LỜI CẢM ƠN

Trước hết, tôi xin gửi lời cảm ơn sâu sắc tới cô GS.TS Thái Trà My đã giành nhiều thời gian để hướng dẫn, góp ý tôi hoàn thành luận văn này. Tôi xin gửi lời cảm ơn chân thành nhất tới thầy PGS.TS Hoàng Xuân Huấn đã giúp đỡ, động viên trong học tập, nghiên cứu khoa học cũng như kinh nghiệm trong cuộc sống.

Tôi cũng xin được bày tỏ lòng biết ơn tới các thầy, cô trong Khoa Công nghệ thông tin, trường Đại học Công nghệ đã tham gia giảng dạy và chia sẻ những kinh nghiệm quý báu cho tập thể và cá nhân tôi nói riêng. Các thầy cô đã tạo ra môi trường học tập, làm việc khoa học nghiêm túc, hiệu quả giúp tôi có thể học hỏi, trau dồi kiến thức.

Tôi cũng xin gửi lời cảm ơn tới Ban giám đốc Học viện An ninh nhân dân, lãnh đạo Khoa Công nghệ và An ninh thông tin cùng các đồng nghiệp đã tạo điều kiện thuận lợi cho tôi tham gia và hoàn thành khóa học.

Trên tất cả, tôi xin gửi lời biết ơn tới bố, mẹ và toàn thể gia đình, người thân. Đặc biệt, Bố mẹ tôi những người nuôi tôi khôn lớn, đã phải làm việc vất vả kể từ khi tôi còn nhỏ để tạo điều kiện cho tôi có thể đến trường theo đuổi ước mơ và hoài bão của mình.

Tác giả

Phạm Văn Cảnh

LỜI CAM ĐOAN

Tôi xin cam đoan, những kiến thức trình bày trong luận văn là do tôi tìm hiểu, nghiên cứu và trình bày lại. Trong quá trình làm luận văn tôi có tham khảo các tài liệu có liên quan và đã ghi rõ nguồn tài liệu tham khảo đó. Những kết quả mới trong luận văn là của riêng tôi, không sao chép từ bất kỳ một công trình nào khác. Nếu có điều gì không trung thực, tôi xin hoàn toàn chịu trách nhiệm.

Tác giả

Phạm Văn Cảnh

Danh sách hình vẽ

Danh sách bảng

Mục lục

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. Hiện nay, có hàng tỷ người sử dụng mạng xã hội trên toàn thể giới. Nhờ có mạng xã hội, người dùng có thể trao đổi thông tin với nhau một cách nhanh chóng bất kể khoảng cách địa lý và thời gian. Không những thế, mạng xã hội còn cung cấp cho người dùng rất nhiều tiện ích và ứng dụng hữu ích, làm cho cuộc sống của con người ngày càng trở nên thuận tiện.

Mạng xã hội không những kế thừa những đặc tính của mạng lưới xã hội thực như: tương tác giữa người dùng, lan truyền thông tin, tạo ảnh hưởng trong mạng lưới vv.. mà còn mang nhiều đặc tính mới như: thông tin trong thế giới thực được cập nhật trên mạng một cách nhanh chóng, sự lan truyền thông tin giữa người dùng xảy ra trong thời gian ngắn, sự bùng nổ thông tin với các nguồn tin tức khác nhau vv.. Có thể nói, hiện nay mạng xã hội là nguồn cung tri thức dồi dào và thuận tiện cho con người.

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. Hoạt động xâm nhập thành công khi người dùng đồng ý yêu cầu kết bạn của kẻ tấn công. Khi đó, người dùng vô tình để lộ các thông tin có giá trị để kẻ tấn công sử dụng với mục đích xấu.

Trong các nghiên cứu liên quan, Elyashar [5], Michael Fire [7], Boshmaf [6] đã thiết kế các Socialbot bắt chước hành động của người dùng thật sau đó tiến hành hoạt động xâm nhập đến người dùng trên mạng xã hội với diện rộng. Đặc biệt, Elyashar [4] đã kết hợp các nghiên cứu trên để thiết kế một mạng lưới Socialbot xâm nhập đến người dùng trong một tổ chức cụ thể. Nghiên cứu này 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. Họ chưa nhận ra các hoạt động cũng như sự hậu quả của sự tấn công. Kẻ tấn công có thể sử dụng những thông tin này cho mục đích xấu như: tấn công phát tán virus, gửi tin nhắn rác, giả mạo người dùng để lừa đảo vv..

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. Kẻ tấn công thể sử dụng những thông tin này cho việc thu thập thông tin, tái tạo lai cơ cấu tổ chức của họ phục vụ cho mục đích xấu. 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 việc tìm hiểu, phân tích hoạt động xâm nhập lấy thông tin của người dùng mạng xã hội diện rộng và đưa ra một giải pháp phòng ngừa sự xâm nhập này. 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. Tác giả cũng trình bày những lợi ích và hậu quả mà mạng xã hội mang lại. Đặc biệt, trong phần này tác giả cũng trình bày tổng quan và phân tích một số hướng nghiên cứu đối với 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 các nguy cơ rò rỉ thông tin của người dùng, 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. Đây là những dữ kiện quan trọng để để tác giả đề xuất giải pháp phòng ngừa sự xâm nhập trong Chương 3.

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. Từ thực trạng đã nêu ở chương 2, tác giả đề xuất bài toán phát hiện sự xâm nhập tới người dùng trong tổ chức trên mạng xã hội. Đưa ra một giải pháp phòng ngừa sự xâm nhập dựa trên sự phân tích hoạt động tấn công có chủ đích. Trong các bước của giải pháp này, tác giả đưa ra một số kết quả phân tích lý thuyết cho mỗi bước. Cuối cùng, là đề xuất giải thuật hiệu quả để xây dựng giải pháp phòng ngừa.

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. Kết quả thực nghiệm cho thấy, giải pháp đề xuất có thể phòng ngừa được sự tấn công xâm nhập tới người dùng trong tổ chức với khả năng thành công cao.

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.

Cùng với sự phát triển mạnh mẽ của Internet, các mạng xã hội đã phát triển một cách nhanh chóng. Người dùng trên mạng có thể giao tiếp với nhau bất chấp khoảng cách địa lý, nhờ đó sự liên kết và tương tác giữa con người với nhau trở nên thường xuyên và nhanh chóng. Các học giả cho rằng thuật ngữ "xã hội" giải thích cho các tính năng giống như một xã hội thực của 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. Qua e-mail và tin nhắn tức thời, các cộng đồng trực tuyến được tạo ra khi mọi người có thể dễ dàng trao đổi thông tin với nhau.

Ngoài ra, mạng xã hội còn xây dựng nhiều môi trường nền tảng cho nhiều tiện ích, ứng dụng cho người dùng. Chính vì vậy, ngoài việc sử dụng mạng xã hội cho việc trao đổi thông tin thì người dùng còn có thể tiến hành nhiều hoạt động khác tùy theo các tiện tích đối với trang mạng xã hội cung cấp.

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 [1], 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.

Trong việc giám sát và phân tích hành vi của con người, các công ty đã sử dụng mạng xã hội để tìm hiểu về tính cách và hành vi của nhân viên, đặc biệt là những nhân viên tiềm năng. Facebook và các mạng xã hội khác đang ngày càng trở thành đối tượng của nghiên cứu học thuật. Các học giả ở nhiều lĩnh vực đã bắt đầu điều tra về tác động của các trang mạng xã hội. Những vấn đề này bao gồm: tính chất, sự riêng tư của người dùng, tính xã hội, văn hóa giới trẻ và giáo dục. Nhiều nghiên cứu cho thấy rằng các cá nhân có xu hướng tăng cường tính ẩn danh trong việc kết bạn trên Facebook để duy trì liên lạc và thường này làm mờ đi ranh giới giữa công việc và cuộc sống gia đình.

Mạng xã hội có nhiều ảnh hưởng tới các hoạt động trong thế giới thực. Theo một nghiên cứu vào năm 2015, 63% số người sử dụng Facebook hay Twitter ở Mỹ xem các mạng này là nguồn thông tin chính thức. Trong đó, những tin tức về giải trí được quan tâm nhất. Khi người dùng đọc các tin tứ mà họ quan tâm, họ có nhiều khả năng sẽ duy trì trò cuộc trò chuyện đó. Ngoài ra, khi nội dung cuộc trò chuyện liên quan đến các vấn đề chính trị, người dùng có nhiều khả năng nói lên ý kiến của mình về quan điểm chính trị. Trong năm 2011, công ty HCL Technologies đã tiến hành nghiên cứu cho thấy rằng 50% các nhà tuyển dụng Anh đã cấm việc sử dụng các trang mạng xã hội hoặc dịch vụ trong giờ làm việc. Nghiên cứu này cũng cho thấy rằng người dùng cũng có ảnh hưởng về cảm xúc khi tham gia vào mạng xã hội.

Mạng xã hội có nhiều ảnh hưởng đến các mối quan hệ trong thế giới thực. Có một số công ty khuyến khích người lao động của mình sử dụng mạng xã hội để tạo ra các kết nối trong nội bộ. Giáo viên cũng thường xuyên sử dụng mạng xã hội để giữ kết nối với các sinh viên của họ hoặc đăng tải tài liệu, thông tin về bài học. Những cá nhân được hưởng lợi từ mạng xã hội muốn giữ kết nối với đối tác của họ. Ngoài ra, người dùng có thể tạo thành các nhóm có cùng sở thích hay

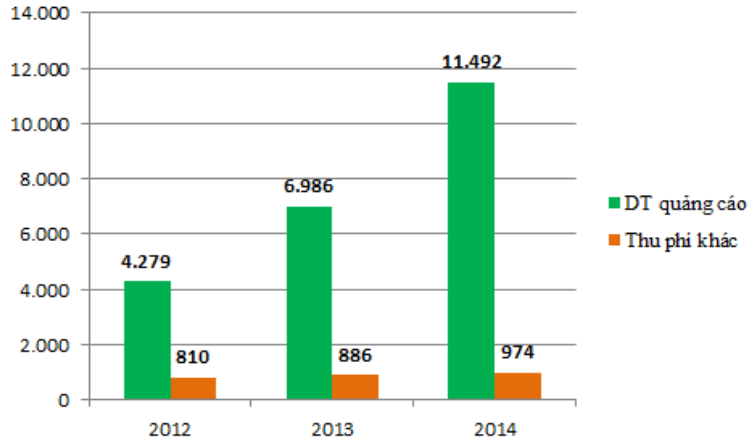
[1] https://www.facebook.com

đam mê về một lĩnh vực nhất định.

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[2] với mục đích kết nối bạn học với nhau. Tiếp theo là sự xuất hiện của SixDegrees[3] vào năm 1997 với mục đích giao lưu kết bạn dựa theo sở thích. Năm 2002, mạng xã hội Friendster[4] ra đời và trở thành một trào lưu mới tại Hoa Kỳ với hàng triệu người dùng đăng ký. Tuy nhiên, với sự phát triển quá nhanh về số người dùng cũng như nhu cầu tương tác giữa họ trên mạng xã hội này ngày càng lớn dẫn đến hệ thống máy chủ của Friendster thường bị quá tải mỗi ngày, gây thất vọng cho người dùng.

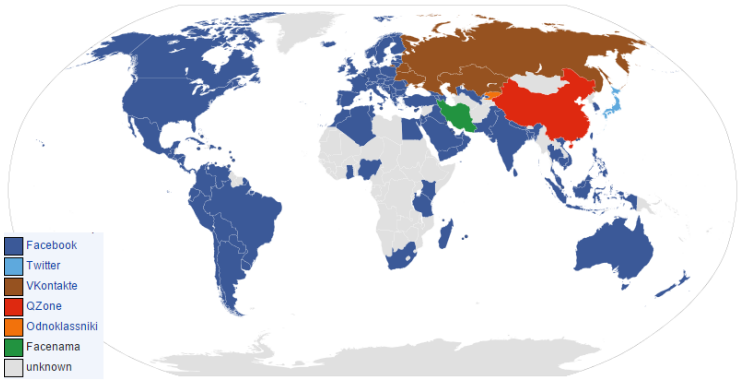
Kế thừa các bước phát triển của các mạng xã hội đi trước, năm 2004 mạng xã hội MySpace[5] ra đời với nhiều tính năng mới cho phép người dùng tải các hình ảnh video nhanh chóng thu hút hàng chục ngàn thành viên mới mỗi ngày. Không những vậy, các thành viên cũ của Friendster cũng chuyển qua MySpace chỉ trong vòng một năm. Điều này cũng phản ánh rõ nhu cầu của người dùng đối với một mạng xã hội càng ngày càng lớn. Mạng xã hội giờ không chỉ là một không gian



Hình 1.1: Doanh thu của mạng xã hội Facebook (đơn vị Triệu USD)

để người dùng trao đổi, tương tác, kết bạn với nhau mà còn là nơi thể hiện quan điểm, ý kiến, sở thích.. của người dùng. Nắm được các nhu cầu của này của người dùng, MySpace trở thành mạng xã hội đầu tiên có nhiều lượt xem hơn cả Google và được tập đoàn News Corporation mua lại với giá 580 triệu USD.

