MỞ ĐẦU

Cùng với sự phát triển của Internet, các mạng xã hội đã phát triển mạnh mẽ và trở thành một xu hướng mới thu hút nhiều người sử dụng trên internet. Ngoài những lợi ích mạng xã hội mamg lại, người dùng trên mạng xã hội còn phải đối mặt với nhiều nguy cơ mất an toàn. Một trong những nguy cơ đó là người dùng bị tấn công, xâm nhập lấy cắp thông tin một cách chủ đích. Hoạt động *xâm nhập* đơn giản là gửi yêu cầu kết bạn một cách chủ động với ý đồ xấu như gửi thư rác, phát tán virus, lừa đảo. Đặc biệt, khi người bị tấn công là người dùng trong một tổ chức cụ thể, những thông tin của họ không chỉ là thông tin cá nhân mà còn là những thông tin liên quan đến tổ chức mà họ tham gia. Trong các nghiên cứu liên quan [5, 7, 6, 4] đã chỉ ra rằng, việc xâm nhập tới người dùng khá dễ dàng với tỷ lệ xâm nhập thành công cao từ 50 đến 70 %. Điều này cho thấy người dùng có xu hướng chưa cẩn trọng trong việc chọn bạn bè của mình trên mạng xã hội.

Thúc đẩy bởi thực tế và nghiên cứu trên, tác giả nhận thấy việc đưa một giải pháp để phòng ngừa sự xâm nhập tới người dùng trên mạng xã hội mang tính cấp thiết bởi sự chủ quan và nhận thức của người dùng về sự nguy hiểm của hoạt động tấn công. Vì vậy, trong luận văn này, tác giả nghiên cứu "**Một giải pháp phòng ngừa xâm nhập trên mạng xã hội trực tuyến**". Đóng góp chính của luận văn là đưa ra một giải pháp phòng ngừa xâm nhập đối với một tổ chức người dùng. Ngoài phần kết luận, bố cục chính của luận văn gồm bốn chương như sau:

Chương 1: Giới thiệu về mạng xã hội

Chương này giới thiệu tổng quan về mạng xã hội gồm: Định nghĩa, sự hình thành và phát triển của mạng xã hội, đặc tính của mạng xã hội.

Chương 2: Các nguy cơ mất an toàn trên mạng xã hội

Chương này trình bày các nguy cơ mất an toàn trên mạng xã hội. Tác giả đi sâu phân tích hoạt động của kẻ tấn công nhằm lấy cắp thông tin của người dùng và đặc biệt hành vi tấn công của Socialbots trên mạng diện rộng.

Chương 3: Giải pháp phòng ngừa xâm nhập lấy thông tin trên mạng xã hội đối với mỗi các nhân trong tổ chức

Chương này trình bày những kết quả chính của luận văn. Trong chương này tác giả đề xuất một giải pháp phòng ngừa sự xâm nhập dựa trên sự phân tích hoạt động tấn công có chủ đích tới người dùng trong một tổ chức cụ thể.

Chương 4: Thực nghiệm

Chương này trình bày kết quả thực nghiệm trên dữ liệu mạng xã hội thực Facebook. Thực nghiệm chọn ra những tổ chức có kích cỡ khác nhau sau đó xây dựng giải pháp phòng ngừa ở chương 3 đối với những tổ chức đã chọn.

Chương 1

GIỚI THIỆU VỀ MẠNG XÃ HỘI

1.1 Giới thiệu chung về mạng xã hội

Mạng xã hội, hay gọi là mạng xã hội ảo (tiếng Anh: Social network) là dịch vụ nối kết các thành viên cùng sở thích trên Internet lại với nhau với nhiều mục đích khác nhau không phân biệt không gian và thời gian. Những người tham gia vào mạng xã hội còn được gọi là cư dân mạng.

Một mạng xã hội thông thường có những tính năng như: chat, e-mail, phim ảnh, voice chat, chia sẻ file, blog và xã luận. Có nhiều cách để các thành viên tìm kiếm bạn bè, đối tác đó là: dựa theo các nhóm (ví dụ như tên trường hoặc tên thành phố), dựa trên thông tin cá nhân (như địa chỉ e-mail hoặc screen name), hoặc dựa trên sở thích cá nhân (như thể thao, phim ảnh, sách báo, hoặc ca nhạc), lĩnh vực quan tâm: kinh doanh, mua bán. Nhờ vào các tính năng này, mạng xã hội có thể kết nối mọi người, chia sẻ sở thích và hoạt động không phân biệt chế độ chính trị, kinh tế và khoảng cách.

Số lượng người dùng mạng xã hội trên toàn cầu tăng nhanh chóng trong những năm gần đây, theo thống kê của các nhà khoa học, mỗi ngày có hàng tỷ người trên thế giới sử dụng tất cả các mạng xã hội [1]. Đối với mạng xã hội Facebook , tính trung bình mỗi người dùng dành 7 giờ và 45 phút mỗi tháng [3]; 32 triệu lượt like và comment mỗi ngày trên Facebook [2]. Những số liệu này cho thấy càng ngày càng có nhiều người dùng sử dụng mạng xã hội và mạng xã hội đã trở thành một xu hướng lớn với tất cả người dùng trên Internet. Cũng theo xu hướng này, các mạng xã hội mới được lập để khai thác các khía cạnh khác nhau đáp ứng toàn diện nhu cầu người dùng.

1.1.1 Lịch sử phát triển của mạng xã hội

Mạng xã hội xuất hiện lần đầu tiên năm 1995 với sự ra đời của trang Classmate với mục đích kết nối bạn học với nhau. Tiếp theo là sự xuất hiện của SixDegreesvào năm 1997 với mục đích giao lưu kết bạn dựa theo sở thích. Năm 2002, mạng xã hội Friendster ra đời và trở thành một trào lưu mới tại Hoa Kỳ với hàng triệu người dùng đăng ký. Kế thừa các bước phát triển của các mạng xã hội đi trước, năm 2004 mạng xã hội MySpace ra đời với nhiều tính năng mới cho phép người dùng tải các hình ảnh video nhanh chóng thu hút hàng chục ngàn thành viên mới mỗi ngày. Năm 2006, sự ra đời của mạng xã hội Facebook đánh dấu bước ngoặt mới cho hệ thống mạng xã hội trực tuyến. Ngày nay có hàng trăm

mạng xã hội trên toàn thế giới, nhìn chung MySpace và Facebook là những mạng xã hội nổi tiếng nhất.

1.1.2 Những đặc điểm chung của mạng xã hội

Khả năng truyền tài và lưu trữ thông tin:
Một đặc điểm quan trọng trên mạng xã hội là những thông tin, xu hướng trên mạng xã hội được lan truyền rộng rãi trong thời gian ngắn.

Tính đa phương tiện:
Hoạt động theo nguyên lý của web 2.0, mạng xã hội có rất nhiều tiện ích nhờ sự kết hợp các yêu tố văn bản, âm thanh, hình ảnh. Một trang mạng xã hội giống có thể cung cấp nhiều ứng dụng khác nhau cho người dùng.

Tính liên kết cộng đồng:

Đây là đặc điểm của mạng xã hội cho phép mở rộng phạm vi kết nối giữa con người với cong người trong một không gian phi thực. Người sử dụng có thể trở thành bạn của nhau thông qua việc lời mời kết bạn mà không cần gặp gỡ trực tiếp. Việc tạo ra liên kết này tạo ra một cộng đồng mạng với số lượng thành viên lớn.

Cấu tạo mạng xã hội: Về cấu tạo, nhìn chung mỗi mạng xã hội đều được cấu thành bởi hai yêu tố chính sau:

- Nut (node): Là một thực thể trong mạng, thực thể này thường biểu diễn mỗi người dùng trong mạng.
- Liên kết (tie, link): là mối quan hệ giữa các thực thể đó. Trong mạng xã hội có nhiều kiểu liên kết khác nhau như: liên kết vô hướng, liên kết có hướng.

Với cấu trúc mạng xã hội như trên, đối với các bài toán liên quan đến mạng xã hội, chúng ta có thể mô hình hóa mạng xã hội bằng đồ thị.

1.2 Lợi ích của mạng xã hội

Với đặc tính lan truyền thông tin nhanh chóng đối với người dùng. Mạng xã hội có nhiều ứng dụng quan trọng trong tất cả các lĩnh vực, trong đó có một số lĩnh vực quan trọng là: kinh doanh, giáo dục, chính trị, y tế và các ứng dụng đối với chính phủ.

