Phát hiện thư rác VoIP bằng Máy học

Satyadhar Kumar1 Ravula Praveen2 Hemanth Pedamallu3 và Ravi Chowdary4

[1] Đại học Bennett e-
mail: satyadhar.29500@gmail.com Đại học
[2] Bennett, ... e-mail:
ravulapraveen31@gmail.com

20 tháng 11 năm 2020

TRỪU TƯỢNG

Thư rác qua Internet Điện thoại có thể trở thành một mối đe dọa nghiêm trọng trong tương lai gần do số lượng người dùng VOIP ngày càng tăng. Ở đây, chúng tôi xác định một quy trình để nhận thấy những kẻ gửi thư rác trong VoIP bằng cách phân loại sự khác biệt trong Biểu đồ cuộc gọi. Điều này được hướng dẫn, bằng cách sử dụng biểu đồ trọng số của bản ghi dữ liệu cuộc gọi và nó được tạo ra nơi tập hợp các tham số cuộc gọi phân tách được sử dụng để xác định trọng số trên các cạnh. và đặc điểm của người gọi. Hệ thống này cung cấp cho chúng tôi một cách thẳng thắn và khiêm tốn để sử dụng khoảng thời gian gọi làm mô hình liên kết được chọn tự động dựa trên hành vi hình người.

1. GIỚI THIỆU

Giao thức Thoại qua internet (VoIP) là một nhóm gồm nhiều giao thức đồng tồn tại và đầy thách thức để truyền thông tin liên lạc bằng giọng nói qua các mạng IP như internet. [1] VoIP đã thay đổi rất nhiều cách thức truyền dữ liệu điện thoại bằng cách sử dụng mạng IP để định tuyến các gói chứa các phần nhỏ của liên lạc thoại. Giao thức Khởi tạo Phiên (SIP) được sử dụng để bắt đầu, duy trì và hủy bỏ các cuộc gọi khi hoàn thành. Giao thức truyền tải thời gian thực (RTP) được sử dụng để truyền âm thanh dưới dạng gói qua mạng IP. Công nghệ này đang thu hút bọn tội phạm xâm nhập vì nó là vấn đề để xác nhận xác định iden của chính người dùng. Ngoài ra, có thể sử dụng VoIP trên một số thiết bị kết nối Internet và máy tính cá nhân (Riêng tư), Cuộc gọi và tin nhắn văn bản sẽ được gửi qua Wi-Fi. [19] VoIP cho phép các công nghệ truyền thông hiện đại bao gồm điện thoại, điện thoại thông minh, hội nghị video và thoại, email và tính năng phát hiện sẽ được kết hợp bằng cách sử dụng một hệ thống liên lạc thống nhất duy nhất. Tuy nhiên, các phương pháp này sử dụng các giá trị đối lập khác nhau và do đó không xác định được liệu một người dùng spam được xác định có giữ lại số tiền này cho các cuộc gọi không được xây dựng hay không. cho những người sử dụng điện thoại nhưng cũng làm họ khó chịu với những cảnh báo đổ chuông không mong muốn. Do đó, các nhà mạng bắt buộc phải chặn những kẻ gửi thư rác điện thoại liên mạng dưới sự kiểm soát của hệ thống mạng để điều đó làm tăng sự tin tưởng của khách hàng (khách hàng) của họ. Ở đây Chúng tôi có thể quan sát thấy rằng một kẻ gửi thư rác sẽ tự nhiên không nhận cuộc gọi hoặc một vài cuộc gọi từ những người dùng khác. [2] Vấn đề thư rác đang gia tăng từng ngày và kết quả cập nhật cho thấy rằng trong số tất cả các e-mail có giá thuê trong mạng ngay lập tức, có tới tám mươi trong số đó là thư rác (thư rác hoặc không mua được). Các kỹ sư mạng có thể nắm bắt và phân tích các gói cuộc gọi VoIP bằng cách sử dụng wirehark để xác định các cuộc gọi đáng ngờ. Wireshark cũng có phần mở rộng VoIP để phát lại âm thanh được ghi lại trong các gói RTP.

Wireshark cũng có tính năng phát hiện cuộc gọi VoIP từ dấu vết. Từ Menu, chuyển đến 'Điện thoại' và chọn Cuộc gọi VoIP. Một giao dịch thắng mới mở ra, nơi chúng ta có thể xem danh sách tất cả các cuộc gọi cùng với thông tin liên quan của nó. Âm thanh từ các luồng RTP có thể được phát cho cuộc gọi VoIP cụ thể bằng cách sử dụng “nút Phát luồng”. Luồng của một cuộc gọi VoIP cụ thể có thể được xem dưới dạng đồ họa bằng cách sử dụng nút 'Trình tự Luồng'.

Giao diện này giữa những người dùng được định nghĩa là một đồ thị có trọng số và việc người dùng spam chỉ ra sự khác biệt trong cấu trúc đồ thị [22]. Khái niệm sử dụng không phù hợp được thúc đẩy bởi chi tiết rằng người dùng thư rác thường có các hình thức giao tiếp khác nhau như tần suất cuộc gọi lớn, số lượng cuộc gọi ngắn hạn lớn, v.v., được sử dụng để hạ thấp các cạnh phù hợp để giúp phân biệt những thư rác thông thường.
người dùng.

Lợi ích của Hệ thống liên lạc VoIP là - Các tùy chọn nâng cao và tính linh hoạt. -Giá cả phải chăng và các tiện ích bổ sung bạn sẽ nhận được. - An toàn hơn điện thoại cố định của bạn. VoIP sẽ chia sẻ ý tưởng, thông tin và suy nghĩ trong khoảng thời gian. Bạn có thể tăng tốc nhanh chóng các dự án bằng các công cụ cộng tác tức thì như Giao tiếp điện tử tức thì (Nhắn tin), trò chuyện nhóm và chia sẻ video.