[2]https://www.classmate.com
[3]https://www.sixgegrees.org
[4]https://www.friendster.org
[5]https://www.myspace.org



Hình 1.2: Sự phân bố của MXH trên toàn thế giới [45]

Năm 2006, sự ra đời của mạng xã hội Facebook đánh dấu bước ngoặt mới cho hệ thống mạng xã hội trực tuyến. Với nền tảng nền tảng *Facebook Platform* hỗ trợ mạng mẽ cho các ứng dụng, người dùng có thể tạo ra những ứng dụng mới cho cá nhân mình cũng như các thành viên khác. Facebook nhanh chóng gặt hái được thành công vượt bậc, mang lại hàng trăm tính năng mới cho Facebook và đóng góp không nhỏ cho con số trung bình 19 phút mà các thành viên bỏ ra trên trang này mỗi ngày [3]. Đến đây khái niệm về mạng xã hội mới thực sự được hình thành và đầy đủ giống như hiện nay.

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. Ngoài ra, còn số một số mạng xã hội lớn khác như Orkut và Hi5 tại Nam Mỹ; Friendster tại châu Á và các đảo quốc Thái Bình Dương. Một số mạng xã hội gặt hái được nhiều công đáng kể như Bebo tại Anh, CyWorld tại Hàn Quốc, Mixi tại Nhật Bản. Ở Việt Nam hiện nay có một số mạng xã hội như: Zing Me, YuMe, Tamtay cũng đã thu hút được nhiều người dùng nhiều mục đích khác nhau.

1.1.2 Những đặc điểm chung của mạng xã hội

Một mạng xã hội giống như một xã hội ảo, trong đó mỗi tài khoản là một cá nhân trong xã hội. Tuy nhiên, khác với thế giới thực, mỗi mạng xã hội bao gồm một số đặc điểm nổi bật: khả năng truyền tài thông tin nhanh và lưu trữ lượng thông tin khổng lồ, tính tương tác, tính liên kết cộng đồng.

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. Những thành viên trong mạng xã hội là một mắt xích để tạo ra mạng lưới truyền tải thông tin đó.

Người dùng trong mạng xã hội có thể tương tác với nhau bất kể khoảng cách về địa lý, ngôn ngữ, giới tính, tôn giáo. Nếu như trong thế giới thực, chúng ta phải gặp nhau để trao đổi, trò chuyện, hay cùng hợp tác thì ngày nay việc đó thật đơn giản và thuận tiện hơn rất nhiều.

Mỗi mạng xã hộ đều có những chức năng tương tự nhau như: đăng trạng thái, đăng tải nhạc, hình ảnh, video clip, tạo thông điệp vv..nhưng được phân bổ dung lượng khác nhau. Các trang mạng xã hội lưu trữ thông tin nhóm và sắp xếp chúng theo những trình tự thời gian, nhờ đó người sử dụng có thể truy cập và tìm lại những thông tin đã đăng tải.

Là những website mở, nội dung được xây dựng hoàn toàn dựa trên các thành viên tham gia. Người dùng cũng có thể chia sẻ các quan đểm cá nhân của mình với những người xung quanh. Đây là một đặc điểm quan trọng trong mạng xã hội, nó giúp mỗi người dùng có nơi thể hiện quan điểm, ý kiến riêng của mình về một vấn đề nào đó.

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. Sau khi đăng ký mở tài khoản, người dùng có thể tự do xây dựng một không gian riêng cho bản thân. Nhờ các tiện ích và dịch vụ mà mạng xã hội cung cấp, người dùng có thể chia sẻ đường dẫn, tệp tin, hình ảnh, video..Không những vậy, họ còn có thể tham gia vào các trò chơi trực tuyến đòi hỏi có nhiều người cùng tham gia, gửi tin nhắn, chat với bạn vè, từ đó tạo dựng các mối quan hệ trong xã hội ảo.

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. Những người chia sẻ cùng một mối quan tâm có thể tập hợp lại thành các nhóm trê mạng xã hội, thường xuyên giao lưu, chia sẻ trên mạng thông qua việc bình luận hay dẫn đến các liên kết chung của nhóm.

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

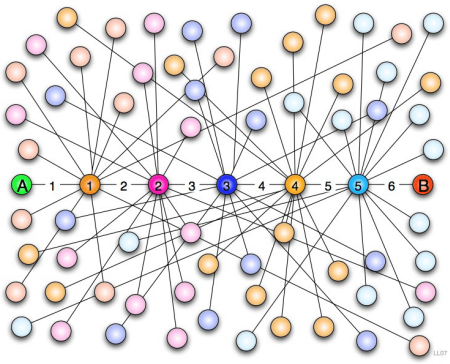
- Nut (node): Là một thực thể trong mạng, thực thể này thường biểu diễn mỗi

Tên	Miêu tả	Số thành viên
Facebook	Phổ biến, nhiều nhân vật nổi tiếng	900,000,000
Twitter	Mạng nhắn tin nhanh, blog nhỏ	310,000,000
LinkedIn	Kinh doanh và mạng lưới chuyên nghiệp	255,000,000
Pinterest	Bảng ghi chú trực tuyến, chia sẻ sở thích	250,000,000
Google+	Tổng hợp	120,000,000
MySpace	Tổng hợp	61,037,000
Others		255,539,000

Bảng 1.1: Một số mạng xã hội tiêu biểu

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.



Hình 1.3: Cấu tạo của một MXH [18]

Như vậy 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. Tùy từng bài toán cụ thể mà mô hình đồ thị có thể là: Đồ thị có hướng, vô hướng, có trọng số vv.. Ngoài ra, một số nghiên cứu đề xuất xét thuộc tính cho các đỉnh tương ứng với sự quan tâm cho người dùng.

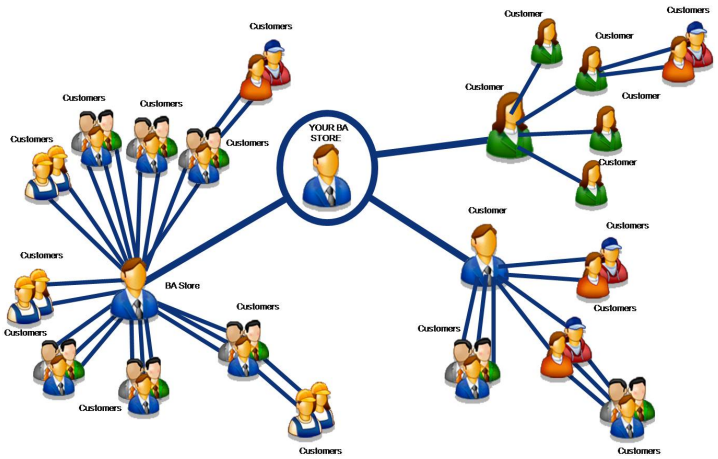
1.2 Lợi ích của mạng xã hội

1.2.1 Ứng dụng trong kinh doanh

Việc sử dụng các dịch vụ mạng xã hội của các doanh nghiệp là một tiềm năng lớn có một ảnh hưởng lớn đối với kinh tế thế giới. Mạng xã hội kết nối mọi người với chi phí thấp; điều này mang lại lợi ích cho các doanh nghiệp tìm cách mở rộng hơn trong hoạt động kinh doanh của họ, từ việc giao dịch với khách hàng, đối tác. Các mạng này thường đóng vai trò như một công cụ quản lý quan hệ khách

hàng cho các công ty bán sản phẩm và dịch vụ, các mạng xã hội có thể làm cho nó dễ dàng hơn để giữ liên lạc với các khách hàng trên toàn thế giới.

Đối với việc quảng bá thương hiệu của doanh nghiệp, các công ty cũng có thể sử dụng mạng xã hội để quảng cáo dưới dạng biểu ngữ và văn bản. Ngoài ra, các ứng dụng cho các trang web mạng xã hội đã mở rộng cho các doanh nghiệp nâng cao khả năng thúc đẩy sản phẩm, tạo môi trường tương tác thuận lợi hơn cho sản phẩm qua đó xây dựng thương hiệu lớn mạnh cho doanh nghiệp.



Hình 1.4: Các nhà kinh doanh sử dụng MXH cho hoạt động marketing [45].

Sức mạnh của các mạng xã hội tạo ra sự hợp tác đối với các người dùng trong doanh nghiệp, các doanh nghiệp khác nhau trên toàn thế giới, không phân biệt lãnh thổ là một xu hướng tất yếu. Điều này tạo ra một môi trường kinh doanh năng động và triển vọng đối với kinh tế toàn cầu.

1.2.2 Tìm kiếm các mối quan hệ

Con người hiện đại có ít thời gian dành cho bản thân và mở rộng các mối quan hệ. Nhờ có mạng xã hội, con người có thể tìm kiếm các mối quan hệ mới cũng như duy trì các mối quan hệ hiện có.

Có nhiều người sử dụng chỉ cần sử dụng nó để giữ liên lạc với bạn bè và đồng nghiệp của họ. Họ có thể nói chuyện với nhau, tương tác với nhau trên mạng xã hội thay vì gặp nhau trực tiếp.

Ngoài ra họ cũng có thể mở rộng các mối quan hệ khác về mọi lĩnh vực về người dùng quan tâm. Người dùng có thể kết bạn với trong nhiều nhóm bạn với những sở thích, sở trường khác nhau. Hầu hết các mạng xã hội đều yêu cầu người dùng để đưa ra một số thông tin nhất định thường bao gồm: độ tuổi, giới tính, địa điểm, quan điểm, sở thích vv.. Tuy nhiên, những thông tin rất cá nhân thường

không được khuyến khích vì lý do an toàn. Điều này cho phép người dùng khác tìm kiếm theo một số loại tiêu chuẩn phù hợp đối với mình và duy trì một mức độ ẩn danh tương tự như hầu hết các dịch vụ hẹn hò trực tuyến.

Một trong việc tìm kiếm mối quan hệ mới theo xu hướng mới đây là nhu cầu hẹn hò, tìm bạn. Nhu cầu này đã trở thành một nhu cầu mạnh mẽ trong thế giới thực trong bối cảnh con người ngày càng trở nên có ít thời gian riêng tư cho bản thân. Nhiều mạng xã hội cung cấp một môi trường trực tuyến để mọi người giao tiếp và trao đổi thông tin cá nhân cho các mục đích hẹn hò.

1.2.3 Ứng dụng trong giáo dục

Các mạng xã hội cũng được sử dụng cho việc học tập. Theo báo cáo của Hội Liên hiệp giáo dục Mỹ (The National School Boards Association), 60 % sinh viên sử dụng mạng xã hội nói chuyện về chủ đề giáo dục trực tuyến, và hơn 50% nói chuyện cụ thể về việc học ở trường. Ngoài ra, hơn 60% giáo viên sử dụng mạng xã hội và các phương tiện truyền thông phục vụ cho việc giảng dạy của mình, gồm: chia sẻ tài liệu, bài giảng, giáo án, bài tập và các thông tin về môn học [45].