1.3 Một số vấn đề được nghiên cứu trên mạng xã hội

1.3.1 Khai phá dữ liệu trên mạng xã hội

Khai phá dữ liệu trên mạng xã hội thực chất là một bài toán không mới vì các mạng xã hội thực chất các mạng xã hội là những trang web. Tuy vậy, do những

đặc điểm riêng của mạng xã hội, việc khai phá và phân tích dữ liệu cũng có nhiều hướng tiếp cận, phương pháp và mục tiêu khác.

1.3.2 Phát hiện cấu trúc cộng đồng trên mạng xã hội

Một mạng lưới được gọi là có cấu trúc cộng đồng nếu như các đỉnh trong mạng có thể dễ dàng nhóm lại thành các tập hợp (có khả năng chồng chéo) sao cho trong tập hợp đó mật độ kết nối giữa các đỉnh biên trong lớn hơn các đỉnh ở bên ngoài [27]. Việc đánh giá cộng đồng có thể dựa theo các tiêu chí sau: Modularity [43], mật độ [44], phương pháp sử dụng các quá trình ngẫu nghiên [40], sử dụng thuộc tính của các đỉnh [41].

1.3.3 Tối đa hóa lan truyền thông tin trên mạng xã hội

Bài toán tối đa hóa ảnh hưởng *(Influence Maximizing)* xuất phát từ nhu cầu thực tiễn khi cần chọn một số lượng k người dùng (giới hạn nguồi lực) để khởi tạo quá trình lan truyền hoặc bắt đầu ảnh hưởng (gọi là tập hạt giống) sao cho số người bị ảnh bởi thông tin lan truyền là cực đại. Kemp [38] là người đầu tiên phát biểu bài toán này trên mô hình mạng xã hội. Đồng thời, ông cũng đã đưa ra hai mô hình lan truyền thông tin là mô hình ngưỡng tuyến tính (Linear Threshold) và mô bậc độc lập (Independent Cascade). Hiện nay, lớp bài toán tối đa hóa ảnh hưởng trên mạng xã hội có nhiều hướng phát triển khác nhau, có thể kể ra một số nghiên cứu liên quan là: [31][32] [55][33].

1.3.4 Phát hiện, giám sát và ngăn ngừa thông tin sai lệnh trên mạng xã hội

Trong thực tế trên mạng xã hội luôn tồn tại những thông tin lệnh lạc, không lành mạnh gây ra ảnh hưởng tiêu cực đến người dùng trên mạng xã hội. Hơn nữa với sự lan truyền thông tin nhanh chóng trên mạng xã hội, nếu những thông tin sai lệnh này đến được nhiều người dùng thì hậu quả sẽ càng lớn. Đối với những vấn đề mang tính xã hội, những thông tin sai lệnh ảnh hưởng tiêu cực đến tâm lý, đời sống tinh thần của người dùng khi chúng được phát tán trên mạng. Các nghiên cứu liên quan điển hình đến vấn đề này là [48] [39].

1.3.5 Phát hiện, ngăn chặn rò rỉ thông tin trên mạng xã hội

Một nguy cơ đối với người dùng khi sử dụng mạng xã hội là sự rò rỉ thông tin. Thông tin bị rò rỉ ở đây có thể là các thông tin cá nhân người dùng như: e-mail, địa chỉ, cơ quan, sở thích, bạn bè vv.. Kẻ xấu có thể dùng các thông tin này để lừa đảo, gửi spam, phát tán virus vv.. Các nghiên cứu liêu quan đến vấn đề này là [51] [53].

Chương 2

CÁC NGUY CƠ MẤT AN TOÀN TRÊN MẠNG XÃ HỘI

2.1 Các nguy cơ mất an toàn truyền thống

2.1.1 Mã độc

Mã độc (*Malware*) là phần mềm độc hại được phát triển để thu thập thông tin của người dùng và truy cập vào thông tin cá nhân của họ. Mã độc sử dụng cấu trúc của các mạng xã hội để lan rộng giữa người dùng và bạn bè của họ.

2.1.2 Phishing

Phishing hay lừa đảo là một dạng của các kỹ thuật tấn công xã hội (social engineering) để lấy được những thông tin riêng tư, có giá trị của người dùng bằng cách giả mạo một người đáng tin cậy trên mạng.

2.1.3 Gửi thư rác

Thư rác (*Spammers*) là thư điện tử được gửi đến người dùng mà họ không mong muốn. Nội dung của các thư này thường là các thông điệp quảng cáo. Kẻ gửi thư giác trên MXH sử dụng nền tảng sãn có của mạng xã hội để gửi các thông điệp quảng cáo đến người dùng khác bằng cách tạo một tài khoản giả mạo.

2.1.4 Tấn công CSS

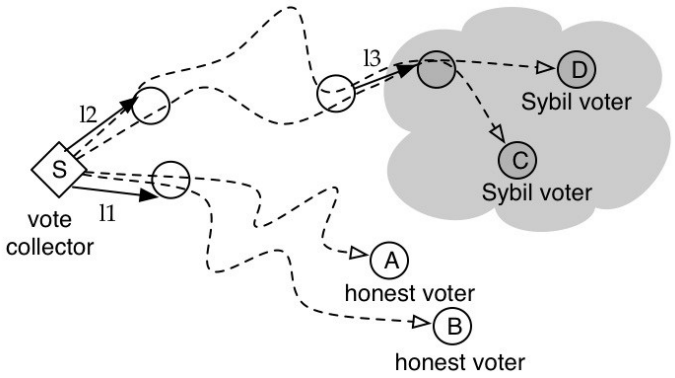
Tân công CSS (*Cross-Site Scripting*) là một kĩ thuật tấn công bằng cách chèn vào các website động (ASP, PHP, CGI, JSP ...) những thẻ HTML hay những đoạn mã script nguy hiểm có thể gây nguy hại cho những người sử dụng khác.

2.1.5 Lừa đảo trên Internet

Lừa đảo trên Internet (*Internet Fraud*): hay còn gọi là lừa đảo trên mạng, dùng để chỉ sự truy cập Internet để lừa đảo hay lợi dụng người dùng trên mạng. Hình thức lừa đảo này xuất phát từ những hình thức lừa đảo trong mạng xã hội thực.

2.2 Tấn công mạo nhận (Sybil attack)

Một hình thức tấn công được các hacker sử dụng là thủ thuật tạo ra nhiều trang web trên nhiều tên miền khác nhau một cách có chủ ý, liên kết đến nhau nhằm tăng thứ hạng cho 1 hay 1 nhóm website cụ thể. Sau đó lợi dụng việc các search engine xem 1 website là có tầm quan trọng cao hơn khi nhiều website khác liên kết đến nó.



Hình 2.1: Tấn công mạo nhận

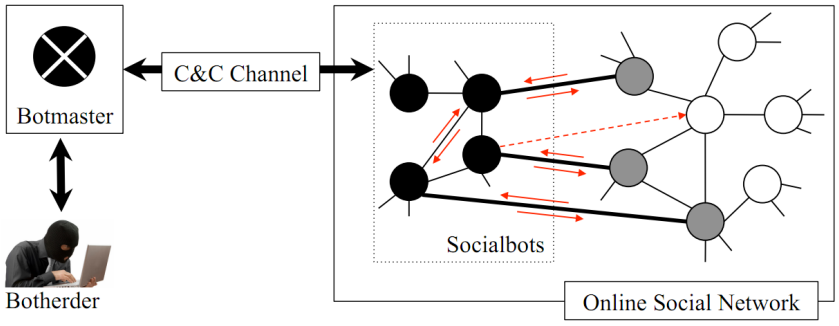
2.3 Rò rỉ thông tin trên mạng xã hội

2.3.1 Nguyên nhân chủ quan

Trong nguyên nhân chủ quan, người dùng vô tình làm lộ lọt thông tin của mình thông qua hình thức chia sẻ thông tin, đăng bài hoặc sử dụng các chức năng khác của mạng xã hội. Thông tin này vô tình sẽ đến được với những người dùng mà họ không mong muốn biết được thông tin này. Các nghiên cứu tiêu biểu về vấn đề này là [51] [53].