Một số Xu hướng Công nghệ VoIP trong năm 2019, United Communication như một dịch vụ có thể tăng Tỷ lệ chấp nhận. 5G sẽ trở thành xu hướng chủ đạo. Tăng cường sử dụng thông tin liên lạc thống nhất di động.

Trí tuệ nhân tạo sẽ thay đổi trải nghiệm của khách hàng Gia tăng rắc rối về bảo mật. Trợ lý VoIP thông minh hơn.

Tạo hiệu ứng VoIP qua truyền thông không dây có tác động kinh tế rõ rệt và các thách thức kỹ thuật khác nhau cần được giải quyết. Một trong những yếu tố quan trọng nhất là băng thông trên mỗi hình thức. [12] Truyền thông dữ liệu không dây vẫn là một nguồn tài nguyên khan hiếm và rất quan trọng cần được sử dụng một cách hiệu quả. Nếu hệ thống di động được sửa đổi mạch hiện đại sẽ hỗ trợ nhiều người dùng VoIP hơn nếu không thì các giá trị phổ có thể được cho phép.

Trong những năm tới, các nhà cung cấp dịch vụ viễn thông cũng nên bắt đầu suy nghĩ về VoIP Spam và ghi nhớ vấn đề này trong khi lập kế hoạch cho các gói điện thoại mới. Ở đây chúng tôi đề xuất một mô hình chỉ bằng một tập dữ liệu và sẽ phát hiện các cuộc gọi spam và bình thường.

2. CÁC CÔNG TRÌNH LIÊN QUAN

Đây là một số kỹ thuật liên quan đến VoIP Spam:

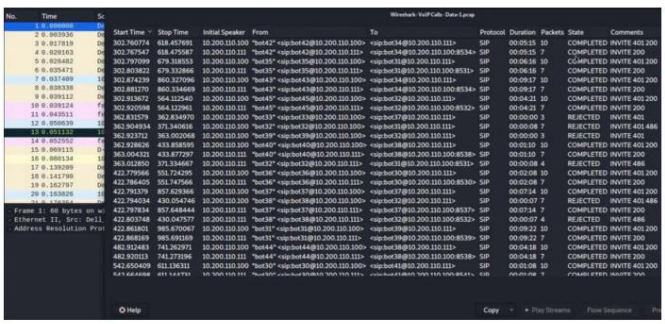
Danh sách trắng: [3] Danh sách trắng chỉ là danh sách các id người dùng được đánh dấu là hợp lệ. Thường thì id id người dùng nằm trong danh sách trắng của người nhận và bạn sẽ nhận được hiệu suất cao. Ngoài ra, danh sách trắng có thể là danh sách bí mật hoặc danh sách các nhóm. Danh sách các nhóm được sử dụng bởi nhiều người dùng và do đó được tập trung và có sẵn cho tất cả những người dùng được ủy quyền. Danh sách riêng tư, đặc biệt khi mỗi người dùng có một danh sách, có thể sẽ nhỏ hơn và có thể được lưu trữ trên bất kỳ chương trình hoặc thiết bị người dùng nào.

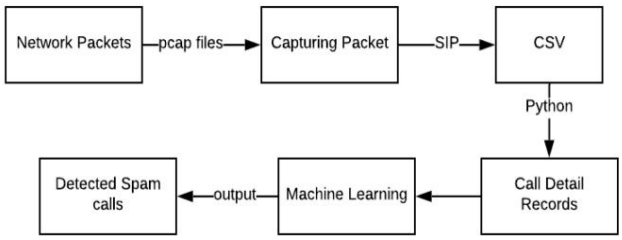
Danh sách đen: [3] Danh sách đen là danh sách các id người dùng bị đánh dấu là người xấu. Thường thì id người dùng trong danh sách đen của người nhận sẽ đạt hiệu suất cao. Danh sách riêng tư, đặc biệt trong đó mỗi người dùng có một danh sách, có thể ít hơn danh sách nhóm và có thể được lưu trữ thêm trong hệ thống hoặc hệ điều hành. Mặc dù danh sách đen có thể là danh sách riêng tư hoặc một nhóm các nhóm, nhưng phổ biến nhất là danh sách nhóm.

Sự tham gia của con người là quan trọng để phân biệt những người gọi không mong muốn. Mặc dù phương pháp này có thể tách những người gửi thư rác, nhưng nó rất khó khăn do quá yếu. [5] Sự tự tin và danh tiếng trong chương trình này được chia sẻ trên toàn miền chứ không phải bởi những người dùng khác nhau. Do đó, một miền cụ thể có số lượng thư rác cao hơn và ít người dùng thực tế hơn, những người dùng không an toàn đó có thể bị đổ lỗi và phần còn lại là thư rác. Người gọi có thể chọn trả lời hoặc từ chối cuộc gọi theo cách này.
Ngoài ra, Xếp hạng cuộc gọi tạo ra giá trị tích cực âm khi người dùng thực mới tham gia vào hệ thống VoIP. [5] Vì anh ta không có kết nối mạng xã hội với hệ thống đó, nên toàn bộ cuộc gọi của anh ta sẽ bị coi là cuộc gọi rác. Do sự tích hợp này sẽ có một số khó khăn. Mọi người dùng đều có quyền kiểm tra độ tin cậy của người dùng khác dựa trên sự tương tác của họ.