Hình 1.5: Mạng xã hội HASTAC

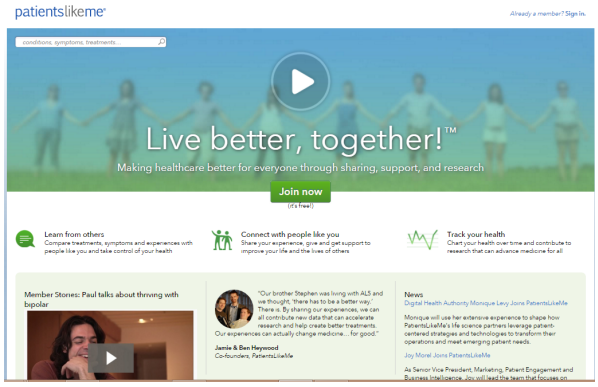
Theo xu thế đó một số mạng xã hội ra đời tập trung vào việc hỗ trợ các mối quan hệ giữa giáo viên và sinh viên cho việc học tập, phát triển sự nghiệp giáo dục và chia sẻ học liệu. Điển hình là mạng xã hội HASTAC tạo môi trường cho việc học tập và nghiên cứu trong giáo dục đại học. Mạng xã hội Ning hỗ trợ giáo viên trong công việc giảng dạy của mình. Một số mạng xã hội khác như: TermWiki, Learn Central, TeachStreet và các trang web khác được xây dựng để thúc đẩy mối các quan hệ trong giáo dục bao gồm các blog giáo dục, ePortfolios cũng như thông tin liên lạc như chat, bài thảo luận, và các diễn đàn học tập. Những trang mạng xã hội này cũng có nội dung tính năng chia sẻ, đánh giá cho phép người

học đánh giá đối với người dạy, tài liệu, bài giảng ... Thêm vào đó, các MXH cũng còn có thêm các chức năng giám sát đối với phụ huynh và giáo viên đối với con em mình.

1.2.4 Ứng dụng trong y tế và sức khỏe

Các mạng xã hội đang cũng bắt đầu ứng dụng các tiện ích chăm sóc sức khỏe như một phương tiện để truyền đạt kiến thức về thể chất hay phổ biến kiến thức của bác sỹ về các loại bệnh thường gặp. Đây là một xu hướng mới nổi được các mạng xã hội tạo ra để giúp các thành viên với chứng bệnh khác nhau về thể chất cũng tinh thần [56].

Đối với những người mắc bệnh do môi trường sống thay đổi mạng xã hội PatientsLikeMe cung cấp cho các thành viên cơ hội để kết nối với những người khác. Đồng thời cung cấp dữ liệu nghiên cứu về bệnh nhân có liên quan với điều kiện giống với họ.



Hình 1.6: Mạng xã hội Patients Like Me.

Đối với những người nghiện rượu và nghiện, Sober cung cấp cho người dân trong việc phục hồi khả năng giao tiếp với nhau và tăng cường sự phục hồi của họ. DailyStrength là một trang web cung cấp các nhóm hỗ trợ cho một loạt các chủ đề và điều kiện, bao gồm các chủ đề hỗ trợ được cung cấp bởi PatientsLikeMe và SoberCircle.

Một số mạng xã hội nhằm mục đích khuyến khích lối sống lành mạnh đối với người dùng. Ví dụ như: Mạng xã hội SparkPeople cung cấp cho cộng đồng các công cụ trợ đồng đẳng trong việc giảm cân, Fitocracy và QUENTIQ tập trung vào hướng dẫn người dùng trong tập thể dục hoặc cho phép người dùng chia sẻ tập luyện của mình và nhận xét về những người dùng khác.

1.2.5 Tác động chính trị và xã hội

Các mạng xã hội gần đây đã cho thấy một giá trị lớn trong phong các trào xã hội và chính trị. Trong cuộc cách mạng Ai Cập năm 2011, Facebook và Twitter đều đóng một vai trò then chốt trong kết nối các cá nhân và tổ chức trong cuộc nổi dậy. Các nhà hoạt động Ai Cập đã đưa các thông tin về kế hoạch hoạt động cho nhóm người của họ trên mạng các mạng này. Họ cũng đưa ra những băng chứng cho hàng ngàn người về sự tàn bạo của chính phủ qua các video.

Tuy vậy, đối với chiều hướng ngược lại, mạng xã hội có thể là một công cụ quan trọng trong cuộc cách mạng và nổi dậy nhưng nó cũng cho phép các cơ quan chính phủ để dễ dàng xác định và đàn áp những người biểu tình hoặc bất đồng chính kiến.

1.2.6 Các ứng dụng cho chính phủ

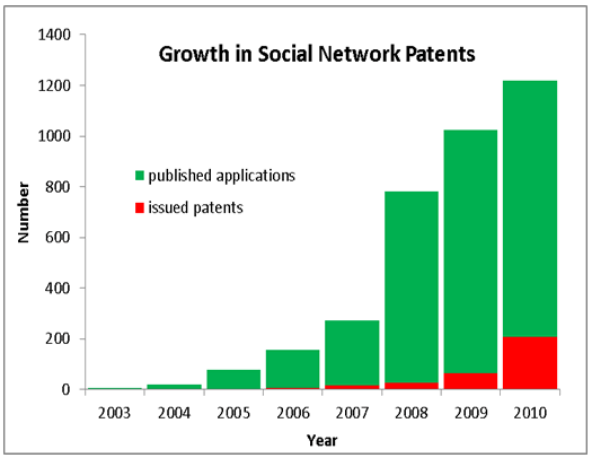
Các cơ quan hành chính cũng sử dụng mạng xã hội với các mục đích khác nhau. Sử dụng công cụ mạng xã hội là một cách nhanh chóng và dễ dàng để tiếp nhận những ý kiến của công chúng và để cho công chúng cập nhật hoạt động của họ. Tuy nhiên điều này đi kèm với một nguy cơ quá lạm dụng các trang mạng xã hội. Điều này cũng có thể gia tăng sự sợ hãi, đề phòng của người dân đối với chính phủ.

Trong vấn đề quản lý nhà nước đối với các hoạt động xã hội và phục vụ người dân, các mạng xã hội có vai trò quan trọng và trở thành những xu hướng mới chưa từng thấy trước đây. Trung tâm kiểm soát dịch bệnh Mỹ đã chứng minh tầm quan trọng của tiêm chủng đối với trẻ em trên trang mạng Whyville. Whyville và Trung tâm điều hành Đại dương và khí quyển (National Oceanic and Atmospheric Administration) của Mỹ đã thông báo có một hòn đảo ảo trên trang mạng Second Life, qua đó mọi người dân có thể khám phá các hang động ngầm hoặc tìm hiểu tác động của sự nóng lên toàn cầu.

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

Với sự ra đời và phát triển mạnh mẽ, hiện nay mạng xã hội đã và đang thu hút nhiều sự chú ý, quan tâm của các nhà nghiên cứu. Rất nhiều những nghiên cứu và bằng sáng chế có tính ứng dụng cao được áp dụng trên MXH. Bảng dưới đây thống kê về số lượng nghiên cứu và bằng sáng chế về MXH ở Mỹ từ 2003 đến

2010 [45].



Hình 1.7: Số lượng nghiên cứu và sáng chế về MXH ở Mỹ từ 2003 đến 2010 [45]

Trong phần này luận văn sẽ đề cập đến những vấn đề đang được quan tâm, nghiên cứu đối với mạng xã hội hiện nay.

1.3.1 Khai phá dữ liệu trên mạng xã hội

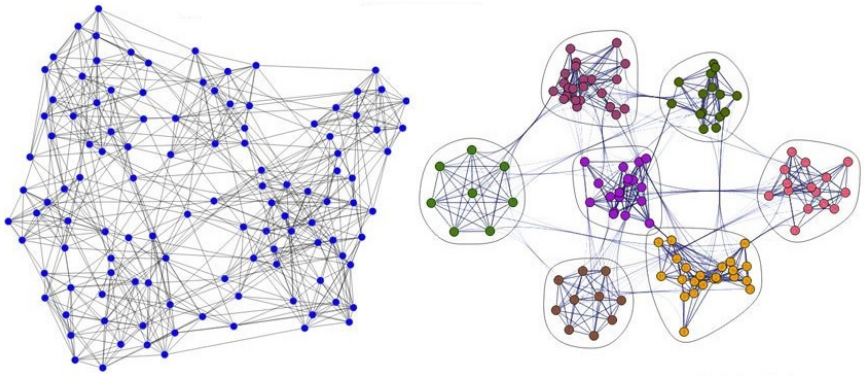
Khai phá dữ liệu trên mạng xã hội thực chất là một bài toán không mới vì các mạng xã hội thực chất các mạng xã hội là những trang web. Tuy vậy, do những đặc điểm riêng của mạng xã hội, việc khai phá và phân tích dữ liệu cũng có nhiều hướng tiếp cận, phương pháp và mục tiêu khác. Một bài toán quan trọng trong lớp bài toán này là khai phá quan điểm cộng đồng mạng xã hội.

Bài toán khai phá quan điểm cộng đồng mạng xã hội là đánh giá quan điểm của người dùng trên mạng xã hội về cùng một sự kiện, hiện tượng. Khai phá quan điểm cộng đồng bao gồm ba bài toán điển hình là: phân lớp quan điểm, khái phá và tổng hợp quan điểm dựa trên đặc trưng, khai phá quan hệ (so sánh). Trong mấy năm gần đây, nhiều công trình nghiên cứu đã đề xuất các phương pháp khai phá quan điểm cộng đồng sử dụng các kỹ thuật trong khai phá dữ liệu và học máy như phương pháp học cây quyết định, mạng Bayes, phương pháp k láng giềng gần nhất (kNN) [16], phương pháp máy véc tơ hỗ trợ (SVM), các kỹ thuật học máy nửa giám sát vv.. Các công bố điển hình có kể kể đến là các công trình [14, 15].

Khi các doanh nghiệm ứng dụng việc khai thác dữ liệu người dùng, họ có thể nâng cao doanh số và lợi nhuận của họ dựa trên những thông tin học có được. Ngoài ra, với dữ liệu này, các công ty tạo ra các hồ sơ khách hàng với và hành vi trực tuyến. Từ đây, họ có thể đưa ra các chiến lược phù hợp nhất cho hoạt động kinh doanh của mình.

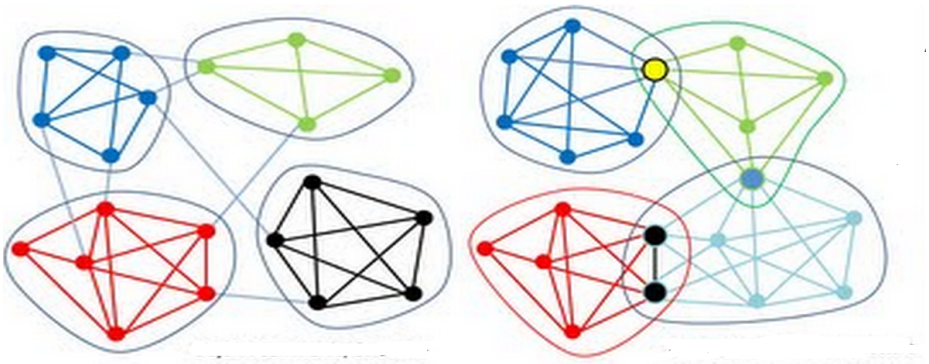
1.3.2 Phát hiện cấu trúc cộng đồng trên mạng xã hội

Bài toán phát hiện cấu trúc cộng đồng (Community Structure) được quan tâm không chỉ trên mạng xã hội mà còn đối với Khoa học mạng lưới (Network Science) nói chung. 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]. Mỗi tập như vậy gọi là một cộng đồng.



Hình 1.8: Mạng và cấu trúc cộng đồng tương ứng sử dụng Modularity [46].

Xét theo tiêu chí cấu trúc, việc đánh giá cộng đồng theo cấu trúc mạng được đánh giá theo hai tiêu chí: Cấu trúc cộng đồng tách rời (không chồng chéo) và cấu trúc cộng đồng chồng chéo. Trong trường hợp phát hiện cộng đồng không chồng chéo, mật độ của nhóm các nút, cạnh với các kết nối dày đặc trong nội bộ và kết nối mỏng manh giữa các nhóm. Mỗi nút trong mạng chỉ thuộc duy nhất một cộng đồng. Cấu trúc cộng đồng chồng chéo là một định nghĩa tổng quát hơn, theo đó mỗi nút có thể thuộc nhiều cộng đồng khác nhau. Các cặp nút có nhiều khả năng được kết nối nếu họ đều là thành viên của một cộng đồng, và ít có khả năng được kết nối nếu họ không nằm chung một cộng đồng.