2.3.2 Nguyên nhân khách quan

Đối với nguyên nhân khách quan, kẻ tấn công chủ đích thực hiện các cuộc tấn công đến người dùng nhằm lấy thông tin người dùng, như: địa chỉ email, thông tin bạn bè, thông tin nơi làm việc, các tổ chức của họ tham gia..hoặc có thể là những thông tin có giá trị như tài khoản người dùng. Trong nghiên cứu liên quan đến vấn đề này, Bosmanf [6] đã thiết kế một Socialbots (là những một tài khoản giả trên mạng xã hội) bắt chước các hành động của người dùng thật rồi tấn công đến người dùng thật bằng cách gửi yêu cầu kết bạn đến họ. Nếu người dùng chấp nhận yêu cầu kết bạn, Socialbot sẽ ngay lập tức có được các thông tin cá nhân của người dùng qua đó thực hiện các chiến lược phát tán thư rác quy mô lớn. Kẻ tấn công cũng có thể dùng các thông tin của người dùng để giả mạo người dùng

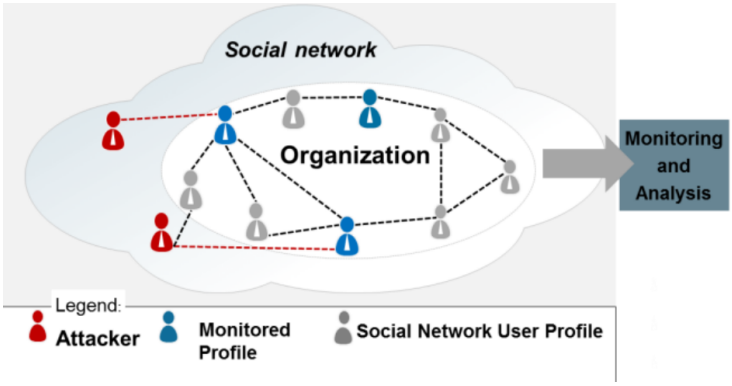


Hình 2.2: Socialbot tấn công đến người dùng

để lừa đảo bạn bè, người thân của họ hoặc thực hiện bán hàng trực tuyến trên mạng

2.4 Tấn công xâm nhập, lấy cắp thông tin đối với cá nhân trong tổ chức

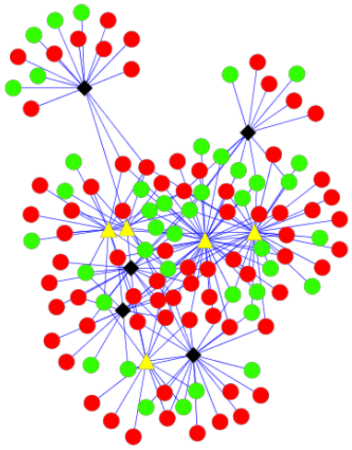
Kẻ tấn công có thể thực hiện các cuộc tấn công đến những người dùng trong một tổ chức để lấy thông tin của người dùng cũng như thông tin về tổ chức mà họ đang tham gia. Những thông tin này được kẻ tấn công sử dụng để tái tạo lại bộ máy tổ chức trong thế giới thực hoặc sử dụng cho các mục đích xấu. Yashar



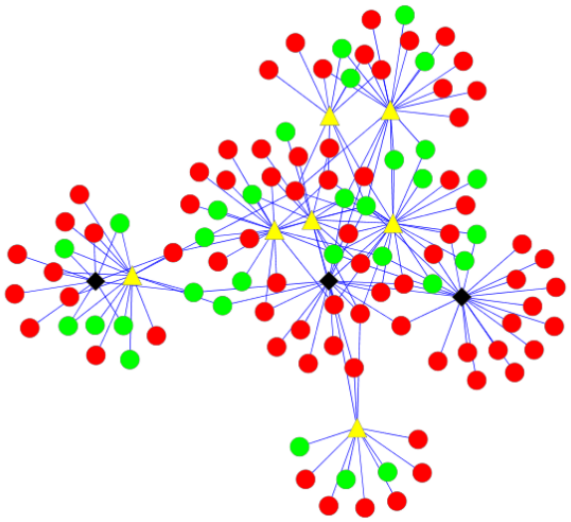
Hình 2.3: Kẻ tấn công xâm nhập lấy cắp thông tin của người dùng trong tổ chức

[4] đã đề xuất một phương pháp kết hợp tất cả các nghiên cứu [5, 6, 7] sử dụng Socialbot để thâm nhập vào người sử dụng cụ thể trong tổ chức mục tiêu. Họ tạo ra ba Socialbot S_1, S_2, S_3 để tấn công công đến ba tổ chức trên mạng xã hội Facebook gọi là O_1, O_2, O_3.

Các Socialbots này họ xâm nhập đến người dùng đích trong một tổ chức bằng cách tạo ra sự tin tưởng cho họ thông qua những người bạn của họ theo phương thức như sau: Đầu tiên, chúng tạo ra thông tin cá nhân giống như người dùng thật. Sau đó chúng gửi kết bạn với ít nhất 50 người dùng bất kỳ trên mạng xã hội, với việc lựa chọn những người có trên 1000 bạn trên mạng xã hội. Socialbot xác định tổ chức đích cần tấn công và chọn ra 10 người dùng trong mỗi tổ chức này. Trước khi gửi yêu cầu kết bạn tới mỗi người dùng đích này, các Socialbot gửi yêu



Kết quả tấn công của S_1 với tổ chức O_1



Kết quả tấn công của S_2 với tổ chức O_2

cầu kết bạn tới những người bạn của người dùng đích để tạo mối tin tưởng qua bạn bè của họ. Cuối cùng chúng gửi yêu cầu kết bạn đến người dùng đích trong tổ chức. S_3 bị vô hiệu hóa do người dùng trong tổ chức thuộc các quốc gia khác nhau đo đó, việc gửi yêu cầu kết bạn với ý đồ xấu dễ dàng bị nhận ra do sự đề phòng cua người dùng. Ngược lại, các Socialbot S_1, S_2 xâm nhập với hiệu quả cao. Qua nghiên cứu trên, họ chỉ ra rằng thật dễ dàng để xâm nhập tới người dùng đích và tỷ lệ thành công của việc xâm nhập là 50 % và 70 % [4]. Họ cũng cũng đưa ra nhận định rằng số lượng người bạn chung chấp nhận yêu cầu kết bạn càng lớn thì khả năng xâm nhập càng cao. Nghiên cứu này cũng cho thấy một thực tế rằng khả năng rò rỉ, bị lấy thông thông tin của người sử dụng rất cao, người sử dụng nên cẩn thận hơn trong việc lựa chọn bạn bè trên các mạng xã hội. Người dùng không nhận thức được khả năng các nguy cơ tấn công này, họ cần có những sự lựa chọn tốt hơn về bạn bè của họ trên mạng xã hội. Kẻ tấn công có thể thực hiện biện pháp này trên mạng diện rộng để thu thập được các thông tin người dùng. Với tỷ lệ thành công trên, cũng có thể nói họ cũng có thế lấy được thông tin từ nhiều tổ chức bằng phương pháp tương tự.

Qua nghiên cứu này, tác giả nhận thấy rằng viêc bảo vệ người dùng trong tổ chức trước sự xâm nhập của các Socialbots là một thách thức lớn cần giải quyết. Cần phải có một giải pháp hiệu quả để phòng ngừa, khuyến cáo trước sự xâm nhập trên. Do vậy, trong luận văn này, tác giả mạnh dạn đề xuất một giải pháp nhằm nhằm phòng ngừa sự xâm nhập. Chi tiết giải pháp này sẽ được luận văn trình bày ở Chương 3.

Chương 3

PHÒNG NGỪA SỰ XÂM NHẬP LẤY THÔNG TIN ĐỐI VỚI NGƯỜI DÙNG TRONG TỔ CHỨC

3.1 Phát biểu bài toán

Như đã trình bày ở chương 2, kẻ tấn công có thể thực hiện hoạt động xâm nhập đến người dùng trong tổ chức để lấy thông tin sau đó sử dụng các thông tin này cho mục đích xấu. Hành động *tấn công* ở đây hiểu đơn giản là gửi *yêu cầu kết* bạn đến người dùng. Nếu người dùng chấp nhận yêu cầu kết bạn này, kẻ tấn công có thể lấy được các thông tin của người dùng. Chúng có thể sử dụng các thông tin này cho các mục đích xấu như: gửi tin nhắn rác, phát tán virus, giả mạo người dùng để lừa đảo vv..

Ngoài ra, người dùng còn có những thông tin trong tổ chức mà họ tham gia kể tấn công có thể sử dụng các thông tin này để tái tạo các thông tin khác về tổ chức và sử dụng cho các mục đích xấu. Với thực tế người dùng trên mạng xã hội vẫn chưa nhận thức rõ được sự cách thức cũng như sự nguy hiểm của hoạt động tấn công xâm nhập này, kẻ tấn công sử dụng Socialbots [4, 5, 6] đạt được tỷ thành công rất cao (từ 50% đến 70%).