3. PHƯƠNG PHÁP ĐỀ XUẤT

Trong phần này, chúng tôi sẽ đề xuất mô hình của chúng tôi một cách chi tiết. Phát hiện thư rác VoIP bằng cách sử dụng máy học. Mô hình học máy sử dụng tương tác xã hội giữa những người dùng để phát hiện thư rác qua điện thoại internet (SPIT). [4] chúng ta phải tách các phản hồi SIP (Giao thức khởi tạo phiên) trong tập dữ liệu có định dạng pcap. Phản hồi SIP là câu trả lời cho các yêu cầu SIP, có nghĩa là phản hồi chứa thông tin và thời lượng cuộc gọi, v.v. chúng tôi có Một số thông tin cơ bản về phiên SIP trong Phần 3.1 để chúng tôi có thể hiểu tại sao chúng tôi tách các phản hồi SIP.





Hình 1: Lưu đồ

Nó thường có ba giai đoạn: Đầu tiên trích xuất các phản hồi SIP từ các tệp pcap và bằng cách sử dụng wirehark trên hệ điều hành linux và chuyển đổi chúng thành định dạng csv.

1	Caller	Callee	Duration
2	35	57	398
3	13	89	106
4	23	87	62
5	32	60	248
6	29	90	194
7	26	74	107

Hình 2: Tệp CSV

Thứ hai, bằng cách sử dụng tập lệnh python trên tệp csv, chúng tôi đã xóa các thông số phân loại của mình Bản ghi chi tiết cuộc gọi (CDR).

1	Caller	Callee	Duration	μ	σ	ψ
2	35	57	398	1	496	0.581818
3	13	89	106	1	106	0.792453
4	23	87	62	1	271.5	0.592593
5	32	60	248	1	321.75	0.782178
6	29	90	194	1	207.3333	0.657407
7	26	74	107	1	107	0.7

Hình 3: Bản ghi chi tiết cuộc

gọi Sau đó, chúng tôi đã sử dụng mô hình phân loại “Khu rừng ngẫu nhiên” để phát hiện spam qua các cuộc gọi VoIP.

3.1. Giao thức bắt đầu phiên

Trong phần này, chúng tôi mô tả mô hình được đề xuất của chúng tôi và bây giờ bằng cách sử dụng wirehark [4], chúng tôi phải tách các phản hồi SIP (Session Initiation Protocol) trong tập dữ liệu có định dạng pcap. Phản hồi SIP là câu trả lời cho các nhiệm vụ lại SIP, có nghĩa là phản hồi chứa thời lượng cuộc gọi và thời lượng đang hình thành, v.v. [4] Như bạn có thể thấy trong Hình 4 Tác nhân người dùng 'A' bắt đầu phiên, bằng cách gửi 'Mời yêu cầu 'tới Người dùng' B. Ứng dụng 'Mời' là cách đầu tiên trong ba cách để bắt tay. Tác nhân người dùng 'B' lặp lại giây và gửi phản hồi tạm thời cho 'Đang thử' trở lại Tác nhân người dùng 'A', theo sau là phản hồi tạm thời cho 'Đổ chuông', cho biết rằng điện thoại của người dùng B đang đổ chuông. Chẳng hạn như 'Đang cố gắng' và 'Nhẫn' .both là tạm thời (tự nguyện) lại

Hình 4: Phiên SIP

tài trợ, không được coi là một phần của ba bên
cái bắt tay [4]. Ngay sau khi người dùng B nhấc điện thoại,
Trả lời OK được thực hiện bởi Tác nhân người dùng 'B' và được gửi đến Người dùng
Đặc vụ 'A'. Tác nhân người dùng 'A' phản hồi bằng cách gửi ACK,
chỉ ra rằng nó vẫn sẵn sàng giao tiếp. Từ
thông báo 'OK' và ACK là thông báo thứ hai và thứ ba trong số
bắt tay ba chiều và tất cả các tham số phiên là
có thể hoán đổi cho nhau, phiên được thiết lập. Trong bài kiểm tra
của chúng tôi, Tác nhân Người dùng B kết thúc phiên bằng yêu cầu 'BYE',
được trả lời bởi Tác nhân người dùng A 'với sự đồng ý
tài trợ.

3.2. Tham số cuộc gọi

Trong phần này, chúng tôi đánh giá sự trình bày của
phương pháp tiếp cận mà chúng tôi đã được đề xuất để đánh giá. Trong
Ngoài việc trình bày điều này, chúng tôi cũng đã thảo luận về lời kêu gọi
tham số và đồ thị có trọng số để biết
hiệu suất phát hiện Người gửi thư rác và Bình thường
cuộc gọi. Ở đây chúng tôi đã xem xét ba loại tham số

3.2.1. Tỷ lệ cuộc gọi thành công

Đối với các cuộc gọi thành công, chúng tôi nhận được trung bình số lượng
cuộc gọi (cuộc gọi thành công) được thực hiện bởi người gọi i
đến số cuộc gọi được thực hiện bởi người gọi khác j. Chỉ định
tỷ lệ cuộc gọi hiệu quả dưới dạng mu và giá trị của nó được tính như trong
phương trình dưới đây. Giá trị mu nằm trong khoảng từ 0 đến 1. Nếu
mu là 0 cho biết rằng không có cuộc gọi đang hoạt động nào đang được thực hiện
bởi người dùng và khi nó hiển thị 1 thì cho biết rằng
cuộc gọi thành công.

$$\mu i\ j = \frac{\text{S uccess f ull cuộc gọi của người dùng i đến người dùng j}}{\text{T otal cuộc gọi do người dùng i khởi xướng đối với người dùng j}} \quad (1)$$