Hình 1.9: Cấu trúc Cộng đồng tách rời và chồng chéo

Giả sử rằng đồ thị $G = (V, E)$ gồm tập đỉnh là V, tập cạnh là E và $|V| = n, |E| = m$. Ma trận kề của đồ thị là $A = A_{ij}$, bặc của đỉnh $v \in V$ là $d(v)$. Việc đánh giá cộng đồng có thể dựa theo các tiêu chí sau:

- Modularity (Newman 2006 [43]): Giả sử tập cộng đồng của đồ thị là $\mathcal{C} = \{C_1, C_2, \ldots, C_l\}$, việc phát hiện cộng đồng dựa trên cực đại hàm Modularity sau:

$$Q(\mathcal{C}) = \frac{1}{2m} \sum_{i,j \in V} (A_{ij} - \frac{d_i d_j}{2m}) \delta_{ij}$$

  Trong đó $\delta_{ij} = 1$ nếu như i và j thuộc cùng một cộng đồng, ngược lại $\delta_{ij} = 0$. Giá trị của hàm Modularity có thể âm hoặc dương, giá trị càng lớn thì cấu trúc cộng đồng của đồ thị càng mạnh mẽ.

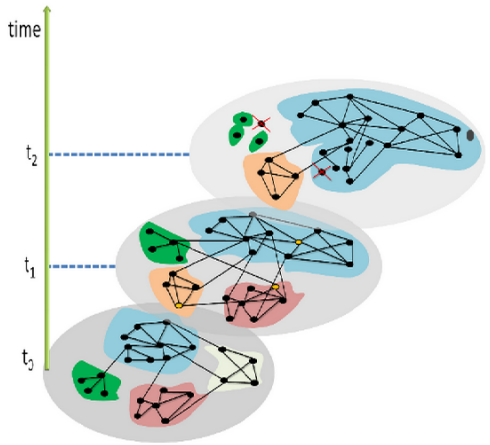
- Đánh giá cộng đồng dựa trên hàm mật độ (Fortunato 2007 [44]):

$$\phi(\mathcal{C}) = \frac{\mathcal{C}^{in}}{C^2_{|\mathcal{C}|}}$$

  Trong đó $\mathcal{C}^{in}$ số lượng các cạnh có đỉnh đầu và đỉnh cuối nằm trong $\mathcal{C}$. Đối với cách đánh giá này, tập $\mathcal{C} \subset V$ được gọi là cộng đồng nếu $\phi(\mathcal{C}) > \tau$, τ là giá trị ngưỡng cho cộng đồng

- Các phương pháp sử dụng các quá trình ngẫu nghiên, xác suất [40], sử dụng thuộc tính của các đỉnh [41].

Việc phát hiện cộng đồng còn được phân loại theo tiêu chí thời gian là: Cộng đồng tĩnh (Static Community) và cộng đồng động (Dynamic Community). Đối với cộng đồng tĩnh, việc xét cấu trúc cộng đồng tại một thời điểm xác định. Đối với cộng đồng động lại xét cấu trúc cộng đồng có sự thay đổi theo thời gian.



Hình 1.10: Cấu trúc Cộng đồng theo thời gian

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

Các mạng xã hội cung cấp một môi trường lan truyền thông tin nhanh chóng và thuận tiện. Đó là một ưu thế lớn đối với việc sử dụng mang trong tiếp thị thúc đẩy sản xuất đối với doanh nghiệp. 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. Bài toàn này có ý nghĩa lớn trong hoạt động tiếp thị (marketing) đối với các hoạt động kinh doanh trên mạng xã hội hiện nay.

Có thể lấy ví dụ như sau: Một doanh nghiệp mới sản xuất một sản phẩm mới, họ muốn thúc đẩy quảng cáo sản phẩm của họ với những đặc tính nổi bật tới người dùng trên mạng xã hội. Để làm việc này họ cần chọn người dùng ban đầu để bắt đầu thuyết phục họ tin dùng sản phẩm của mình (thái độ tích cực). Sau đó thông tin về sản phẩm bắt đầu lan truyền đến các người dùng khác. Tuy nhiên, do hoành cảnh về nhân lực và tài chính, họ chỉ có thể tiến hành hoạt động tiếp thị, thuyết phục đối với k người dùng nhất định. Yêu cầu đặt ra chọn k người dùng nào để bắt đầu sự lan truyền tin về sản phẩm của mình trên MXH sao cho người dùng có thái độ tích cực là lớn nhất.

Có thể nhận xét nếu người dùng được chọn là người quan trọng trong mạng lưới, có sức ảnh hưởng lớn thì sức ảnh hưởng sẽ lớn. Bài toán này nhận được nhiều sự quan tâm của những nhà nhiên cứu trong thời gian gần đây, nó không chỉ quan trọng đối với mạng xã hội mà còn đối với khoa học mạng lưới nói chung.

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 trên mạng xã hội đó là Mô hình ngưỡng (Threshold) và mô bậc độc lập (Independent Cascade), trong hai mô hình này, ông chỉ ra bài toán tối đa ảnh hưởng (Influence Maximum) là bài toán NP-Khó và đưa ra một thuật toán tham lam có tỷ lệ xấp xỉ là $1 - 1/e$ dựa trên tính chất của hàm mục tiêu là *submodular*.

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 như sau:

- Tối đa hóa ảnh hưởng tích cực đối với người dùng trên mạng xã hội [31]: Tìm k người dùng hạt giống để khởi tạo lan truyền sao cho ảnh hưởng tích cực mà họ gây ra trên mạng xã hội là cực đại.

- Tối đa hóa ảnh hưởng đến một người dùng cụ thể [32]: Tìm k người dùng trên mạng xã hội để khởi tạo lan truyền sao cho ảnh hưởng gay ra đến người dùng x là lớn nhất.

- Tìm số người dùng cực tiểu có thể gây ảnh hưởng trên mạng trong diện rộng [55]: Tìm số người nhỏ nhất có thể gây ra ảnh hướng đến $\beta.|V|, \beta \in (0,1)$ người trên mạng, với V là số đỉnh của đồ thị biểu diễn mạng xã hội.

- Tối đa hóa ảnh hưởng trên mạng xã hội động: Giải quyết bài toán trên mô hình mạng xã hội động thay đổi theo thời gian [33].

Trong lớp bài toán này, có hai lớp mô hình lan truyền thông tin được sử dụng đó là mô hình ngưỡng và mô hình thác nước [38]:

- *Mô hình ngưỡng tuyến tính (Linear Threshold Model)*: Cho đồ thị có trọng số $G = (V, E, w)$ với $|V| = n, |E| = m$. Trong mô hình này, mỗi đỉnh v có một ngưỡng θ_v. Gọi $N(v)$ là tập đỉnh hàng xóm của v, các trọng số thỏa mãn điều kiện: $\sum_{v \in N(u)} \leq 1$. Quá trình lan truyền thông tin được thực hiện theo từng bước rời rạc. Tại bước t, một đỉnh chưa được kích hoạt v được kích hoạt nếu thỏa mãn điều kiện sau:

$$\sum_{u \in N^a(v)} w(u,v) \geq \theta_v$$

  Trong đó $N^a(v)$ là tập hàng xóm của v đã được kích hoạt. Mỗi đỉnh khi đã được kích hoạt sẽ giữ nguyên trạng thái, quá trình diễn ra đến khi không có thêm đỉnh nào được kích hoạt.

- *Mô hình bậc độc lập (Independent Cascade Model)*: Trong mỗi bước, khi một đỉnh v được kích hoạt, nó sẽ có một cơ hội duy nhất để gây ảnh hưởng với một đỉnh láng giềng u với xác xuất thành công là $p(u,v)$.

Ngoài những hướng nghiên cứu trên, hiện nay bài toán này còn phát triển theo hướng ràng buộc lan truyền theo thời gian, xác suất lan truyền dưới hai mô hình LT và IC và tốc độ lan truyền [42].

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

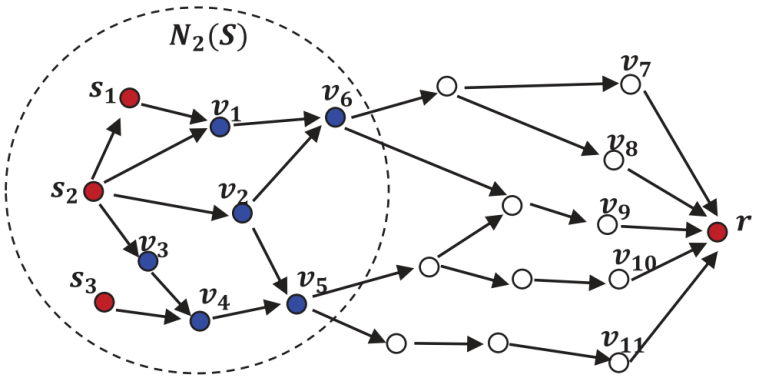
Trong thực tế trên mạng xã hội luôn tồn tại những thông tin lệnh lạc, không lành mạnh gây ra ảnh hưởng tiêu cực đến người dùng trên mạng xã hội. Hơn nữa

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. Ví dụ: Những thông tin không đúng về sự phát tán một dịch bệnh nguy hiểm ảnh hưởng tiêu cực đến người dùng trên mạng. Nó có thể ảnh hưởng đến tinh thần, thái độ, thậm chí cả kinh tế của khu vực người dùng sinh sống. Trong hoạt động kinh doanh, những thông tin sai lệnh tiêu cực về sản phẩm của một doanh nghiệp ảnh hưởng xấu đến tài chính, giá bán, doanh thu, và thậm chí là thương hiệu của doanh nghiệp đó. Đối với từng cá nhân, những thông tin sai lệnh về họ có thể ảnh hưởng rất xấu, làm đảo lộn cuộc sống của họ.

Những trường hợp trên cho ta thấy, việc đối phó với các thông tin sai lệnh là vô cùng cấp bách. Tuy nhiên, việc phát hiện những nguồn chứa thông tin sai lệnh là không đơn giản. Do đó thay vì việc phát hiện các thông tin này, những nghiên cứu thường tập trung vào việc giám sát và lan truyền thông tin tốt để đối kháng, lấn át các thông tin xấu. Trong việc giám sát các thông tin sai lệnh H Zhang [48] đã đề xuất giải pháp tìm số node giám sát nhỏ nhất sao cho có thể phát hiện được thông tin sai lệnh trên MXH với tỷ lệ τ.

Trong việc hạn chế phát tán thông tin sai lệnh, Zhang [39] để xuất bài toán tìm số nút nhỏ nhất trong khoảng cách δ (vùng $N_\delta()$) đối với nguồn phát thông tin sai lệnh để vô hiệu hóa sao cho thông tin sai lệnh đến nút đích r được giới hạn.



Hình 1.11: Vô hiệu hóa các nút trong vùng $N_2(s)$ để ngăn chặn thông tin sai lệnh [39]

Trong hình 1.11, tập nút $S = \{s_1, s_2, s_3\}$ là nguồn phát, khi $\delta = 2$, tập đỉnh tối ưu để tiến hành vô hiệu hóa trong trường hợp này là $\{v_5, v_6\}$.

Trong việc khử nhiễm đối với nguồn tin sai lệnh, Nguyen [36] đề xuất bài toán

tìm tập người dùng hạt giống sao cho tỷ lệ khử nhiễm sau thời gian T đối vơi nguồn thông tin sai lệnh I trong mạng là $\beta \in (0, 1)$. Tức là khử nhiễm đối với các nguồn phát này sao cho số người dùng được khử nhiễm là $\beta.|V|$. Họ đa đưa ra bốn trường hợp cho cả T và I, tuy nghiên trong nghiên cứu này họ chỉ giải quyết cho trường hợp I chưa biết và T là hữu hạn. Họ cũng đưa ra một thuật toán gần đúng có chặn trên trong việc tìm lời giải bài toán.

Ceren [34] đưa ra bài toán phản bác lại thông tin sai lệnh bằng cách chọn k người dùng để thuyết phục họ nhận thức được các thông tin để phản bác lại, triệt tiêu các thông tin sai lệnh. Trong nghiên cứu này, tác giả đã xây dựng mô hình Oblivious Independent Campaign, họ chứng minh đây là bài toán NP-Khó và hàm mực tiêu là hàm đơn điệu tăng và *submodular*.

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.. Đây là những thông tin mà kẻ xấu có thể lợi dụng để phục vụ cho các mục đích của chúng. Chúng có thể dùng các thông tin này để lừa đảo, gửi spam, phát tán virus, ... Vấn đề này sẽ được luận văn đề cập chi tiết hơn ở Chương 2.