Xuất phát từ thực tế này, một yêu cầu cấp thiết đặt ra là: *Làm thế nào có thể bảo vệ người dùng trước hoạt động xâm nhập tới người dùng trong một tổ chức của Socialbots?*

Để giải quyết vấn đề trên, trong chương này, luận văn đưa ra một giải pháp để phòng ngừa tấn công dựa trên việc xây dựng một *vùng an toàn* bao quanh tổ chức mà họ tham gia. Người dùng trong tổ chức được khuyến cáo chỉ nên kết bạn với các người dùng khác trong vùng an toàn này và thận trọng hơn đối với những lời mời kết bạn bên ngoài *vùng an toàn.*

Trong luân văn này, một mạng xã hội được biểu diễn bởi một đồ thị *có hướng, có trọng số* $G = (V, E, w)$ với:

- V là tập hợp n đỉnh biểu diễn người dùng mạng trong MXH.
- E là tập hợp m cạnh của đồ thị biểu diễn mối quan hệ bạn bè giữa hai người dùng.
- $w(u, v)$ là trọng số của các cạnh (u, v) là một số thực dương biểu diễn cho các tần số tương tác, trao đổi giữa hai người dùng. $w(u, v) = 0$ nếu giữa hai đỉnh u và v không tồn tại cạnh, $w(u, v) > 0$ nếu giữa u và v tồn tại cạnh nối.

$N_-(v)$ và $N_+(v)$ tương ứng là đỉnh kề đi vào và đi ra từ đỉnh v, số lượng các đỉnh này lần lượt là $d_-(v)$ và $d_+(v)$.

Một tập hợp $U \subset V$, $U = \{u_1, u_2, ., u_k\}$ gồm k phần tử biểu diễn cho tất cả người dùng trong một tổ chức mà chúng ta cần phải bảo vệ. Trên mô hình đồ thị này, bài toán được phát biểu như sau.

Định nghĩa 3.1 (Bài toán phòng ngừa xâm nhập) *Cho đồ thị $G = (V, E, w)$ biểu diễn một mạng xã hội, tập $U \subset V$ biểu diễn cho người dùng trong một tổ chức cụ thể. Làm thế nào đề phát hiện sự xâm nhập của kẻ tấn công có chủ ý gửi kết bạn đến những người dùng trong tổ chức U?*

3.2 Giải pháp phòng ngừa sự xâm nhập

Trong phần này, luận văn đưa ra một giải pháp phòng ngừa xâm nhập bao gồm các quá trình sau: *Bài toán phòng ngừa xâm nhập* nói trên bao gồm các quá trình như sau:

1. Đầu tiên, luận đề xuất một độ đo mới nhằm đánh giá mối quan hệ giữa hai người dùng gọi là $\Phi(u, v)$. Ý tưởng của độ đo này là đánh giá mối quan hệ giữa hai người dùng thông qua T người dùng trung gian giữa họ. Độ đo này mở rộng ý tưởng của các nghiên cứu [8, 21] trong việc đánh giá sự thân thiết hay mức độ quan trọng của mối quan hệ giữa hai người dùng.

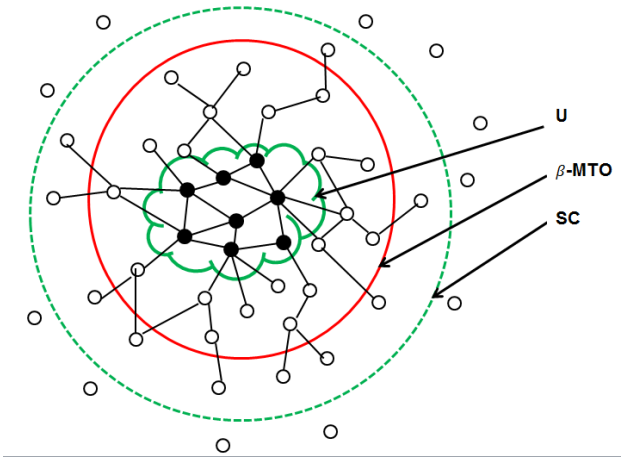
2. Thứ hai, dựa trên độ đo $\Phi()$ luận văn xây dựng một mô hình *Cộng đồng an toàn (Safety Community)* $G^{sc} = (V^{sc}, E^{sc})$ đối với mỗi tổ chức mà chùng ta cần bảo vệ khỏi sự xâm nhập. Cộng đồng an toàn là một vùng an toàn gồm có một tập người dùng và liên kết an toàn, có tác dụng tạo ra một môi trường an toàn cho tất cả mọi người dùng trong tổ chức.

3. Cuối cùng, luận văn xây dựng bài toán *Tối đa hóa sự tin tưởng* trong cộng đồng an toàn nhằm chọn ra những người dùng an toàn nhất với tỷ lệ $\beta \in (0, 1)$ trong cộng đồng an toàn G^{sc} (gọi là bài toán β-MTO), các đỉnh trong lời giải gọi là *vùng β-MTO*. Mục đích bài toán này là chọn ra những người dùng an toàn nhất đối với tất cả người dùng trong tổ chức trong cộn đồng an toàn. Người dùng trong tổ chức sẽ được khuyến cáo chỉ nên kết bạn với các người dùng khác trong cộng đồng an toàn này để phòng ngừa sự xâm nhập của kẻ tấn công.

3.3 Độ đo quan hệ và liên kết an toàn giữa hai người dùng

3.3.1 Chuẩn hóa trọng số trong đồ thị

Gọi đồ $G' = (V, E', w')$ là đồ thị biểu diễn một mạng xã hội. Để đánh giá ảnh hưởng giữa các đỉnh trong đồ thị, luận văn sử dụng cấu trúc đồ thị tổng quát nhất là đồ thị có hướng để biểu diễn lại đồ thị. Theo đó đồ thị $G' = (V, E', w')$ được



Hình 3.1: Tập người dùng U, vùng β-MTO và Cộng đồng an toàn SC

biểu diễn lại bởi một đồ thị có hướng, có trọng số $G = (V, E, w)$, trong đó trọng số $w(u, v)$ biểu diễn tỷ lệ ảnh hưởng của đỉnh u đối với đỉnh v. Với mỗi trường hợp cụ thể, trọng số này được định nghĩa như sau:

Nếu G' là đồ thị vô hướng:

$$w(u, v) = \frac{w'(u, v)}{\sum_{i \in N(v)} w'(u, i)} \tag{3.1}$$

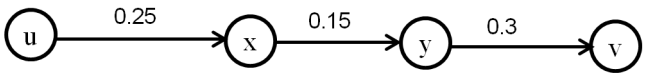
Nếu G' là đồ thị có hướng:

$$w(u, v) = \frac{w'(u, v)}{\sum_{i \in N_+(u)} w'(u, i)} \tag{3.2}$$

3.3.2 Độ đo quan hệ giữa hai người dùng

Trong thực tế, hai người sử dụng có thể ảnh hưởng đến nhau bằng truyền miệng và mạng xã hội cũng thừa hưởng tính chất đó của mạng xã hội thực. Luận văn sử dụng ước lượng trong [47] để đánh giá ảnh hưởng giữa hai người dùng thông qua những người dùng trung gian bằng tích trọng số trên đường đi giữa hai người dùng. Theo đó, gọi $P(u, v)$ là một đường đi đơn có hướng từ u đến v, ảnh hưởng của u đến v theo đường đi $P(u, v)$ được ước lượng bởi:

$$W(P(u, v)) = \prod_{(a,b) \in P(u,v)} w(a, b) \tag{3.3}$$



W(P(u,v))=w(u, x) × w(x, y) × w(y, v)=0.25×0.15×0.3=0.0125

Hình 3.2: Ước lượng ảnh hưởng đối với đường đi.

Bằng các áp dụng các ước lượng ở công thức (3.3) và các phân tích trên, luận văn đề xuất một độ đo mới khắc phục nhược điểm của Fire [8] để đánh giá mối quan hệ giữa hai người dùng dựa trên ý tưởng sau:

1. Đánh giá độ đo giữa hai người sử dụng thông qua $t, t \geq 0$ người dùng trung gian.
2. Đánh giá đối với tất cả các đường đi đơn (không có chu trình) giữa hai người dùng.

Áp dụng công thức (3.3), luận văn đưa ra một đánh giá mối quan hệ giữa hai người dừng u, v (theo chiều từ u đến) bằng tổng ảnh hưởng đối với tất cả đường đi từ u đến v qua t người dùng trung gian giữa họ bằng công thức sau:

$$\varphi(u, v, t) = \sum_{P(u,v) \in P, |P|=t+1} W(P(u, v)) \tag{3.4}$$

Trong đó $P(u, v)$ là đường đi từ u đến v, P là tất cả các đường đi đơn (không tạo thành chu trình) đi qua t người dùng trung gian (tức là có độ dài $t + 1$).