3.2.2. Thời gian đàm thoại trung bình cho mỗi cuộc gọi

Trong tham số này, chúng tôi đo độ dài của khoảng thời gian
của mỗi cuộc gọi từ người dùng I đến j. chúng tôi sử dụng sigma để tìm
thời gian nói chuyện trên điện thoại và giá trị của chúng tôi được tính
bằng phương trình dưới đây và giá trị sigma lớn hơn
hoặc bằng 0.

$$\sigma i\ j = \frac{\text{T otal T alk - thời gian trong cuộc gọi từ người dùng i rom cho người dùng j}}{\text{T otal thành công f ul cuộc gọi được thực hiện bởi người dùng i cho người dùng j}} \quad (2)$$

3.2.3. Vai trò của người dùng trong cuộc gọi

Nó là tỷ số giữa số lần người dùng u gọi và
số lần người dùng u đã gọi. Nó được tính bằng phương trình be
low.

$$\psi u = \frac{\text{Số lần người dùng u là người gọi}}{\text{Số lần người dùng u là một callee}} \quad (3)$$

4. THÍ NGHIỆM VÀ KẾT QUẢ

4.0.1. Tham số mô phỏng và tập dữ liệu

Thông số	Giá trị	Sự mô tả
Thời lượng cuộc gọi bình thường (giây). Hơn 20 giây Phân phối bình thường		
Thời lượng cuộc gọi spam (giây). Dưới 15 giây Phân phối Bình thường		
Số cuộc gọi Bình thường. 445336 Số cuộc gọi Spam 154664		được dán nhãn là 1
		được dán nhãn là 0

Bảng 1: Các thông số mô phỏng

Bản ghi dữ liệu cuộc gọi mẫu:

Thời lượng Calle của người gọi μ ψ						Nhãn mác
357,5 2,6520 47 64 5						1
1157 3				12	0,75 8,33	0
						1
				12		0
						0
						1
						0
			1	10		0

Bảng 2: Bản ghi dữ liệu cuộc gọi mẫu

4.1. Tập huấn luyện:

GIÁ TRỊ THÔNG SỐ	
Tổng số cuộc gọi 600000	
Cuộc gọi bình thường 445336	
Cuộc gọi rác 154664	
Tổng số người gọi VoIP 10000	

Bảng 3: Các thông số cho việc huấn luyện

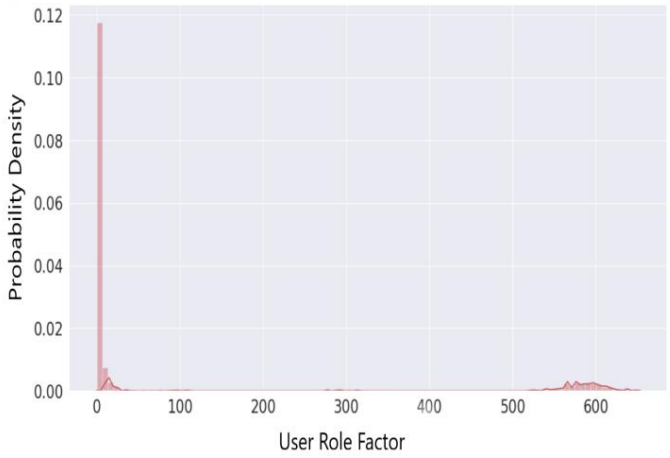
Từ Bảng trên.3 Đây là một số tham số
nằm trong Bộ thử nghiệm và ở đây tổng số cuộc gọi là 600000
nơi mà cuộc gọi bình thường 445336 và cuộc gọi rác 154664, tại đây
tổng số người dùng VoIP là 10000.

4.2. Bộ thử nghiệm

THÔNG SỐ Tổng số cuộc	GIÁ TRỊ
gọi Cuộc gọi bình	10000
thường Tổng số người	4000
gọi VoIP	100

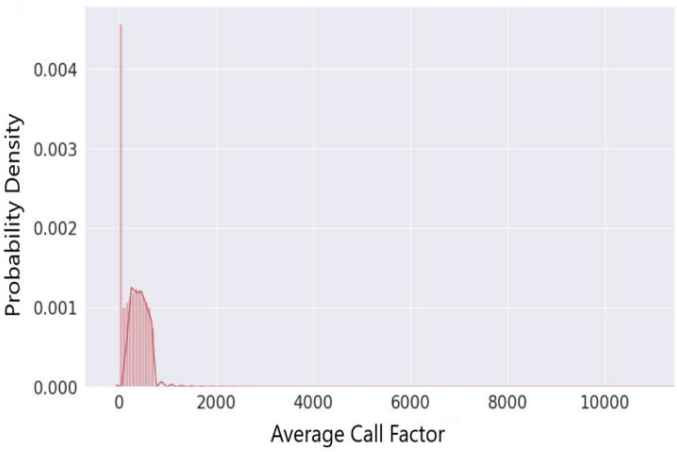
Bảng 4: Các thông số để kiểm tra

Từ Bảng trên.4 Đây là một số tham số
nằm trong Bộ thử nghiệm và ở đây tổng số cuộc gọi là 10000
trong đó như bình thường gọi 100 và ở đây là tổng số người dùng VoIP
là 100.