Ngoài những thông tin cá nhân, người dùng cũng còn để lộ những thông tin nội dung bài đăng, đề cập hay chia sẻ của mình. Ví dụ: Khi một người dùng muốn chia sẽ những thông tin, trạng thái của mình cho bạn bè mà không muốn hạn chế người dùng trong mạng. Nhưng thông tin này có thể vô tình bị những người không mà họ không mong muốn biết. Về vấn đề này, Shen [51] [53] đã xây dựng bài toán tối đa hóa tin tưởng trong chia sẻ thông tin tưởng trong chia sẻ thông tin với bạn bè trong khi hạn chế khả năng thông tin đến được người dùng không mong muốn với xác suất nhỏ hơn hoặc bằng ngưỡng $\tau \in (0, 1)$.

Chương 2
CÁC NGUY CƠ MẤT AN TOÀN TRÊN MẠNG XÃ HỘI

Trong phần này, luận văn nêu lên các nguy cơ mất an toàn khi sử dụng mạng xã hội. Trong những nguy cơ này, có những nguy cơ truyền thống đã xuất hiện trước khi các mạng xã hội trở nên phổ biến. Ngoài ra, luận văn cũng đề cập đến các nguy cơ mới nảy sinh bởi đặc tính của mạng xã hội. Trong đó đặc biệt tập trung vào những nguy cơ rò rỉ thông tin. Đây là những nguy cơ mới được quan tâm trong thời gian gần đây. Những nguy cơ này nảy sinh và phổ biến dựa vào đặc tính lan truyền thông tin mạnh mẽ của các mạng xã hội. Những kết quả nghiên cứu cho thấy rằng việc rò rỉ thông tin của người dùng một cách chủ quan hay khách quan là khá dễ dàng và kẻ xấu có thể tấn công đến người dùng để lấy cắp thông tin một cách dễ dàng. Đặc biệt hơn, kẻ tấn công thực hiện những cuộc tấn công lấy cắp thông tin với quy mô lớn. Chúng thực hiện cuộc tấn công nhằm lấy thông tin của những người dùng mạng xã hội trong tổ chức nhất định với tỷ lệ thành công cao. Đây cũng là nội dung chính mà luận văn đã tìm hiểu để đưa ra biện pháp phòng ngừa hiệu quả.

2.1 Các nguy cơ mất an toàn truyền thống

Các nguy cơ mất an toàn truyền thống đã xuất hiện từ khi mạng Internet được sử dụng rộng rãi. Trong những nguy cơ này, kẻ tấn công thường sử dụng các phần mềm độc hại, thư rác, tấn công CSS (Cross-Site Scripting), phishing. Các vấn đề này tiếp tục diễn ra trên các mạng xã hội quy mô lớn. Mặc dù những nguy cơ này đã được giải quyết trước đó, tuy nhiên chúng có xu hướng phát triển mạnh do tính chất lan truyền nhanh chóng của các mạng xã hội. Các nguy cơ này lợi dụng thông tin của người dùng trên MXH để tấn công không chỉ người dùng mà còn tấn công bạn bè của họ bằng cách giả mạo hay lừa đảo.

Ví dụ, kẻ tấn công có thể gắn mã độc bên trong một thư rác hấp dẫn có sử dụng các thông tin của người dùng bên trong nó. Do tính chất cá nhân hoặc phản xạ tự nhiên khi nhìn thấy những thông tin của mình, khả năng cao người dùng mở thư và lây nhiễm mã độc. Trong nhiều trường hợp, mục tiêu của các cuộc tấn

công hướng đến là tài sản có giá trị và thiết yếu của người dùng như số thẻ tín dụng, mật khẩu tài khoản vv.. Đáng báo động là các nguy cơ kiểu này có thể khai thác các thông tin bị đánh cắp của người dùng bị nhiễm để gửi tin nhắn giả mạo của người dùng hoặc thậm chí thay đổi thông tin cá nhân của người dùng.

Dưới đây, luân văn nêu ra một số nguy cơ truyền thống phổ biến hiện được thực hiện rộng rãi trong những năm gần đây.

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.

Trong một số trường hợp, các phần mềm độc hại có thể sử dụng các thông tin thu được để mạo danh người dùng và gửi tin nhắn dễ lây lan đến bạn bè của người dùng.

Một trong các mã độc đầu tiên hoạt động theo nguyên tắc trên là Koobface. Koobface là phần mềm độc hại đầu tiên lan rộng thành công qua các mạng xã hội như Facebook, MySpace và Twitter. Khi người dùng nhiễm mã độc này, Koobface cố gắng để thu thập thông tin đăng nhập và lây nhiễm máy tính của người dùng để lan nhanh thành một mạng lưới rộng lớn gọi là botnet [54], giống như một "đội quân zombie" mà đối tượng bị lợi dụng là các máy tính. Sau đó các máy tính trong mạng botnet được sử dụng cho các hoạt động tội phạm, chẳng hạn như gửi tin nhắn rác và tấn công các máy tính và máy chủ khác trên Internet.

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. Trong nghiên cứu gần đây về vấn đề này cho thấy rằng người dùng trên mạng xã hội có khả năng bị lừa đảo bởi hình thức này cao hơn do bản chất tương tác của mạng xã hội giống như một xã hội thực [9].

Hơn nữa, trong những năm gần đây, những hoạt động lừa đảo trong các mạng xã hội đã tăng mạnh. Theo báo cáo tình báo an ninh của Microsoft, $84,5\%$ tất cả các cuộc tấn công lừa đảo nhắm vào người sử dụng trên các trang mạng xã hội [17]. Đối với mạng xã hội Facebook, kẻ tấn công có thể thu hút người dùng đăng

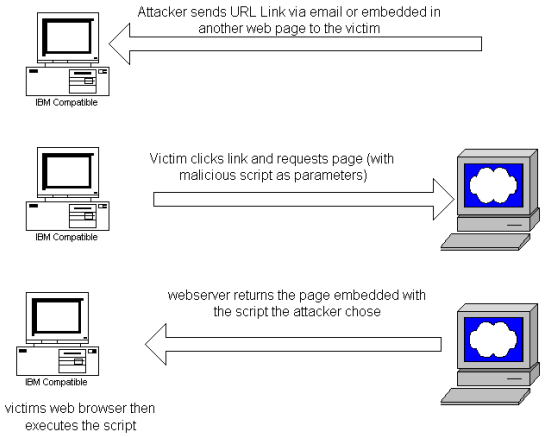
nhập và các trang Facebook giả mạo. Sau đó, lây lan giữa người dùng bằng cách mời bạn bè click vào một liên kết được đăng trên của người dùng. Tuy nhiên, sau đó Facebook đã hành động để ngăn chặn các cuộc tấn công này.

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. Kẻ gửi thư giác cũng có thể gửi các thông điệp này bằng các dạng bình luận trên các trang được nhiều người theo dõi, đề cập. Một ví dụ về sự phổ biến của thư rác có thể tìm thấy trên mạng xã hội Twitter. Vào tháng 8 nănm 2009 11% các tin nhắn Twitter là tin nhắn rác. Tuy nhiên, vào đầu năm 2010, Twitter đã cắt thành công xuống tỷ lệ thư rác xuống còn 1% [10].

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. Trong đó, những đoạn mã nguy hiểm đựoc chèn vào hầu hết được viết bằng các Client-Site Script như JavaScript, JScript, DHTML và cũng có thể là cả các thẻ HTML.



Hình 2.1: Tấn công XSS

Đối với CSS, người bị tấn công là người dùng chứ không phải là các website, kẻ tấn công có thể dùng XSS để gửi những đoạn script độc hại tới một người dùng

bất kỳ và trình duyệt của người dùng sẽ thực thi những đoạn script đí và gửi về cho kẻ tấn công những thông tin của người dùng thông qua email hoặc server do kẻ tấn công định sẵn từ trước.

Những trang mạng xã hội cũng là nền tảng để kẻ tấn công sử dụng kỹ thuật này. Hơn nữa, kẻ tấn công có thể sử dụng lỗ hổng CSS kết hợp với với môi trường mạng xã hội để tạo một sâu CSS có thể lan rộng trên toàn bộ mạng [11]. Trong tháng 4 năm 2009, một sâu XSS có tên là Mikeyy đã nhanh chóng lan rộng các tweet tự động trên mạng xã hội Twitter tới nhiều người dùng, trong đó có những người dùng nổi tiếng như Oprah Winfrey và Ashton Kutcher. Các sâu Mikeyy đã sử dụng một điểm yếu XSS và cấu trúc mạng Twitter để lây lan trên mạng xã hội này [12].

2.1.5 Lừa đảo trên Internet

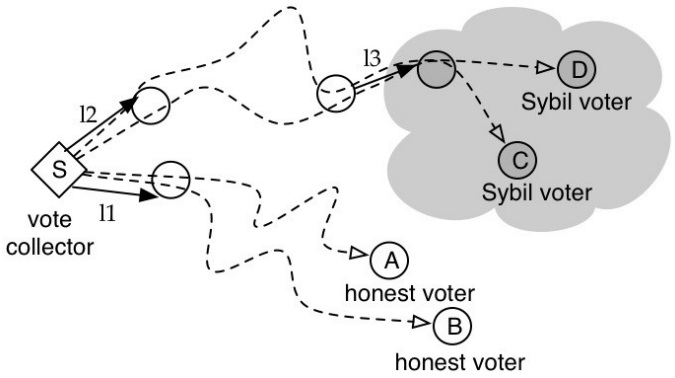
Lừa đảo trên Internet (*Internet Fraud*): hay còn gọi là lừa đảo trên mạng, dùng để chỉ sự truy cập Internet để lừa đảo hay lợi dụng người dùng trên mạng. Hình thức lừa đảo này xuất phát từ những hình thức lừa đảo trong mạng xã hội thực. Trong những năm gần đây, những kẻ lừa đảo hack được vào tài khoản của người dùng và chiếm quyền đăng nhập vào tài khoản của họ. Một khi họ quản lý để đăng nhập vào tài khoản của người dùng, những kẻ lừa đảo khéo léo hỏi bạn bè của người dùng để hỗ trợ trong việc chuyển tiền vào tài khoản ngân hàng của người lừa đảo. Một nạn nhân của kiểu lừa đảo này là Abigail Pickett. Trong khi đi du lịch ở Colombia, Abigail phát hiện tài khoản Facebook của mình đã bị hack bởi một người nào đó ở Nigeria. Sau đó cô ta phát hiện ra nó đã được sử dụng và yêu cầu gửi tiền cho bạn bè của mình với lý do rằng cô đang "mắc kẹt" [13]. Ngoài ra có nhiều hình thức lừa đảo trên mạng này đa dạng, phức tạp và càng ngày càng nhiều thủ đoạn tinh vi hơn.

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.

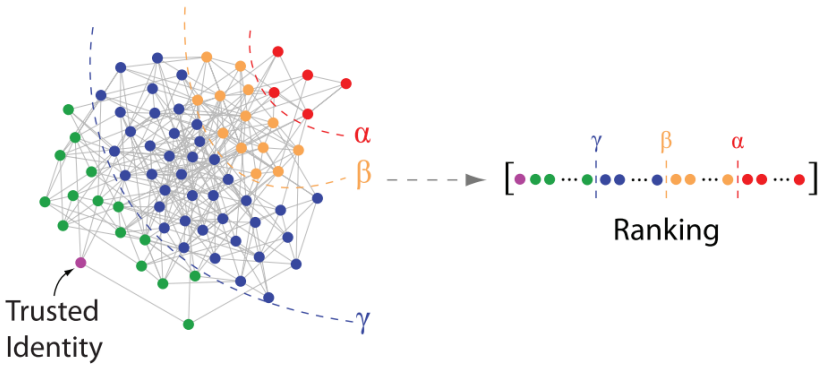
Nếu coi các website được xem là các nút mạng, có liên kết đến nhau tương

ứng với các cạnh trong đồ thị. Nút nào càng nhận nhiều liên kết đến nó thì càng chứng tỏ nút đó quan trọng. Những người phát tán nội dung rác hay spammer lợi dụng quy tắc này để tạo ra một liên kết nhằm bẫy các cổng tìm kiếm và người dùng. Đây chính hình thức của tấn công *mạo nhận* mà đối tượng khai thác của nó là các hệ thống dựa vào tầm quan trọng của một liên kết trong mạng hay còn gọi là *hệ thống danh tiếng* (reputation system). Cái tên Sybil Attack lấy tên theo một bệnh nhân "Sybil" (Shirley Ardell Mason) mắc chứng rối loạn đa nhân cách (multiple personality disorder) để ám chỉ việc giả mạo nhiều định danh dùng cho mục đích không trung thực. Trong các mạng xã hội, người có chủ đích tấn công



Hình 2.2: Tấn công mạo nhận

mạo nhận sẽ tạo một số lượng các nút ảo đủ lớn để tăng cường ảnh hưởng lên mạng. Mỗi một nút ảo mới sẽ đóng vai trò như là một phiếu bầu cho người tấn công. Ví dụ trên hệ thống mạng xã hôi Yotube. Kẻ tấn công có thể tạo các nút giả để đăng ký hay "like" đối với một số kênh nhằm có lợi cho chúng. Trong việc ngăn chặn sự giả mạo này Bimal [59] đã đề xuất một phương pháp nhằm xếp hạng các vùng tin cậy của các node theo các mức khác nhau. Tuy nhiên, phương pháp này phụ thuộc vào tham số α, β, γ mà mang tính chất định tính cao.