Định nghĩa 3.2 *Độ đo hàm lượng mối quan hệ giữa hai người dùng trong một mạng xã hội $G = (V, E, w)$ (có hướng hoặc vô hướng) qua T người dùng trung gian được xác định bởi:*

$$\Phi(u, v, T) = \sum_{t=0}^{T} \varphi(u, v, t) \tag{3.5}$$

3.3.3 Liên kết an toàn

Để định lượng quan hệ là an toàn, đáng tin cậy tác giả sử dụng một ngưỡng an toàn là θ, một người dùng v nào đó có $\Phi(u, v, T) \geq \theta$ thì mối quan hệ này an toàn đối với u.

$$\Phi(u, v, T) = \begin{cases} \geq \theta & \text{an toàn với } u \\ < \theta & \text{không an toàn với } u \end{cases}$$

3.4 Cộng đồng an toàn

Như đã phân tích ở phần trước, việc đánh giá quan hệ người dùng thông qua Φ có thể lọc được Socialbot. Dựa trên nhận định này luận văn đề xuất xây dựng một mô hình gọi là *Cộng đồng an toàn (Safety Community model)* đối với mỗi tổ chức với mục đích tạo thành một vùng an toàn đối với tổ chức bao gồm những người dùng trong tổ chức và những người dùng khác trong mạng xã hội được liên kết với nhau bởi liên kết an toàn.

Định nghĩa 3.3 (Độ tin tưởng) *Độ tin tưởng của một tổ chức U đối với người dùng v không thuộc tổ chức U được ước lượng bằng công thức sau:*

$$f(v) = \frac{1}{|U|} \sum_{u \in U} \Phi(u, v, T) \tag{3.6}$$

Gọi tập người dùng $U = \{u_1, u_2, .., u_k\}$, có số lượng là $|U| = k$, θ là ngưỡng an toàn, T là các tham số cho trước, tập $f = f(v), v \in G^{sc}$ là giá trị độ an toàn của một đỉnh v với tổ chức U. Cộng đồng an toàn (SC model) được định nghĩa như sau:

Định nghĩa 3.4 (Cộng đồng an toàn) *Cộng đồng an toàn của tập người dùng U trên đồ thị $G = (V, E, w, \Phi)$ với số bước k ký hiệu là k-$SC(U, \theta)$ là đồ thị $G^{sc} = (V^{sc}, E^{sc}, w^{sc}, \theta, f)$. Với các đại lượng: V^{sc}, E^{sc} được định nghĩa đệ quy như sau:*

1. *Bắt đầu: $V^{sc} = U$, nghĩa là Cộng đồng an toàn ban đầu chỉ bao gồm những người dùng trong tổ chức.*
2. *Lặp: Từ mỗi đỉnh $u \in V^{sc}$, xét các đỉnh $v \in V \setminus V^{sc}$, nếu $\Phi(u, v, T) \geq \theta$ thì thêm v vào V^{sc}, cạnh (u, v) vào E^{sc}, $w^{sc}(u, v) = \Phi(u, v, T)$. Việc lặp dừng lại khi số bước lặp là k.*

3.5 Bài toán cực đại tin tưởng trong Cộng đồng an toàn

3.5.1 Xây dựng bài toán

Luận văn đề xuất một bài toán chọn ra những người dùng an toàn theo các tiêu chí sau:

1. Chọn ra những người dùng trong Cộng đồng an toàn có mối quan hệ an toàn gián tiếp với người dùng trong tổ chức.
2. Chọn số người dùng nhỏ hơn số người dùng trong Cộng đồng an toàn, có tỷ lệ là $\beta \in \left(\frac{|U|}{|V^{sc}|}, 1\right)$.
3. Chọn người dùng theo độ an toàn của người dùng với cả tổ chức U, hàm mục tiêu là tổng độ tin tưởng $\sum_{v \in G^{sc}} f(v)$.

Với các tiêu chí trên, bài toán Cực đại an toàn cho tất cả người dùng trong tổ *(Maximizing Trust for Organization - MTO)* chức được phát biểu như sau:

Định nghĩa 3.5 (Bài toán cực đại an toàn (β-MTO)) *Cho Cộng đồng an toàn của tập người dùng: $U = \{u_1, u_2, .., u_k\}$ trên đồ thị $G = (V, E, w)$ là $SC(G, U, \theta)$ là đồ thị $G^{sc} = (V^{sc}, E^{sc}, f)$.*
Hãy tìm đồ thị $G_m = (V_m, E_m)$ là đồ thị con của $G^{sc} = (V^{sc}, E^{sc})$ thỏa mãn $U \subset V_m$, mọi đỉnh $v \in V_m$ liên thông với ít nhất một đỉnh $u \in U$ sao cho số lượng đỉnh của $|V_m| \leq \beta.|V^{sc}|, \beta \in \left(\frac{|U|}{|V^{sc}|}, 1\right)$ và tổng giá trị độ tin tưởng: $H(G_m) = \sum_{v \in V_m} f(v)$ đạt cực đại.

Định lý 3.1 *β-MTO là bài toán* NP*-Đầy đủ.*

Algorithm 1: Thuật toán tham lam - GA

Data: $G^{sc} = (V^{sc}, E^{sc}, w^{sc}, f), \beta, U = \{u_1, u_2, \ldots, u_k\}$.
Result: $G_m = (V_m, E_m)$.

```
1  begin
2      V_m ← U;
3      while |V_m| ≤ β.|V^sc| do
4          f_max ← 0;
5          foreach v ∈ V^sc \ V_m do
6              if f(v) ≥ f_max then
7                  f_max ← f(v);
8                  u ← v;
9              end
10         end
11         V_m ← u;
12         E_m ← E_m + (u, v);
13     end
14     Return G_m;
15 end
```

3.5.2 Thuật toán tham lam GA

Độ phức tạp của thuật toán được phát biểu và chứng minh bởi bổ đề sau:

Bổ đề 3.1 *Thuật toán tham lam có độ phức tạp là* $\mathcal{O}(\beta.n^2)$*, với* $|V^{sc}| = n$.

Chương 4

THỰC NGHIỆM

4.1 Mục đích thực nghiệm

1. Mô phỏng lại quá trình tấn công của Socialbots đối với người dùng trong một tổ chức trên mạng xã hội dựa trên phương pháp trong [4, 5, 7] trên dữ liệu mạng xã hội thực được thu thập và được ẩn danh.
2. Xây dựng Cộng đồng an toàn cho mỗi tổ chức.
3. Xây dựng vùng β-MTO trong Cộng đồng an toàn bằng thuật toán GA tương ứng với mỗi tổ chức. Đưa ra kết quả cách ly của vùng an toàn β-MTO đối với các Socialbots.
4. Kết luận và phân tích.

4.2 Dữ liệu tiến hành thực nghiệm

Các bộ dữ liệu tiến hành thực nghiệm được biểu diễn dưới dạng đồ một thị vô hướng không có trọng số. Cấu hình máy tính như sau: Chipset: Intel (R)

Tên mạng	**Số lượng người dùng**	**Số liên kết**	**Số nhóm**	Nguồn
Flickr	80,513	5,899,882	195	[61]
BlogCatalog	10,312	333,983	39	[60]

Bảng 4.1: Dữ liệu tiến hành thí nghiệm

Tổ chức	**Số lượng người dùng**	**Tên mạng**
U_1	101	Flickr
U_2	895	Flickr
U_3	167	BlogCatalog
U_4	778	BlogCatalog

Bảng 4.2: Các tổ chức người dùng tiến hành thí nghiệm

Xeon CPU-E3-1231 v3 @3,4 GHz (8 core), RAM: 16 GB, hệ điều hành Microsoft Window 7, 64 bit.