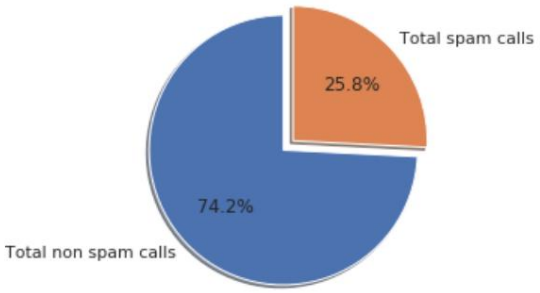
Hình 5: Vai trò của người dùng trong cuộc gọi

Biểu đồ mật độ cho thấy sự phân bố của một biến số.
Bằng cách biểu diễn đồ họa trên, nó truyền đạt rằng vai trò của người dùng trong cuộc gọi. Đó là biểu đồ dòng chảy- PSI so với nó về mật độ. Trên trục X, người dùng bình thường nằm trong phạm vi (0-dưới 3.0), điều này cho thấy rằng người dùng hoặc người dùng nam nằm trong phạm vi được chỉ định theo biểu diễn đồ họa và trong trường hợp người gửi thư rác, PSI dựa trên mật độ của nó nằm trên 3.0 và nó bắn tối đa 600 trở lên. Các cuộc gọi rác có mật độ ít hơn so với các cuộc gọi thông thường, đó là do vai trò người dùng của người gọi rác. Thông thường, Các cuộc gọi bình thường sẽ được hiển thị xung quanh (0,5-2).



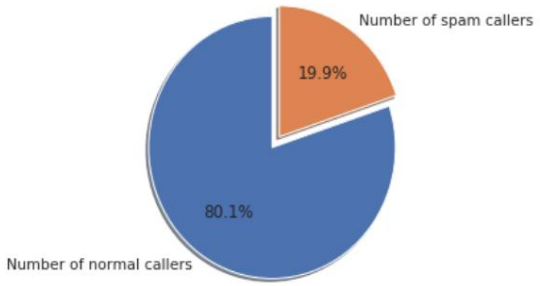
Hình 6: Thời gian đàm thoại trung bình

cho mỗi cuộc gọi Biểu đồ trên chỉ ra rằng người gửi thư rác đóng vai trò trong tham số thời gian thoại. Vì Người gửi thư rác có thời gian thoại thấp hơn rất nhiều so với Người dùng bình thường. Mật độ của Người dùng bình thường được quảng cáo ở một phạm vi cao hơn so với Người gửi thư rác. Biểu đồ này truyền tải rằng tổng diện tích được bao quanh bởi người dùng Nor mal cung cấp tổng diện tích khi tính toán, nó cho kết quả UNIT Khác với các loại có viền / phủ đều là spam
mers.



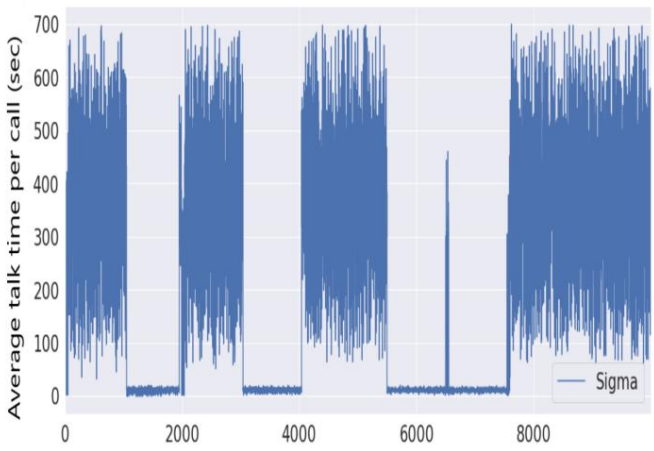
Hình 7: Số cuộc gọi

Biểu đồ hình tròn trên truyền đạt rằng tổng số cuộc gọi rác trên tổng số cuộc gọi bình thường.



Hình 8: Số lượng người gọi

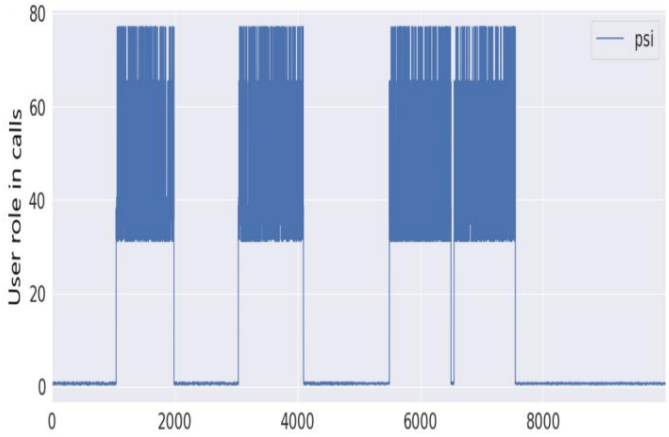
Biểu đồ hình tròn trên truyền đạt rằng tổng số người gọi spam trên tổng số người gọi bình thường.



Cuộc gọi VoIP

Hình 9: Kiểm tra sigma

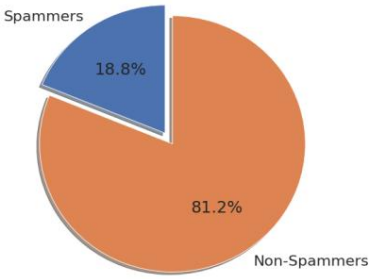
Biểu đồ đường thanh ở trên chuyển thông tin mà giá trị SIGMA cho cuộc gọi giữa người dùng Bình thường và người dùng Spam. Nó cho thấy rằng giá trị yếu tố SIGMA thấp hơn nữa đối với các cuộc gọi Spam (ví dụ: 0-7,5), trong khi giá trị SIGMA cho các cuộc gọi thông thường thay đổi từ (50-800)