Hình 2.3: Xếp hạng vùng

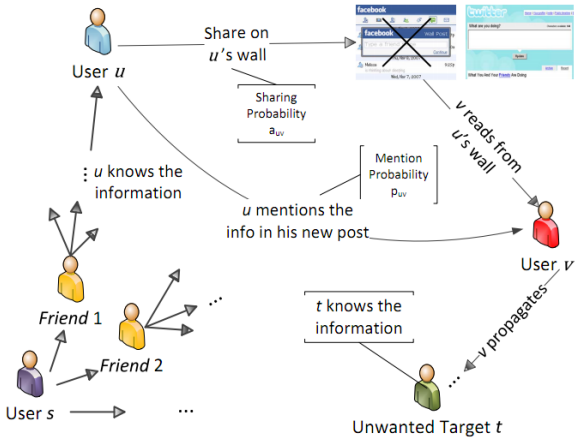
2.3 Rò rỉ thông tin trên mạng xã hội

Ngoài những nguy cơ mất an toàn truyền thống nói trên, người dùng trên mạng xã hội còn đối mặt với những nguy cơ rò rỉ thông tin. Sự rò rỉ thông tin đem lại cho người dùng cũng như cộng đồng mạng xã hội nói chung những tác hại to lớn.

Đối với cá nhân, những thông tin bị rò rỉ đến những người dùng khác mà họ không muốn chia sẻ thông tin ảnh hưởng lớn đến tính riêng tư qua đó có thể ảnh hưởng đến đời sống tin thần của họ hay lợi ích của họ. Đối với những tổ chức hoặc cộng đồng, sự rò rỉ thông tin của mỗi thành viên có thể tiết hộ về cơ cấu tổ chức, hoạt động và những thông tin của tổ chức đó. Có hai nhóm nguyên nhân dẫn tới sự dò rỉ thông tin của người dùng bao gồm: nguyên nhân chủ quan và nguyên nhân khách quan.

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.



Hình 2.4: Sự rò rỉ thông tin

Trong việc phòng ngừa sự rò rỉ thông tin, Dinh [51] đã đặt ra bài toán tối đa hóa sự chia sẻ thông tin trong khi hạn chế thông tin rò rỉ đến người dùng không mong muốn, tức là xác suất rò rỉ thông tin nhỏ hơn một ngưỡng cho trước.

Trong nghiên cứu này họ đã xây dựng bài toán trên mô hình mạng xã hội SML có hai tính năng là *chia sẻ* và *đề cập* trạng thái tương ứng với các chức năng chia sẻ và đề cập trạng thái đối với các mạng xã hội hiện nay, họ chỉ ra đây là

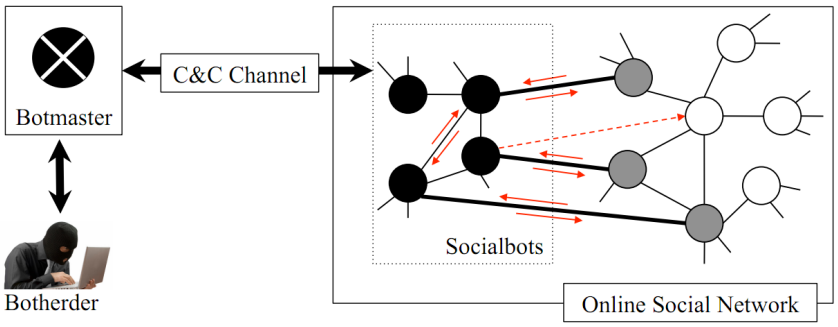
bài toán NP-đầy đủ và đưa ra thuật toán hiệu quả để giải quyết. Trong kết quả thực nghiệm họ chỉ ra rằng không nên chia sẻ thông tin với những người có số lượng bạn bè lớn vì khả năng để rò rỉ thông tin cao hơn so với người dùng khác. Nghiên cứu này còn được Shen [53] tiếp tục phân tích về lý thuyết độ phức tạp trong các trường hợp khác nhau của bài toán cũng như tính đảm bảo về mặt tối ưu của thuật toán.

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.

Khi lấy cắp được những thông tin trên, kẻ tấn công có thể sử dụng chúng cho những mục đích xấu. Ví dụ, chúng có thể thu thập e-mail của người dùng nhằm gửi spam, thư rác đề lừa đảo, phát tán virus phục vụ cho mục đích xấu. 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.



Hình 2.5: Socialbot tấn công đến người dùng

Socialbot (nút màu đen) tấn công đến đến các nút màu xám qua đó lan rông tấn công đến các nút màu trắng (chưa bị tấn công).

Kẻ tấn công cũng có thể dùng các thông tin của người dùng để giả mạo người dùng để lừa đảo bạn bè, người thân của họ hoặc thực hiện bán hàng trực tuyến

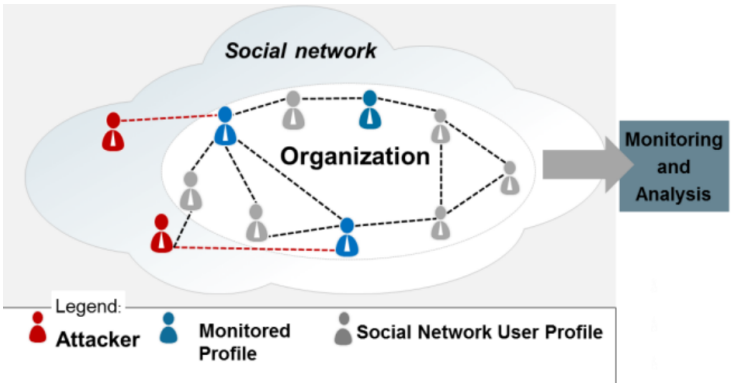
trên mạng

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 thônng 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. Qua đó nắm rõ vai trò của mỗi người dùng trong tổ chức, cơ cấu bộ máy tổ chức, hay thâm chí là những thông điệp mà người dùng trong tổ chức trao đổi với nhau. Những thông tin này có thể phục vụ cho các mục đích xấu như các trong các hoạt động gián điệp thương mại hoặc các hoạt động mang tính cạnh tranh khác.

Trong hướng nghiên cứu về vấn đề này, Yashar [7] đã đưa ra một thuật toán để thu thập thông tin của các nhân viên trong một tổ chức cụ thể trên mạng xã hội từ công chúng và từ đó có thể thể được tái tạo thông tin về tổ chức, ngoài ra ông cũng đã sử dụng Socialbots để trích xuất thông tin trong một tổ chức trên mạng xã hội [5].

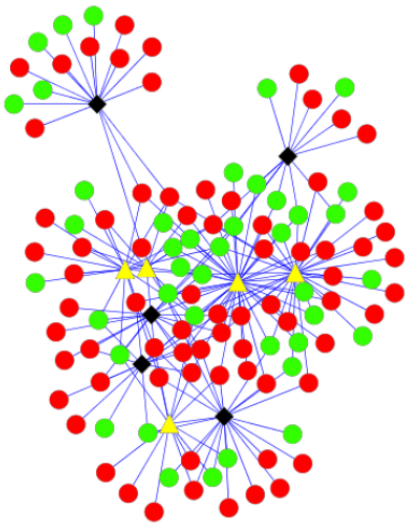
Socialboot đã được gửi yêu cầu kết bạn với những người sử dụng trong tổ chức cụ thể trên các mạng xã hội. Khi chấp nhận yêu cầu kết bạn này, Socialbot sẽ có được các thông tin về người dùng và các thông tin liên quan đến tổ chức mà họ đang tham gia.



Hình 2.6: Kẻ tấn công xâm nhập lấy cắp thông tin của người dùng trong tổ chức

Yashar [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.

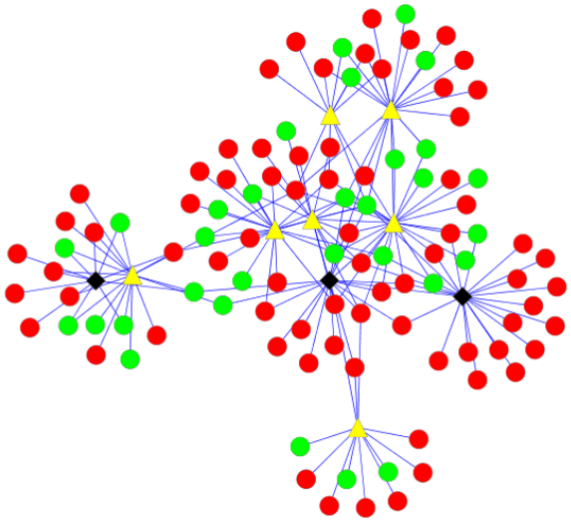
Các Socialbots này họ xâm nhập đến người dùng đích trong một tổ chức bằng cách tạo ra sự tin tưởng cho họ thông qua những người bạn của họ theo phương thức như sau: Đầu tiên, chúng tạo ra thông tin cá nhân giống như người dùng thật. Sau đó chúng gửi kết bạn với ít nhất 50 người dùng bất kỳ trên mạng 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 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.



Hình 2.7: Kết quả tấn công của Socialbot S_1 với tổ chức O_1.

Kết quả thí nghiệm này được thể hiện trong hình 2.7 và2.8. Các nút màu xanh lá cây biểu diễn người dùng chấp nhận yêu cầu kết bạn, màu đỏ là những người đã từ chối, màu vàng hình tam giác là người dùng đích đã chấp nhận yêu cầu và màu đen hình thoi là những người đã từ chối

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



Hình 2.8: Kết quả tấn công của Socialbot S_2 với tổ chức O_2.

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.

$N(u)$ là tập các đỉnh kề (hàng xóm) của đỉnh v, $d(v)$ là bậc của đỉnh v. $N_-(v)$ 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 kể 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

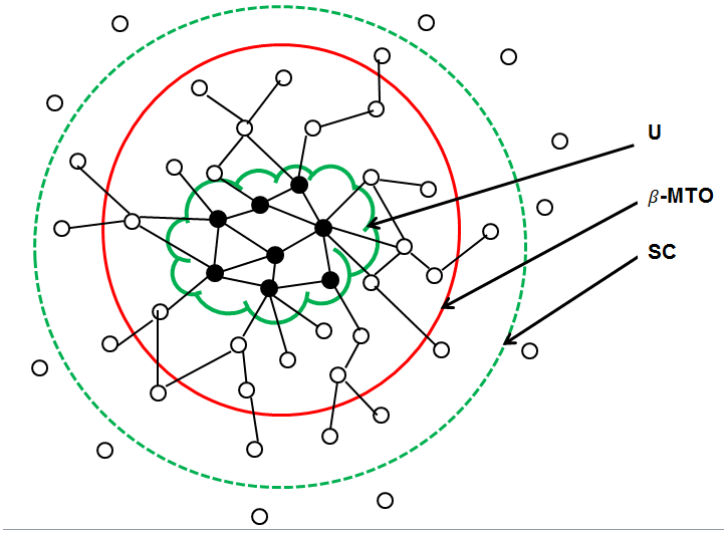
Trong phần này, luận văn đưa ra một giải pháp phòng ngừa xâm nhập bao gồm các quá trình sau: *Bài toán phòng ngừa xâm nhập* nói trên bao gồm các quá trình như sau:

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 an toàn* 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.