4.3 Mô phỏng tấn công của Socialbots

Trong phần này, luận văn mô phỏng tấn công tới một người dùng cụ thể trong tổ chức bằng Thuật toán 2 [4].
Các thủ tục và các biến trong phương pháp này được mô tả như sau:

Algorithm 2: Simulation of Socialbots's attack

Data: S-Socialbot, O-target organization, OrgPublicGraph

$OrgPublicGraph \leftarrow Organizational - Crawler(S, Uids, O)$;
$i \leftarrow 0$;
while $i < 10$ **do**
  $TUsers \leftarrow ChooseRandomTargetedUsers(O)$;
  $i \leftarrow i + 1$
end
$TargetedUserFriends \leftarrow FindOrgFriends(O, TUsers, OrgPublicGraph)$;
for $f \in TargetedUsersFriends$ **do**
  $SendFriendRequest(f)$;
end
for $TU \in TargetedUsers$ **do**
  $SendFriendRequest(TU)$;
end

- $OrgPublicGraph$: Dữ liệu về mạng xã hội có chứa tổ chức.
- S: Socialbots.
- O: Tổ chức mà Socialbots muốn tấn công.
- $Organizational - Crawler(S, Uids, O)$: Lấy dữ liệu về mạng xã hội chứa tổ chức O.
- $TUsers$: Là tập người dùng đích trong tổ chức O mà Socialbot muốn tấn công.
- $ChooseRandomTargetedUsers(O)$: Thủ tục chọn ngẫu nhiên một người dùng trong tổ chức O.
- $FindOrgFriends(O, TUsers, OrgPublicGraph)$: Thủ tục tìm các bạn bè của người dùng đích TUsers.
- $SendFriendRequest(v)$: Thủ tục gửi yêu cầu kết bạn đến người dùng v.

Đối với mỗi tổ chức U_i, quy trình tấn công của Socialbot S được mô phỏng lại theo các bước sau:

1. Tạo một đỉnh mới biểu diễn cho Sociabots trong mạng (gọi là đỉnh S_i) đối với mỗi tổ chức U_i.
2. Chọn ra 10 người dùng một cách ngẫu nhiên trong các tổ chức.
3. Tìm kiếm bạn bè (bạn chung) của các *người dùng đích* X trong U. Sau đó gửi yêu cầu kết bạn đến các bạn chung này theo tỷ lệ thành công là $p_{accpet} = 0.325$. Thực hiện 10 lần đối với mỗi bạn chung sau đó lấy kết quả trung bình.
4. Tạo liên kết giữa đỉnh S_i với bạn chung tương ứng nếu kết bạn thành công.

Luận văn sử dụng phương pháp tấn công này đối với các tổ chức U_1, U_2, U_3, U_4. Kết quả của quá trình tấn công được trình bảy ở các bảng 4.3, 4.4, 4.5 và 4.6.

Người dùng đích	Số bạn chấp nhận	Tổng số bạn	Tỷ lệ chấp nhận
T1	72	193	37.31
T2	1	3	33.33
T3	11	22	50.0
T4	64	193	33.16
T5	19	47	40.43
T6	2	11	18.18
T7	5	11	45.45
T8	3	9	33.33
T9	3	11	27.27
T10	67	200	33.50
Tổng số	247	700	**35.29**

Bảng 4.3: Kết quả mô phỏng tấn công của Socialbot với U_1

Người dùng đích	Số bạn chấp nhận	Tổng số bạn	Tỷ lệ chấp nhận
T1	55	144	38.19
T2	21	70	30.00
T3	44	135	32.59
T4	129	368	35.05
T5	50	174	28.74
T6	315	928	33.94
T7	25	76	32.89
T8	2	4	50.00
T9	182	524	34.73
T10	5	9	55.56
Tổng số	828	2,432	**34.04**

Bảng 4.4: Kết quả mô phỏng tấn công của Socialbot với U_2

Kết quả này mô phòng này hoàn toàn phù hợp với kết quả nêu trong [4] về tỷ lệ số bạn chung của người dùng đích chấp nhập kết bạn.

4.4 Hiệu quả phòng ngừa xâm nhập của vùng an toàn β-MTO

Trong phần này, luận văn tiến hành thực nghiệm xây dựng vùng an toàn β-MTO theo thuật toán tham lam để đánh giá hiệu quả cách ly.

4.4.1 Tiền xử lý dữ liệu

Để thu được trọng số từ dữ liệu, tác giả sử dụng phương pháp lấy trọng số trong [38] theo công công thức:

$$w'(u,v) = \frac{c(u,v)}{d(u)} \tag{4.1}$$

Trong đó, $c(u,v)$ là số cạnh giữa hai đỉnh u và v. Sau khi thu được đồ thị có trọng số $G' = (V', E', w')$ biểu diễn dữ liệu thực nghiệm, luận văn áp dụng phương pháp chuẩn hóa trọng số trong Chương 3 để chuẩn hóa trọng số của đồ thị G'.

Người dùng đích	Số bạn chấp nhận	Tổng số bạn	Tỷ lệ chấp nhận
T1	10	20	50.00
T2	10	27	37.04
T3	32	67	47.76
T4	22	69	31.88
T5	5	14	35.71
T6	14	33	42.42
T7	1	3	33.33
T8	6	12	50.00
T9	6	12	50.00
T10	6	26	23.08
Tổng số	111	283	**39.22**

Bảng 4.5: Kết quả mô phỏng tấn công của Socialbot với U_3

Người dùng đích	Số bạn chấp nhận	Tổng số bạn	Tỷ lệ chấp nhận
T1	3	8	37.5
T2	2	11	18.18
T3	11	27	40.74
T4	50	133	37.59
T5	2	4	50.00
T6	26	73	35.62
T7	3	8	37.50
T8	3	6	50.00
T9	56	164	34.15
T10	5	9	55.56
Tổng số	161	443	**36.34**

Bảng 4.6: Kết quả mô phỏng tấn công của Socialbot với U_4

4.4.2 Kết quả xây dựng Cộng đồng an toàn

4.4.3 Hiệu quả của β-MTO

Sau khi đã xây dựng cộng đồng an toàn cho mỗi tổ chức, luận văn tiến hành tìm lời giải cho bài toán β-MTO bằng thuật toán tham lam GA. Thuật toán được tiến hành với các tham số $\beta = \{0.30; 0.90\}$ với các mốc cách nhau 0.05. Hiệu quả cách ly cho 04 tổ chức U_1, U_2, U_3 và U_4 được trình bày trong các bảng 4.8, 4.9, 4.10 và 4.11.

4.5 Kết luận

Từ kết quả trên cho thấy hiệu quả của vùng an toàn β-MTO tìm bởi thuật toán GA có hiệu quả phòng ngừa tốt. Đa số các trường hợp Socialbot không thể xâm nhập được vào vùng này, đo đó có thể dùng kết quả này gửi cảnh báo tới người dùng trước một lời mời yêu cầu kết bạn.

Tổ chức	U_1	U_2	U_3	U_4
Mạng	Flickr	Flickr	BlogCatalog	BlogCatalog
Số lượng người dùng	101	895	167	778
T	2	1	2	2
k	4	4	3	5
θ	0.23	0.35	0.33	0.23
V^{sc}	1,646	7,052	1,270	5,527
E^{sc}	1,920	10,050	3,044	56,744
$f(S_i)$	0.0007407	0.0184033	0.0190195	0.0145107
Thời gian chạy	12h	48h	gần 12h	48h

Bảng 4.7: Kết quả xây dựng cộng đồng an toàn cho mỗi tổ chức

Tham số β	**Số đỉnh**	Hàm mục tiêu	**Kết quả cách ly** S_1
0.30	493	142.97	Cách ly
0.35	576	161.28	Cách ly
0.40	658	171.08	Cách ly
0.45	740	185.04	Cách ly
0.50	823	192.72	Cách ly
0.55	905	208.15	Cách ly
0.60	987	217.14	Cách ly
0.65	1069	224.49	Cách ly
0.70	1152	236.76	Cách ly
0.75	1234	246.82	Không cách ly được
0.80	1316	250.12	Không cách ly được
0.85	1399	251.82	Không cách ly được
0.90	1481	252.34	Không cách ly được

Bảng 4.8: Kết quả tìm vùng β-MTO đối với tổ chức U_1

Tham số β	**Số đỉnh**	**Hàm mục tiêu**	**Kết quả cách ly** S_2
0.30	2115	676.81	Cách ly
0.35	2468	765.08	Cách ly
0.40	2820	846.65	Cách ly
0.45	3173	936.07	Cách ly
0.50	3526	1022.54	Cách ly
0.55	3878	1085.84	Cách ly
0.60	4231	1163.52	Cách ly
0.65	4583	1237.41	Cách ly
0.70	4936	1380.05	Cách ly
0.75	5289	1401.59	Cách ly
0.80	5641	1466.62	Cách ly
0.85	5994	1528.47	Cách ly
0.90	6346	1523.04	Không cách ly được