Cuộc gọi VoIP

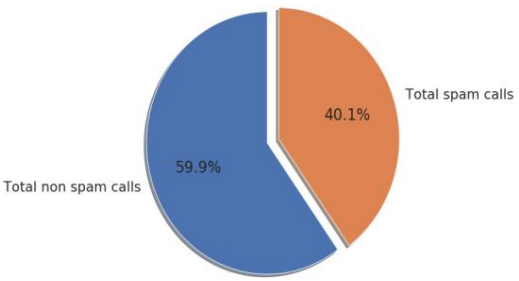
Hình 10: Kiểm tra Psi

Biểu đồ thanh ở trên chuyển cho chúng ta thông tin giá trị PSI cho các cuộc gọi giữa Người dùng bình thường và Người dùng Spam. Nó cho thấy rằng giá trị yếu tố PSI quá cao đối với các cuộc gọi Spam do những kẻ gửi thư rác thực hiện (ví dụ: 30-100), trong khi giá trị PSI cho các cuộc gọi Bình thường nhỏ hơn nữa, từ (0-2).



Hình 11: Kiểm tra người gọi

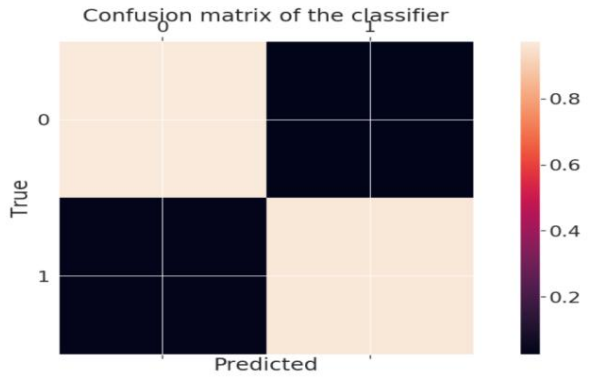
Biểu đồ hình tròn trên truyền đạt rằng tổng số người gọi spam trên tổng số người gọi bình thường



Hình 12: Kiểm tra cuộc gọi

Biểu đồ hình tròn trên truyền đạt rằng tổng số cuộc gọi rác trên tổng số cuộc gọi bình thường

5. Phân tích:

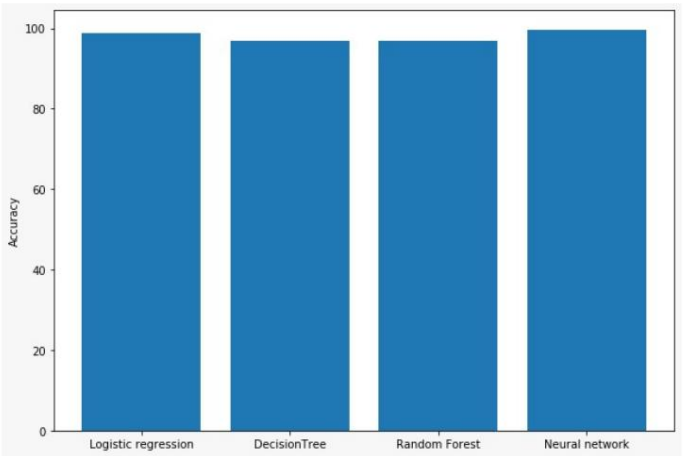


Hình 13: Phân tích

	Precision	Recall	f1-Score	Support
Spam	0.95	0.97	0.96	4001
Non-Spam	0.98	0.97	0.97	5999
Accuracy			0.97	10000
Macro avg	0.97	0.97	0.97	10000
Weighted avg	0.97	0.97	0.97	10000

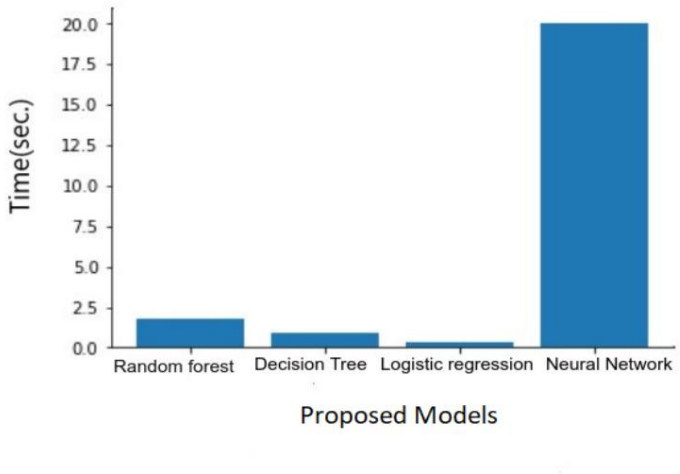
Hình 14: Ma trận nhầm lẫn Báo cáo

phân loại Phân tích này được sử dụng để biết chất lượng của các ước tính từ một thuật toán phân loại. Bằng cách này, chúng ta có thể biết có bao nhiêu dự đoán là Đúng và bao nhiêu dự đoán là Sai. Hình 14 là báo cáo phân loại ma trận.