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

Mục đích cuối cùng của giải pháp này là tìm kiếm lời giải của bài toán β-MTO (tức là tìm vùng β-MTO) để xây dựng một vùng an toàn trên mạng bao bọc và bảo vệ cho tập người dùng U. Chi tiết và sự phân tích của mỗi quá trình trong giải pháp phòng ngừa này được luận văn nêu ở các mục tiếp theo.

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

Trong phần này, luận văn đưa đề xuất một độ đo để đánh giá mối quan hệ giữa hai người dùng trong mạng xã hội. Trước hết, để phân tích và ước lượng ảnh hưởng giữa người dùng qua những người dùng trung gian, luận văn áp dụng phương pháp chuẩn hóa trọng số của mạng.

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 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:

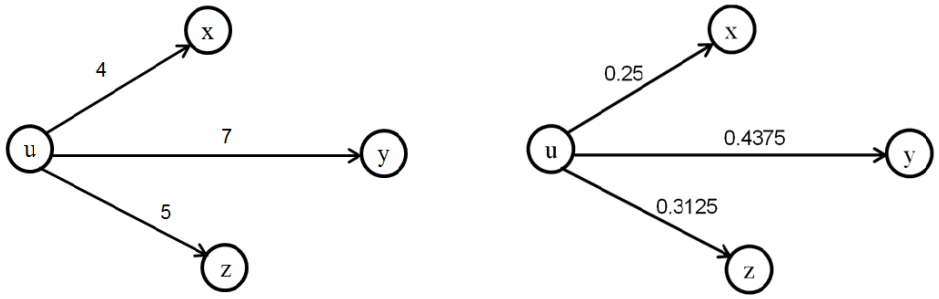
Nếu G' là đồ thị vô hướng:

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

Nếu G' là đồ thị có hướng:

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

Trong hai trường hợp ta đều đó tổng trọng số các cạnh đến một đỉnh $u \in V$ đều bằng 1. Trọng số $w(u,v)$ thể hiện tỷ lệ sự ảnh hưởng, mức độ quan tâm của đỉnh u tới đỉnh v so với tất cả các đỉnh láng giềng của v. Trọng số này càng cao thì mức độ quan tâm của u đến v càng lớn và ngược lại.



Hình 3.2: Ví dụ chuẩn hóa trọng số.

Việc đánh giá này phù hợp với thực tiễn tương tác giữa hai người dùng, nếu người dùng u "dành nhiều sự quan tâm" cho người dùng v thì tỉ lệ tương tác giữa u và v chiếm tỷ lệ cao hơn so với các người dùng khác là bạn của u.

3.3.2 Độ đo quan hệ giữa hai người dùng

Trong việc xác định mối quan hệ giữa hai người dùng trên MXH, đã có nhiều nghiên cứu đề cập đến vấn đề này. Trong đó nổi bật hơn cả là những nghiên cứu của Leskovec[21] và Fire[8].

Leskovec [21] nhận xét rằng bạn của bạn trong các mạng xã hội có khả năng cao là bạn của nhau. Fire [8] đưa ra một độ đo gọi là friend-measure. Độ đo này cho rằng càng nhiều kết nối giữa các nước láng giềng của hai người dùng, thì khả năng hai người dùng kết nối với nhau càng cao. Theo đó, độ đo giữa hai người dùng u và v được định nghĩa như sau:

$$\text{friend-measure}(u,v) = \sum_{x \in N(u)} \sum_{y \in N(v)} \delta(x,y) \tag{3.3}$$

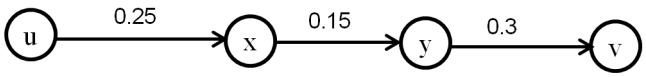
Trong đó, $\delta(x, y) = 1$ nếu $(x, y) \in E$ hoặc $(y, x) \in E$, $\delta(x, y) = 0$ trong trường hợp ngược lại. Hạn chế của độ đo này là chỉ được sử dụng đồ thị vô hướng, đồ thị không trọng số và chỉ xác định các mối quan hệ thông qua những người bạn chung không xét thông qua thông qua nhiều hơn một người dùng trung gian.

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, thậm chí còn nhanh chóng và mạnh mẽ hơn. Người dùng có thể gây ảnh hưởng qua lại thông qua người dùng trung gian giữa hai người dùng đó. Do đó, chúng ta có thể đánh giá mối quan hệ giữa hai người sử dụng thông qua những người dùng trung gian giữa họ.

Có thể lấy một ví dụ đơn giản như sau: Có ba người dùng x, y, z trên mạng xã hội, người dùng x và y thân thiết với nhau, y và z cũng thân thiết với nhau. Theo quan hệ này, người dùng x có thể gây ảnh hưởng đến y và sự ảnh hưởng này được y gây nên đối với z. Do đó, x có thể gây ảnh hưởng gián tiếp đến z thông qua người trung gian y.

Bằng cách sử dụng đồ thị $G = (V, E, w)$ để đánh giá ảnh hưởng giữa hai người dùng, 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:

$$W(P(u, v)) = \prod_{(a,b) \in P(u,v)} w(a, b) \tag{3.4}$$



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

Hình 3.3: Ước lượng ảnh hưởng đối với đường đi.

Chú ý rằng điều kiện áp dụng với ước lượng này là đường sơ cấp, tức là không có chu trình. Trong trường hợp đường đi xuất hiện chu trình thì việc đánh giá không còn chính xác.

Bằng các áp dụng các ước lượng ở công thức (3.4) 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 (3.4), 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:

$$\varphi(u, v, t) = \sum_{P(u,v) \in P, |P| = t+1} W(P(u, v)) \tag{3.5}$$

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 $t + 1$).

Cuối cùng, luận văn xuất độ đo hàm lượng mối quan hệ $\Phi(u, v)$ giữa hai người dùng qua nhiều nhất T người dùng trung gian, trong đó T là một tham số được cho trước bởi định nghĩa sau:

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:*

$$\Phi(u, v, T) = \sum_{t=0}^{T} \varphi(u, v, t) \tag{3.6}$$

Ý nghĩa của công thức (3.6) cho phép xác định các mối quan hệ giữa người sử dụng dựa trên việc đánh giá quan hệ của họ thông qua nhiều T người dùng trung gian đối với tất cả các mối quan hệ mà họ đã tham gia. Chú ý rằng việc đánh giá này theo chiều ảnh hưởng từ điểm đầu đến điểm cuối. Do vậy nếu đảo vị trí giữa u và v trong công thức (3.6) thì giá trị sẽ thay đổi.

Việc đánh giá này cũng thể hiện đúng mối quan hệ giữa hai người dùng trên mạng xã hội. Ảnh hưởng giữa hai người dùng đến nhau trên mạng đối với nhau có thể khác nhau do mức độ ưu tiên và sự quan tâm khác nhau.

Trong một mạng xã hội quy mô lớn, thông tin trên các cạnh giữa những người dùng thường bị thiếu. Việc mất thông tin xảy ra trong quá trình trích xuất thông tin. Bằng cách sử dụng biện pháp này, chúng ta có thể làm giàu (làm tăng thêm những thông tin cần thiết) của mạng bằng cách tính toán kết nối giữa người dùng một cách gián tiếp.

3.3.3 Thuật toán tính $\Phi(.)$

Áp dụng của ý tưởng thuật toán *loang* duyệt đồ thị theo chiều rộng, trong phần này luận văn đưa ra một thuật toán hiệu quả để tính độ đo Φ từ một đỉnh u tới các đỉnh v khác có khoảng cách nhỏ nhất với u là: $d(u,v) \leq T+1$. Do nếu $d(u,v) > T+1$ thì không tồn tại đường đi qua T đỉnh trung gian từ u đến v nên $\Phi(u,v) = 0$. Với nhận định này, việc tính toán sẽ được giảm bớt nhiều do không phải xét tất cả cặp đỉnh $(u,v) \in V^2$.

Algorithm 1: Thuật toán tính $\Phi(u,v,T)$

```
Data: G = (V, E, w), u, T.
Result: Φ(u, v, T), ∀v ∈ V, (u ≠ v)|d(u, v) ≤ T + 1.
1  begin
2      P(v, t) ← ∅ ;
3      Q_old ← ∅; Q_new ← ∅;
4      t ← 0;
5      Q_new ← u;
6      while t ≤ T do
7          for x ∈ Q_old do
8              \\ Tìm tất cả các đỉnh có thể đi đến từ x.
9              for v ∈ V, w(x, v) ≠ 0 do
10                 foreach P ∈ P(x, t − 1) do
11                     if Việc thêm v vào P không tạo chu trình then
12                         Q_new ← Q_new ∪ {v};
13                         P(v) ← P + {v};
14                         P(v, t) ← P(v) + P(v, t);
15                         W(v, t) ← W(P).w(x, v);
16                         Φ(u, v, T) ← W(v, t) + Φ(u, v, T);
17                     end
18                 end
19             end
20         end
21         Q_old ← Q_new;
22         Q_new ← ∅;
23         t ← t + 1;
24     end
25 end
```

Dựa trên ý tưởng của thuật toán *loang*, thuật toán tính độ đo từ một đỉnh u tới các đỉnh v có khoảng cách $d(u,v) \in T+1$ được mô tả như sau: Gọi $P(v,t)$ là tập các đường đi từ u đến v qua t người dùng trung gian, $W(P(v,t))$ là tổng trọng số của tất cả các đường đi thuộc $P(v,t)$. Q_{old} và Q_{new} là hai danh sách duyệt theo chiều rộng.

Bắt đầu từ các đỉnh x thuộc Q_{old}, thuật toán tìm các đỉnh v có thể đi đến từ x, sau đó cập nhật đường đi từ u đến các v bằng cách xét việc thêm v vào đường đi từ u đến x là $P \in P(x,t-1)$ đang xét có tạo thành chu trình không.

Nếu việc thêm v vào P không tạo thành chu trình, tao có một đường đi mới từ u đến v (gọi là $P(v)$) qua t, người dùng trung gian. Thêm đỉnh v vào danh sách mới và thêm đường đi này vào tập $P(v,t)$ và tính toán trọng số của đường đi này để cập nhật kết quả vào $W(u,t)$ và $\Phi(u,v)$.

Cuối cùng, thuật toán cập nhật lại các danh sách Q_{old}, Q_{new} để tính toán đối với các đường đi mới số người dùng trung gian tăng thêm 1, tiếp tục quá trình này đến khi $t = T$.

Việc tính toán độ đo quan hệ có ý nghĩa rất quan trọng trong việc xây dựng cộng đồng an toàn. Sau đây, ta sẽ xét độ phức tạp trong việc tính toán độ đo này. Xét vòng lặp for từ dòng 7 đến dòng 20, vòng lặp này sẽ xét tất cả các đỉnh có thể đi từ đỉnh u với khoảng cách bằng $t+1$ tức là qua t người dùng trung gian. Gọi $M(t)$ là số đỉnh trong tập Q_{new} trong mỗi bước t. Rõ ràng $M(t)$ cũng chính là số cạnh từ những người dùng trong Q_{old} và Q_{new}.

Xét vòng lặp while (ngoài vòng lặp for) từ dòng 6 đến dòng 24, theo quy tắc nhân ta có số phép toàn là: $M(0) + M(1) + \ldots + M(T)$.

Đây là một khối lượng tính toán khá lớn đối với việc đối với mỗi đỉnh đối với một mạng xã hội lớn. Các đại lượng $M(t)$ phụ thuộc số bậc của đỉnh. Số bậc càng lớn, số phép toán để tính đại lượng này càng lớn. Xét một trường hợp đơn giản khi tất cả các đỉnh có cùng bậc là d_0, thì $M(t) = d_0^{t+1}$.

3.3.4 Liên kết an toàn

Một câu hỏi đặt ra sau khi lượng hóa được mối quan hệ giữa hai người dùng, một câu hỏi đặt ra là làm thế nào để biết một mối quan hệ là tin cậy hay an toàn?

Để giải quyết vấn đề trên ta 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.

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

Ngưỡng an toàn này có thể thu được nhờ các phương pháp thống kê thực nghiệm. Sự an toàn đánh giá tính an toàn bằng $\Phi(u,v)$ có thể chống lại sự xâm nhập của Socialbots S đề cập trong [4].