Bảng 4.9: Kết quả tìm vùng β-MTO đối với tổ chức U_2

Tham số β	**Số đỉnh**	**Hàm mục tiêu**	**Kết quả cách ly với S_3**
0.30	381	123.81	Cách ly
0.35	444	135.59	Cách ly
0.40	508	145.01	Cách ly
0.45	571	153.66	Cách ly
0.50	635	160.02	Cách ly
0.55	698	165.71	Cách ly
0.60	762	170.63	Cách ly
0.65	825	175.29	Cách ly
0.70	889	179.96	Cách ly
0.75	952	182.58	Cách ly
0.80	1016	185.07	Không cách ly được
0.85	1079	187.96	Không cách ly được
0.90	1143	190.69	Không cách ly được

Bảng 4.10: Kết quả tìm vùng β-MTO đối với tổ chức U_3

Tham số β	**Số đỉnh**	**Hàm mục tiêu**	**Kết quả cách ly với S_4**
0.30	1658	530.56	Cách ly
0.35	1934	599.34	Cách ly
0.40	2210	603.12	Cách ly
0.45	2487	733.67	Cách ly
0.50	2763	801.27	Cách ly
0.55	3039	867.72	Cách ly
0.60	3316	895.32	Cách ly
0.65	3592	933.92	Cách ly
0.70	3868	967.18	Cách ly
0.75	4145	994.81	Cách ly
0.80	4421	1016.83	Cách ly
0.85	4697	1033.34	Cách ly
0.90	4974	1044.54	Không cách ly được

Bảng 4.11: Kết quả tìm vùng β-MTO đối với tổ chức U_4

KẾT LUẬN

Sự rò rỉ thông tin trên mạng xã hội là một nguy cơ lớn đối với người dùng. Sự rò rỉ này có thể đến từ sự chủ quan của người dùng hoặc được kẻ tấn công thu thập một cách có chủ đích. Do kẻ tấn công sử dụng các hoạt động tinh vi, người dùng dễ dàng bị xâm nhập và để lô các thông tin đối với kẻ tấn công. Hơn nữa, hoạt động này đem những hậu quả nghiêm trọng cho người dùng vì kẻ tấn định sẵn mục tiêu từ trước và kẻ tấn công có thể thực hiện hoạt động này trên mạng với quy mô lớn. Do đó, việc đưa ra một giải pháp phòng người sự xâm nhập lấy cắp thông tin là việc làm hết sức cấp thiết đối với người dùng trên mạng xã hội.

Trong luận văn này, tác giả đưa ra một phương pháp để phòng ngừa sự xâm nhập tới người dùng trong một tổ chức cụ thể. Luận văn dựa trên nghiên cứu [4, 5, 6] để phân tích sự tấn công trên mạng diện rộng của Socialbots, qua đó đề một phương pháp để phòng ngừa quá trình xâm nhập. Luận văn đã đạt được một số kết quả chính như sau:

- Tìm hiểu, khái quát về mạng xã hội, một số bài toán được quan tâm trên mạng xã hội. Tìm hiểu về các nguy cơ mất an toàn đối với người dùng trên mạng xã hội. Đặc biệt luận văn đi sâu tìm hiểu về các nguy cơ rò rỉ thông tin trên mạng xã hội, hình thức tấn công lấy cắp thông tin có chủ đích bằng việc sử dụng Socialbot.

- Đề xuất một giải pháp phòng ngừa sự xâm tới người dùng trong tổ chức bao gồm nhập gồm nhiều quá trình gồm các công việc: Xây dựng độ đo mối quan hệ giữa hai người dùng. Sử dụng độ đo này xây dựng một Cộng đồng an toàn bao tất cả các người dùng trong tổ chức.

- Trong cộng đồng an toàn, xây dựng bài toán tối ưu độ an toàn nhằm chọn ra vùng β-MTO gồm những người dùng có độ an toàn cao nhất đối với mọi người dùng trong tổ chức (bài toán β-MTO), bài toán này được chứng minh thuộc lớp NP-Đầy đủ. Luận văn đề xuất một thuật toán tham lam để giải quyết bài toán này.

- Kết quả thực nghiệm cho thấy vùng an toàn β-MTO có khả năng cách ly được sự tấn công của Socialbots với hiệu quả cao.

Mặc dù đã cố gắng và nỗ lực hết mình, nhưng do thời gian nghiên cứu và trình độ của bản thân có hạn nên luận văn không thể tránh khỏi những thiếu sót và hạn chế, tác giả rất mong nhận được những ý kiến đóng góp để luận văn đạt được kết quả tốt hơn.

Hướng phát triển:

Trong thời gian tới, tác giả đề xuất một số hướng phát triển của luận văn như sau:

- Thiết kế thuật toán xấp xỷ tốt hơn cho việc tìm vùng an toàn β-MTO. Thuật toán đảm bảo thời gian đa thức luôn đảm bảo tỷ lệ kết quả so với lời giải tối ưu.
- Tiến hành thực nghiệm nhiều hơn với những tổ chức có cấu trúc khác nhau, trên các mạng xã hội khác nhau. Qua đó, đưa ra các giải pháp lựa chọn các tham số: T, θ, k, β tốt nhất cho mỗi cấu trúc mạng.
- Phát triển phương pháp phòng ngừa cho các mạng phức hợp mà mỗi người dùng có nhiều tài khoản trên các mạng khác nhau và có sự ánh xạ tương ứng giữa các mạng.

Danh mục công trình công bố

Canh V. Pham, Huan X. Hoang, Manh M. Vu (2015), Preventing and detecting the infiltration on Online Social Networks, *Proceeding of 4th International Conference on Computation Social Networks (CsoNet)*, pp. 60-73.

Tài liệu tham khảo

[1] Aron O'Cass, and Tino Fenech .: Webretailing adoption: exploring the nature of internet users Webretailing behaviour, Journal of Retailing and Consumer Services 10 81–94 (2003)

[2] 216 social media and internet statistics. http://thesocialskinny.com/ 216-social-media-and-interne t-statistics-september-2012.

[3] 99 new social media stats for 2012. http://thesocialskinny.com/ 99-new-social-media-stats-for-2012/.

[4] Aviad Elyashar, Michael Fire, Dima Kagan, Yuval Elovici .: Homing Socialbots: Intrusion on a specific organization's employee using Socialbots, IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (2013)

[5] Aviad Elyashar, Michael Fire, Dima Kagan, and Yuval Elovici.: Organizational Intrusion: Organization Mining using Socialbots,ASE International Conference On Cyber Security, Washington D.C, USA, (2012).

[6] Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu (2012), Design and Analysis of a Social Botnet, July 9.

[7] Michael Fire, Rami Puzis, and Yuval Elovici .: Organization Mining Using Online Social Networks, ACM Transactions on Embedded Computing Systems, Vol. 9, No. 4, Article 39, June, (2012).

[8] Fire, M., Tenenboim, L., Lesser, O., Puzis, R., Rokach, L., Elovici, Y.: Link prediction in social networks using computationally efficient topological features. In: SocialCom/PASSAT, pp. 73–80. IEEE (2011).

[9] E. Mills, Facebook Hit by Phishing Attacks for a Second Day, Apr. 2009, accessed Jan. 14, 2014. [Online]. Available: http://news.cnet.com/8301-1009 3-10230980-83.html.

[10] A. Chowdhury, State of Twitter Spam,Mar. 2010, accessed Jan. 14, 2014. [Online]. Available: https://blog.twitter.com/2010/state-twitter-spam

[11] B. Livshits and W. Cui, "Spectator: Detection and containment of java- script worms," in Proc. USENIX Annu. Tech. Conf., 2008, pp. 335–348.

[12] I. Paul, "Twitter worm: A closer look at what happened," PCWorld, San Francisco, CA, USA, Apr. 2009.

[13] J. Halliday, "Facebook fraud a 'Major Issue'," The Guardian, London, U.K., Sep. 2010. [Online]. Available: http://www.theguardian.com/technology/2010/sep/20/facebook-fraud-security

[14] Hu, M. and Liu, B. (2006). Opinion extraction and summarization on the Web, Proceedings of the 21th National Conference on Artificial Intelligence (AAAI), 2006.

[15] Jiyang Chen (2010) Community Mining - Discovering Communities in Social Networks. Thesis, University of Alberta.

[16] Jason D. M. Rennie (2001) Improving Multi-class Text Classication with Naïve Bayes, Master of Science - Department of Electrical Engineering and Computer Science on September 10, 2001.