Hình 15: Độ chính xác cho các kiểu máy khác nhau

Nhiều kỹ thuật đã được phát triển để giúp các chuyên gia hiểu rõ các mô hình phân loại. Mô hình phân loại cố gắng thu được một kết luận cụ thể từ các giá trị đầu vào được đưa ra để đào tạo. Nó sẽ dự đoán nhãn / danh mục phục vụ cho dữ liệu mới. Chúng tôi đã phân tích quá trình đào tạo và thử nghiệm bộ dữ liệu của chúng tôi qua các mô hình phân loại khác nhau như rừng Ran dom, cây quyết định. Chúng tôi cũng đã xây dựng một mô hình học sâu với mạng nơ-ron để phân loại tập dữ liệu đào tạo và kiểm tra của chúng tôi. Kết quả về độ chính xác của các mô hình khác nhau và thời gian thực hiện của từng mô hình được mô tả trong đồ thị Hình 15 và Hình 16:



Hình 16: Đồ thị thời gian

6. Thảo luận

Khi hệ thống điện thoại chuyển sang mạng 'tất cả IP' và mạng IP có vấn đề về độ tin cậy, nhiều mối đe dọa đang chạy trên mạng IP đột nhiên hoạt động với điện thoại. [3] Khi việc sử dụng điện thoại dựa trên IP ngày càng trở nên hấp dẫn hơn đối với một loại Thư rác mới, Thư rác VoIP. Vì trong mạng VoIP chi phí (ví dụ thời gian và tiền bạc) của nhà phát triển thấp hơn chi phí (ví dụ thời gian và tiền bạc) cho người nhận, VoIP Spam là một vấn đề tiềm ẩn.

Trạng thái hiện tại của mạng Giao thức thoại qua Internet yêu cầu người gọi SPIT (Thư rác qua điện thoại Internet) phải được khuyến khích gọi trong khi cài đặt cuộc gọi thay vì chặn trong khi trao đổi thoại sau khi cài đặt điện thoại [16]. Tính năng phát hiện thư rác bằng phương pháp chỉnh sửa cuộc gọi giúp tăng cường sự hài lòng từ việc không nhận các cuộc gọi không cần thiết và cải thiện việc sử dụng các tài nguyên dành riêng cho người gọi thực. [số 8]
Thu thập dựa trên SPIT dựa trên nội dung không phải là một lựa chọn khả thi vì nó yêu cầu các nguồn nhận dạng giọng nói và xử lý giọng nói, cơ sở dữ liệu lời nói spam được cập nhật và các lệnh gọi Không gửi spam để phân tích dữ liệu theo thời gian thực và ngày càng khó sử dụng trong giọng nói được mã hóa. [10] Ngoài ra, quy trình phát biểu mâu thuẫn với việc bảo vệ dữ liệu người dùng. Các meth dựa trên danh sách đòi hỏi sự cẩn thận khi nhận được các cuộc gọi từ nhiều nguồn khác nhau. Các phương pháp dựa trên sự khen ngợi bao gồm trạng thái của người gọi bằng cách nhận cuộc gọi từ người gọi hoặc sử dụng thời gian gọi cố định, nhưng dựa vào người gọi để đưa ra kết quả cuối cùng bằng cách từ chối hoặc nhận cuộc gọi.

7. Kết luận

Các mạng máy tính đang phải đối mặt với nhiều mối đe dọa như thư rác VoIP, v.v. mà người dùng không nhận thức được. [9] Pháp y mạng là cần thiết vì nhiều phương pháp được thực hiện cho an ninh mạng không đủ hiệu quả để phát hiện tất cả các cuộc tấn công trên mạng. Wireshark là một trong những công cụ hiệu quả nhất để nắm bắt và phân tích các gói tin trong pháp y mạng vì các tính năng phong phú và khả năng hiển thị thông tin càng chi tiết càng tốt. Trong Phát hiện thư rác Giao thức thoại qua Internet (VOIP) này, chúng tôi đã đưa ra một phương pháp kết hợp các giao thức và đặc điểm của người gọi. Hệ thống này cung cấp cho chúng tôi một cách đơn giản và dễ dàng để sử dụng thời gian cuộc gọi (Thời gian) như một thông tin liên quan được chọn tự động dựa trên người gọi và Callee. [13] Quy trình được đề xuất tiếp tục được thực thi phù hợp với việc ra quyết định và suy nghĩ có đạo đức của con người. Tuy nhiên, người dùng thực tế có thể được nhân đôi cho các cuộc gọi dài hạn. Điều này hỗ trợ cả hai biểu đồ giao tiếp theo chiều về quyết định của người dùng thực tế. Đối với một số tính năng Phát hiện lều cũ, chúng tôi thường thêm một phương pháp được sử dụng để tăng độ tin cậy trong trường hợp người gọi không có tàu quan hệ trực tiếp. Kết quả mô phỏng chính xác được hỗ trợ, [7] chúng tôi nhận thấy rằng quá trình dự đoán sẽ thấy toàn bộ Spam Over Internet Telephony (SPIT) khi một số giai đoạn học tập giữ một lượng ngắn tỷ lệ dương tính giả. Chúng tôi cũng đảm bảo rằng khi số lượng thư rác tăng lên thì số lượng thư rác thực tế và các cuộc điện thoại thực tế vẫn cao hơn lần lượt là 95 và 98%. Mối quan hệ giữa các cá nhân này sẽ không ảnh hưởng đến độ chính xác của việc mua lại. Ở đây chúng tôi kết luận rằng phương pháp đề xuất của chúng tôi có thể được sử dụng trong Mạng giao thức thoại qua Internet thực tế.

Người giới thiệu

[1] Goode, B. (2002). Giao thức thoại qua internet (VoIP). Kỷ yếu của IEEE, 90 (9), 1495-1517

[2] Dantu, Ram và Prakash Kolan. "Phát hiện Spam trong Mạng VoIP." SRUTI 5 (2005): 5-5.

[3] Mathieu, Bertrand, Saverio Niccolini và Dorgham Sisalem. "SDRS: một hệ thống phát hiện và phản ứng thư rác bằng giọng nói qua IP." IEEE Security Privacy 6, không. 6 (2008): 52-59.

[4] Rosenberg, Jonathan, Henning Schulzrinne, Gonzalo Camarillo, Alan Johnston, Jon Peterson, Robert Sparks, Mark Handley và Eve Schooler. "SIP: giao thức bắt đầu phiên." (Năm 2002).

