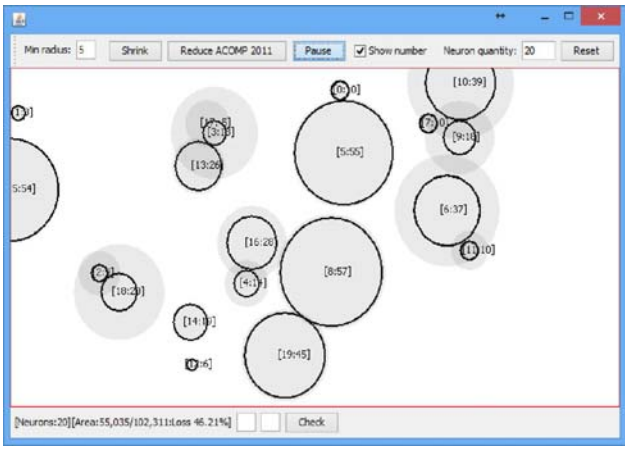
Hình 11: Ổn định dương tính giả



Hình 12: Ổn định âm tính giả



Hình 13: Trước khi phân chia



Hình 14: Sau khi phân chia.

Hệ thống ổn định khi số bước đào tạo rlen lớn hơn 10.000. Những thay đổi của giá trị alpha, bán kính ảnh hưởng nhiều đến sự thay đổi của sai dương và sai âm (trạng thái bình thường được phát hiện và trạng thái bất thường không đa dạng). Chúng tôi đã chọn các tham số sau cho tất cả các thử nghiệm với rlen: 10.000, alpha: 0,05 và bán kính: 10.

Chúng tôi thực hiện hai phiên bản của hệ thống IDS để phát hiện các trạng thái bất thường. Đầu tiên với thuật toán Shrink: giúp thu nhỏ các nơron để loại bỏ sự chồng chéo, số lượng nơron không thay đổi. Thứ hai là thuật toán Giảm-sự phân chia: sẽ làm giảm nơron sau đó thu nhỏ các nơron còn lại. Điều này khiến số lượng nơron sẽ giảm vì quá trình giảm sẽ giúp giảm thời gian phát hiện xâm nhập. Làm tăng khả năng phát hiện cho hệ thống IDS.

III. KẾT LUẬN

Trong bài báo này, chúng tôi đề xuất kiến trúc cho một IDS để phát hiện các cuộc tấn công không xác định đã được trình bày. Cải thiện bản đồ tự tổ chức cho hệ thống phát hiện xâm nhập dựa trên hành vi. So với các phương pháp khác, thiết kế của chúng tôi thể hiện các đặc tính và hiệu suất tốt hơn.

REFERENCES:

[1] Farhoud Hosseinpour, Payam Vahdani Amoli, Fahimeh Farahnakian, Juha Plosila, and Timo Hämäläinen, “Artificial Immune System Based Intrusion Detection: Innate Immunity using an Unsupervised Learning Approach”, International Journal of Digital Content Technology & its Applications 8.5, 2014.

[2] Kyung -min Kim, Hak Ju Kim ; Kwangjo Kim; “Design of an Intrusion Detection System for Unknown - attacks based on Bio -inspired Algorithms” Computer Security Symposium 20 15.

[3] Tao Li and Nan -feng Xiao, "Novel heuristic dual -ant clustering algorithm for network intrusion outliers detection", Optik -International Journal for Light and Electron Optics 126.4, 2015, 494 -497.
[4] Urszula Boryczka, "Ant clustering algorithm", Intelligent Information Systems, 1998, 455-458.
[5] Karen Scarfone and Peter Mell, "Guide to intrusion detection and prevention systems", NIST Special Publication 800, 2007.
[6] Ali Shiravi, Hadi Shiravi, Mahbod Tavallaee, and Ali Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection", Computers & Security, Vol.31.3, 2012, 357 -374.

Abstract: Nowadays, attacks are very diverse. As such, people use Intrusion Detection System to detect the attacks. There are two approaches of IDS implementation: one detects the attacks based on signature and the other based on behavior. This paper follows the second approach which is based on the behavior. In training phase, processed by SOM (Self-Organizing Map) application, the system generates some vectors which specify the normal state of the system. The cluster of these vectors will be characterized by a neuron (quantum core) with radius r (r: quantum radius). A geometric display of neuron (with radius r) is considered as a sphere with radius r. Based on construction of vectors describing the state of the system in real time, we can detect a new anomaly activity by comparing between distance d (from above vectors to all neurons) and the threshold r (quantum radius). If the distance is smaller than the threshold, the IDS system will treat this new activity as normal state and do not raise any warning. If the distance is bigger than the threshold, the IDS system will treat this new activity as anomaly state and generate an alert. The problem of the research occurs when two or more than two spheres overlap each other. This problem makes the IDS system difficult to determine. The objective of our research is to develop a geometric algorithm to make all spheres not to overlap any more. Then, the system will be deterministic and keep the system still precise.

Key words: IDS, SOM, Security

Le Dien Tam was born in Vietnam in 1987. He received Master Computer science in Universite Pierre et Marie CURIE, France, 2014. He is currently a PhD. Candidate in Computer science and engineering from Posts and Telecoms Institute of Technology,Vietnam in 2022.

Nguyen Xuan Vinh was born in Vietnam in 1987. He received the B.E in Computer Science with the top-1 final thesis from Nong Lam University Vietnam, 2009. He received the Master of Engineering degree in Computer network course from Pierre and Marie Curie University in Vietnam with first-class honors, 2013. His main research areas are Anomaly Detection, Applied Machine Learning and Cyber Security. He is, currently, Solution Architect & Data Analytics Lead of Tyme Digital Vietnam.

Tran Cong Hung was born in Vietnam in 1961. He received the B.E in electronic and Telecommunication engineering with first lass honors from HOCHIMINH University of technology in Vietnam, 1987. He received the B.E in informatics and computer engineering from HOCHIMINH University of technology in Vietnam, 1995. He received the master of engineering degree in telecommunications engineering course from postgraduate department Hanoi University of technology in Vietnam, 1998. He received Ph.D at Hanoi University of technology in Vietnam, 2004. His main research areas are B – ISDN performance parameters and measuring methods, QoS in high speed networks, MPLS, Wireless Sensor Network, Cloud Computing, Blockchain. He is, currently, Associate Professor PhD. of Faculty of Information Technology II, Posts and Telecoms Institute of Technology in HOCHIMINH, Vietnam