[17] D. Cavit et al., Microsoft Security Intelligence Report Volume 10, 2010, accessed Mar. 11, 2014. [Online]. Available: http://www.microsoft.com/ en-us/download/details.aspx?id=17030

[18] https://vi.wikipedia.org/wiki/M

[19] S. Fortunato.: Community detection in graphs. Physics Reports, 486(3-5):75 – 174, (2010)

[20] S. Fortunato and C. Castellano.: Community structure in graphs. eprint arXiv: 0712.2716, (2007)

[21] Leskovec, J., Huttenlocher, D., Kleinberg, J.: Predicting positive and negative links in online social networks. In: Proceedings of the 19th international conference on World wide web, WWW '10, pp. 641–650. ACM, New York, NY, USA (2010)

[22] Viswanath, B., Mislove, A., Cha, M., Gummadi, K.P.: On the evolution of user interaction in facebook. In: 2nd ACM SIGCOMM Workshop on Social Networks (2009)

[23] N. P. Nguyen, M. A. Alim, T. N. Dinh, and M. T. Thai.: A Method to Detect Communities with Stability in Social Networks Social Network Analysis and Mining, Vol. 4, Issue 1, DOI: 10.1007/s13278-014-0224-2, 2014

[24] T. N. Dinh, Y. Shen, and M. T. Thai.: The Walls Have Ears: Optimize Sharing for Visibility and Privacy in Online Social Networks, in Proceedings of ACM Int Conference on Information and Knowledge Management (CIKM), 2012.

[25] J. Leskovec, K. Lang, A. Dasgupta, M. Mahoney.: Community Structure in Large Networks: Natural Cluster Sizes and the Absence of Large Well-Defined Clusters. Internet Mathematics 6(1) 29-123, 2009.

[26] M. Richardson and R. Agrawal and P. Domingos. Trust Management for the Semantic Web. ISWC, 2003.

[27] https://en.wikipedia.org/wiki/$Community_structure$

[28] Veremyev, A., Boginski, V., Pasiliao, E.: Exact identification of critical nodes in sparse networks via new compact formulations. Optimization Letters 8(4), 1245-1259 (2014). DOI 10.1007/s11590-013-0666-x. URL http://dx.doi.org/10.1007 s11590-013-0666-x

[29] Goldberg, A.V., Tarjan, R.E.: A new approach to the maximum flow problem. In Proceedings of the eighteenth annual ACM symposium on Theory of computing, STOC '86, pp. 136-146. ACM, New York, NY, USA (1986). DOI http://doi.acm.org/10.1145/12130. 12144. URL http://doi.acm.org/10.1145/12130.12144

[30] Canh V. Pham, Huan X. Hoang, Manh M. Vu.: Preventing and detecting the infiltration on Online Social Networks, in Proceeding of 4th Conference Computation Social Networks, Spinger, 2015.

[31] Huiyuan Zhang, Thang N. Dinh, and My T. Thai .: Maximizing the Spread of Positive Influence in Online Social Networks, in Proceedings of the IEEE Int Conference on Distributed Computing Systems (ICDCS), 2013.

[32] J Zhang, P Zhou, C Cao, Y Guo L .: Personalized Influence Maximization on Social Networks, Proceedings of the 22nd ACM international conference on Conference on information and knowledge management.

[33] Honglei Zhuang, Yihan Sun, Jie Tang, Jialin Zhangz and Xiaoming Sunz , Influence Maximization in Dynamic Social Networks

[34] Ceren Budak, Divyakant Agrawal, Amr El Abbadi, Limiting the Spread of Misinformation in Social Networks

[35] N. P. Nguyen, G. Yan, M. T. Thai, and S. Eidenbenz, Containment of Misinformation Spread in Online Social Networks, in Proceedings of ACM Web Science (WebSci), 2012

[36] D. T. Nguyen, N. P. Nguyen, and M. T. Thai, Sources of Misinformation in Online Social Networks: Who to Suspect?, in Proceedings of the IEEE Military Communications Conference (MILCOM), 2012.

[37] H. Zhang, X. Li, and M. Thai, Limiting the Spread of Misinformation while Eectively Raising Awareness in Social Networks, in Proceedings of the 4th International Conference on Computational Social Networks (CSoNet), 2015.

[38] D. Kempe, J. Kleinberg, and E. Tardos. Maximizing the spread of influence through a social network. In Ninth ACM SIGKDD international conference on Knowledge discovery and data mining, KDD 03, pages 137–146, New York, NY, USA, 2003.

[39] Huiling Zhang, Md Abdul Alim, Xiang Li, My T. Thai, and Hien T. Nguyen. 2016. Misinformation in online social networks: Detect them all with a limited budget. ACM Trans. Inf. Syst. 34, 3, Article 18 (April 2016), 24 pages. DOI: http://dx.doi.org/10.1145/2885494

[40] N. P. Nguyen, T. N. Dinh, Y. Shen, and M. T. Thai, Dynamic Social Community Detection and its Applications PLoS ONE 9(4): e91431. doi:10.1371/journal.pone.0091431, 2014.

[41] J. Yang, J. McAuley, J. Leskovec:. Community Detection in Networks with Node Attributes, IEEE International Conference On Data Mining (ICDM), 2013.

[42] Wen Xu , Weili Wu, Lidan Fan, Zaixin Lu, Ding-Zhu Du :. Influence Diffusion in Social Networks, Book chapter Optimization in Science and Engineering, doi 10.1007/978-1-4939-0808-027, 2014

[43] M. E. J. Newman, "Modularity and community structure in networks," PNAS, vol. 103, 2006.

[44] S. Fortunato and C. Castellano. Community structure in graphs. eprint arXiv: 0712.2716, 2007.

[45] https://en.wikipedia.org/wiki/Social-networking-service

[46] http://www.orbifold.net/default/portfolio/community-detection/

[47] N. P. Nguyen, M. A. Alim, T. N. Dinh, and M. T. Thai, A Method to Detect Communities with Stability in Social Networks Social Network Analysis and Mining, Vol. 4, Issue 1, DOI: 10.1007/s13278-014-0224-2, 2014

[48] H Zhang, M. Alim, M. T. Thai, and H. Nguyen, Monitor Placement to Timely Detect Misinformation in Online Social Networks, in Proceedings of the 2015 IEEE International Conference on Communications (ICC), 2015

[49] H. Zhang, H. Zhang, X. Li, and M. T. Thai, Limiting the Spread of Misinformation while Effectively Raising Awareness in Social Networks, in Proceedings of the 4th International Conference on Computational Social Networks (CSoNet), 2015.

[50] T. N. Dinh, H. Zhang, D. T. Nguyen, and M. T. Thai.: Cost-effective Viral Marketing for Time-critical Campaigns in Large-scale So-

cial Networks, IEEE/ACM Transactions on Networking (ToN), DOI: 10.1109/TNET.2013.2290714, 2013

[51] T. N. Dinh, Y. Shen, and M. T. Thai, The Walls Have Ears: Optimize Sharing for Visibility and Privacy in Online Social Networks, in Proceedings of ACM Int Conference on Information and Knowledge Management (CIKM), 2012.

[52] Y. Shen, Y-S. Syu, D. T. Nguyen, and M. T. Thai, Maximizing Circle of Trust in Online Social Networks, in Proceedings of ACM Conference on Hypertext and Social Media (Hypertext), 2012.

[53] Y. Shen, M. T. Thai, and H. Nguyen, Staying Safe and Visible via Message Sharing in Online Social Networks, Journal of Combinatorial Optimization (JOCO), DOI: 10.1007/s10878-013-9667-z, 2013.

[54] J. Baltazar, J. Costoya, and R. Flores, "The real face of koobface: The largest web 2.0 botnet explained," Trend Micro Res., vol. 5, no. 9, p. 10, 2009.

[55] A. Goyal, F. Bonchi, and L. V. S. Lakshmanan, "Learning influence probabilities in social networks," WSDM '10, pp. 241–250, 2010.

[56] http://primarypsychiatry.com/social-networking-now-professionally-ready/

[57] Feige, U.: A threshold of ln n for approximating set cover. Journal of the ACM (JACM) 45(4), 634–652.

[58] http://www-01.ibm.com/software/commerce/optimization/cplex-optimizer/

[59] B. Viswanath, M. Mondal, A. Clement, P. Druschel, K. P. Gummadi, A. Mislove, A. Post, Exploring the design space of social network-based Sybil defenses, Proc. 4th International Conference on Communication Systems and Networks (COMSNETS).

[60] Lei Tang and Huan Liu. Relational Learning via Latent Social Dimensions. In Proceedings of The 15th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD'09), pp. 817–826, (2009).

[61] Lei Tang and Huan Liu. Scalable Learning of Collective Behavior based on Sparse Social Dimensions. In Proceedings of the 18th ACM Conference on Information and Knowledge Management (CIKM'09), 2009.