[5] Chaisamran, Noppawat, Takeshi Okuda và Suguru Yamaguchi. "Phát hiện spam voip dựa trên niềm tin dựa trên các hành vi gọi điện và các mối quan hệ của con người." Tạp chí Xử lý Thông tin 21, số. 2 (2013): 188-197.

[6] Reumann, J., Saha, D., Shae, ZY và Sripanidkulchai, K., Abbott Laborato ries và International Business Machines Corp, 2007. Hệ thống và phương pháp phát hiện thư rác. Đơn đăng ký bằng sáng chế Hoa Kỳ 11 / 334,920.

[7] Piche, C., Eyeball Networks Inc, 2010. Phương pháp và hệ thống ngăn chặn thư rác qua điện thoại internet. Đơn đăng ký bằng sáng chế Hoa Kỳ 12 / 067,168.

[8] Quittek, Juergen, Saverio Niccolini, Sandra Tartarelli và Roman Schlegel. "Về ngăn chặn thư rác qua điện thoại internet (SPIT)." Tạp chí Truyền thông IEEE số 46, số. 8 (2008): 80-86.

[9] Rao A, McRae M, Harrington K, Huotari A, các nhà phát minh; Cisco Technology Inc, đơn vị được chuyển nhượng. Phương pháp và hệ thống ngăn chặn SPam qua điện thoại Giao thức Internet và Nhắn tin tức thời SPam. Đơn xin cấp bằng sáng chế Hoa Kỳ US 11 / 203.449. 2007 ngày 22 tháng 2.

[10] MacIntosh, Robert và Dmitri Vinokurov. "Phát hiện và giảm thiểu thư rác trong mạng điện thoại IP bằng cách sử dụng phân tích giao thức báo hiệu." Trong Hội nghị chuyên đề IEEE / Sarnoff về những tiến bộ trong giao tiếp có dây và không dây, 2005., trang 49-52. IEEE, 2005.

[11] Rebahi, Yacine, Dorgham Sisalem và Thomas Magedanz. "Phát hiện spam." Trong Hội nghị Quốc tế về Viễn thông Kỹ thuật số (ICDT'06), trang 68-68. IEEE, 2006.

[12] Huang, H., Yu, HT và Feng, XL, 2009, tháng 11. Một phương pháp phát hiện khạc nhổ bằng cách sử dụng phân tích hoạt động giọng nói. Năm 2009, Hội nghị Quốc tế về Mạng và An ninh Thông tin Đa phương tiện (Tập 2, trang 370-373). IEEE.

[13] Kim, Hyung-Jong, Myuhng Joo Kim, Yoonjeong Kim và Hyun Cheol Jeong. "Mô hình dựa trên DEVS về hành vi của người gọi spam VoIP để tính mức SPIT." Thực hành và lý thuyết mô hình mô phỏng 17, không. 4 (2009): 569-584.

[14] Vinokurov, Dmitri và Robert W. MacIntosh. "Phát hiện và giảm thiểu các cuộc gọi hàng loạt không mong muốn (thư rác) trong mạng VoIP." Bằng sáng chế Hoa Kỳ 7.307.997, cấp ngày 11 tháng 12 năm 2007.

[15] Jones, Wesley Stuart, Timothy Cotton và Robert Victor Holland. "Hệ thống và phương pháp thoại qua giao thức internet." Bằng sáng chế Hoa Kỳ 6.141.341, cấp ngày 31 tháng 10 năm 2000.

[16] Rao, Anup, Matthew McRae, Kendra Harrington và Allen Huotari. "Phương pháp và hệ thống ngăn chặn SPam qua điện thoại Giao thức Internet và Nhắn tin tức thời SPam." Đơn đăng ký bằng sáng chế Hoa Kỳ 11 / 203.449, nộp ngày 22 tháng 2 năm 2007.

[17] Piche, Christopher. "Phương pháp và hệ thống để ngăn chặn thư rác qua điện thoại internet." Đơn xin cấp bằng sáng chế Hoa Kỳ 12 / 067,168, nộp ngày 9 tháng 9 năm 2010.

[18] Shaw, Urjashee và Bobby Sharma. "Một bài khảo sát về giao thức thoại qua internet (VOIP)." Tạp chí Quốc tế về Ứng dụng Máy tính 139, số. 2 (2016): 16-22.

[19] Dritsas, Stelios, John Mallios, Marianthi Theoharidou, Giannis F. Marias, và Dimitris Gritzalis. "Phân tích mối đe dọa của giao thức bắt đầu phiên liên quan đến thư rác." Năm 2007 Hội nghị Hiệu suất, Máy tính và Truyền thông Quốc tế IEEE, trang 426-433. IEEE, 2007.

[20] Baumann, Rainer, Stéphane Cavin và Stefan Schmid. "Thoại qua IP-bảo mật và SPIT." Quân đội Thụy Sĩ, FU Br 41 (2006): 1-34.

[21] Hwang, Lin Yuh-Ing, Leroy Lacy và Li Ling. "Phương pháp phát hiện thư rác qua điện thoại internet (SPIT)." Bằng sáng chế Hoa Kỳ 8.141.152, cấp ngày 20 tháng 3 năm 2012.

[22] Bai, Y., Su, X. and Bhargava, B., 2009, June. Phát hiện và lọc Thư rác qua Điện thoại Internet – một phương pháp dựa trên mạng trung gian nhận biết hành vi của người dùng. Năm 2009 Hội nghị quốc tế IEEE về đa phương tiện và hội chợ triển lãm (trang 726-729). IEEE.