Thật vậy, trong [4] đưa ra giải pháp xâm nhập tời một cá nhân X trong một tổ chức U bằng cách gửi yêu cầu kết bạn với những người bạn chung của X (tức là số người dùng trung gian là $t = 1$). Một khi chúng ta sử dụng độ đo $\Phi(u,v)$ để xem xét việc gửi yêu cầu kết bạn tới X với tham số $T \geq 2$ chúng ta sẽ hạn chế

sự xâm nhập. Trong trường hợp này, chúng ta xem xét mối quan hệ giữa S và X qua T người trung gian nên có thể thể tránh được việc kết bạn S thông qua người bạn chung của X (tức là $T = 1$) và nếu chọn chọn được tham số θ phù hợp sẽ lọc được việc tấn công có chủ đích từ S.

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.

Hầu hết các nghiên cứu về phát hiện cấu trúc cộng đồng dựa trên tối đa hóa *modularity* [19] và *mật độ* cạnh trong mạng [20]. Tuy nhiên, trong luận văn này không áp dụng những đánh giá trước đây về cấu trúc cộng đồng. Mục tiêu hướng tới trong xây dựng Cộng đồng an toàn là tạo một môi trường an toàn giữa người dùng với nhau bao quanh tổ chức người dùng. Ngoài ra, một yếu tố cần hướng đến là những người trong Cộng đồng an toàn phải thực sự là an toàn đối với tất cả những người dùng trong tổ chức. Theo tiêu chí đó, luận văn đưa ra một ước lượng sự an toàn của một cá nhân với tổ chức bởi định nghĩa sau:

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:*

$$f(v) = \frac{1}{|U|} \sum_{u \in U} \Phi(u, v, T) \tag{3.7}$$

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, tâp $f = f(v), v \in G^{sc}$ 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.*

Việc giới hạn xây dựng Cộng đồng an toàn trong k bước để giới hạn về độ dài các liên kết an toàn đối với tổ chức U. Nếu độ dài liên kết này quá lớn thì người dùng trên chuỗi liên kết này không có ý nghĩa nhiều với tổ chức U.

Cộng đồng an toàn $k - SC(U)$ là một đồ thị có hướng các cạnh đều là các liên kết an toàn. Mỗi đỉnh bất kì luôn có khoảng cách nhỏ hơn hoặc bằng k với ít nhất một đỉnh $u \in U$.

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

3.5.1 Xây dựng bài toán

Việc thêm người dùng mới vào Cộng đồng an toàn không đảm bảo rằng người đó đều an toàn với tất cả mọi người trong tổ chức U vì cách xây dựng cộng đồng này từ định nghĩa. Trong mô hình SC, tồn tại những người dùng chỉ mối quan hệ an toàn đối với một người dùng cụ thể (gọi là X) trong tổ chức và chúng ta không thể xác nhận sự an của họ toàn với những người khác trong tổ chức. Nói cách khác, nó là một sự an toàn có tính địa phương, không phải toàn diện cho tất cả.

Nếu kẻ tấn công sử dụng Socialboots S được đề xuất trong [4] có thể xâm nhập đến X bằng cách tạo ra mối quan hệ an toàn X (qua T người trung gian) và sau đó họ có thể xâm nhập vào Cộng đồng an toàn. Việc này có thể được thực hiện được khi S đã chọn người trong tổ chức có số lượng bạn bè ít nhất và xâm nhập đến họ theo phương pháp đã nêu trong [4]. Bằng phân tích trên, 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.

3.5.2 Độ khó của bài toán

Đây là một bài toán tối ưu rời rạc trên đồ thị, bài toán này được chứng minh là NP-Đầy đủ qua định lý sau.

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

Chứng minh. Để chứng minh MTO là bài toán NP-Đầy đủ, ta cần chứng minh hai khẳng định sau:

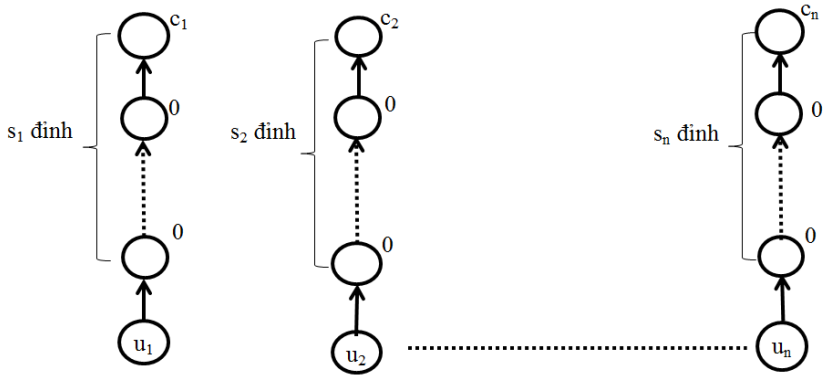
1) MTO thuộc lớp bài toán NP.

2) MTO là bài toán NP-Khó.

Xét phiên bản quyết định của bài toán β-MTO như sau:
Cho đồ thị $G^{sc} = (V^{sc}, E^{sc}, f)$, tập $U = \{u_1, u_2, .., u_k\}, U \subset V^{sc}$, một số thực $\beta \in \left(\frac{|U|}{|V^{sc}|}, 1\right)$ và một số thực Z. Có tồn tại hay không một 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: $|V_m| \leq \beta.|V^{sc}|$.
- Tổng số giá trị độ an toàn của mỗi đỉnh: $H(G_m) = \sum_{v \in V_m} f(v) \geq Z$.

Ta thấy rằng với một đồ thị con G_m của G^{sc}, việc kiểm tra một đồ đồ thị này có thỏa mãn yêu cầu của bài toán trên hay không trước hết ta cần kiểm tra tất cả các đỉnh $v \in V_m$ có thỏa mãn điều kiện liên thông với đỉnh $U \in V^{sc}$. Việc kiểm tra tính liên thông cần một thuật toán thời gian đa thức (thuật toán duyệt đồ thị theo chiều sâu hoặc rộng). Do đó, đối với G_m, cần một thuật toán thời gian đa



Hình 3.4: Chuyển thể hiện từ β-MTO đến 0-1 Knapsack

thức để kiểm tra G_m có phải là lời giải chấp nhận được của β-MTO hay không? Điều này kéo theo β-MTO là bài toán thuộc lớp NP.

Để chứng minh MTO là bài toán NP-Khó, ta tiến hành làm giảm (reduce) từ một bài toán NP-đầy đủ đã biết, ở đây ta chọn bài toán 0-1 Knapsack.

Bài toán 0-1 Knapsack: Bài toán này phiên bản quyết định được phát biểu dưới dạng 0-1 như sau: Cho $2n+2$ số nguyên dương: $S, K, s_1, s_2, .., s_n,\ c_1, c_2, .., c_n$. Có tồn tại hay không một dãy $\{x_1, x_2, .., x_n\}, x_i \in \{0, 1\}$ sao cho: $\sum_{i=1}^{n} s_i x_i \leq S$ và $\sum_{i=1}^{n} c_i x_i \geq K$?

Thuật toán chuyển đổi thể hiện từ 0-1 Knapsack sang MTO:

Cho $(S, K, s_1, s_2, .., s_n, c_1, c_2, .., c_n)$ là một thể hiện của bài toán 0-1 Knapsack, ta xây dựng đồ thị đồ thị (G^{sc}, G_m, β, Z) như sau:

- Số đỉnh của đồ thị là $n + \sum_{i=1}^{n} s_i$
- Đầu tiên, tạo U gồm n đỉnh có độ an toàn $f(u_i) = 0, u_i \in U$.
- Với mỗi đỉnh gốc u_i ta dựng một *đường đi* p_i gồm có s_i+1 đỉnh. Đỉnh đầu tiên của đường đi là u_i, $s_i - 1$ đỉnh tiếp theo được nối tiếp với nhau có $f(u) = 0$, đỉnh cuối cùng có $f(u_{s_i+1}) = c_i$.
- Đặt $\delta = [\beta.|V^{sc}|] = S + n$ và $Z = K$, trong đó $[x]$ là số nguyên lớn nhất không vượt quá x.

Ta thấy rằng phép xây dựng dữ liệu từ bài toán 0-1 Knapsack sang bài toán MTO được thực hiện trong thời gian đa thức theo n.

Phần thuận: *Nếu bài toán β-MTO có lời giải thì bài toán 0-1 Knapsack cũng có lời giải tương ứng.*

Giả sử bài toán tìm thấy một đồ thị con $G_m = (V_m, E_m)$ của G^{sc} thỏa mãn yêu cầu, tức là: $U \in V_m$ và mỗi đỉnh $v \in V_m$ đều liên thông với ít nhất một đỉnh $u \in U$

sao cho $V \leq \beta.|V^{sc}|$ và $H(G_m) \geq Z$. Do mỗi một đường đi p_i chỉ có một đỉnh cuối cùng (đỉnh thứ $s_i + 1$) độ an toàn $f(.)$ khác 0 là c_i, nên $H(G_m)$ sẽ bằng tổng nhãn của một số đỉnh này, tức là: $H(G_m) = \sum_{i \in I} c_i$ trong đó I là tập chỉ số của các đỉnh có giá trị hàm f là c_i được chọn, do đó: $\sum_{i \in I} c_i \geq Z = K$.

Do tính chất của G_m nên nếu đỉnh có nhãn là c_i được chọn thì tất cả các đỉnh trên đường đi p_i phải được chọn. Do đó tổng số đỉnh trên các đường đi được chọn và số đỉnh gốc là: $\sum_{i \in I} s_i + n$ (vì chúng ta luôn phải chọn các đỉnh gốc và số đỉnh gốc ở đây là n). Số đỉnh này luôn nhỏ hơn hoặc số đỉnh của đồ thị G_m vì G_m có thể có những đỉnh khác có giá trị hàm f bằng 0. Do đó: $\sum_{i \in I} s_i + n \leq = \delta = S + n$, hay $\sum_{i \in I} s_i \leq S$. Vậy bài toán Knapsack được thỏa mãn với lời giải là tập chỉ số I.

Phần nghịch: *Nếu bài toán 0-1 Knapsack có lời giải thì bài toán β-MTO cũng có lời giải tương ứng.*

Giả sử rằng bài toán Knapsack được thỏa mãn, và I là tập chỉ số được lựa chọn trong bài toán Knapsack tức là: $\sum_{i \in I} s_i \leq S, \sum_{i \in I} c_i \geq K$.

Trong đồ thị G^{SC} được xây dựng ở trên ta chọn đồ thị G_m bao gồm các đường đi p_i với $i \in I$. Số đỉnh của đồ thị G_m chính là số đỉnh của các đường được chọn và số đỉnh gốc: $\sum_{i \in I} s_i + n \leq S + n = \delta$ và $H(G) = \sum_{i \in I} c_i \geq K = Z$. Vậy MTO cũng được thỏa mãn.

Định lý được chứng minh hoàn toàn!

3.5.3 Thuật toán tham lam GA

Do β-MTO là bài toán NP-Đầy đủ, do đó không tồn tại một thuật toán có thời gian chạy là đa thức cho bài toán này (với giải thuyết $P \neq NP$).

Trong mục này, luân văn đưa ra một thuật toán tham lam *Greedy Algorithm -GA* tìm kiếm nhanh lời giải dựa trên ý tưởng cập nhật lời giải qua từng bằng cách thêm vào các đỉnh có độ an toàn toàn $f(.)$ lớn nhất.

Thuật toán này sẽ cập nhập lời giải của bài toán từng bước bằng cách thêm đỉnh $v \in V^{sc}$ có độ an toàn $f(u)$ cao nhất vào lời giải ở mỗi bước. Tiếp tục lặp lại quá trình này cho đến khi trước khi số đỉnh của lời giải không thỏa mãn yêu cầu, tức là lớn hơn $\beta.|V^{sc}|$.

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 $|V^{sc}| = n$.*

Chứng minh. Vòng lặp while (từ dòng 3 đến 13) mất thời gian tính toán tối đa

Algorithm 2: 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
```

là $[\beta.n]$. Vòng lặp foreach (từ dòng 5 đến dòng 10) cần $|V^{sc}| - |V_m| \leq n$ phép tính. Theo quy tắc nhân, độ phức tạp của thuật toán là $\mathcal{O}(\beta.n^2)$

Do $\beta \in (0, 1)$ nên trong trường hợp β nhỏ rất nhỏ thuật toán này có thể coi thuật toán này có độ phức tạp tuyến tính. Trong trường hợp này thuật toán đảm bảo tìm kiếm lời giải một cách nhanh chóng nhưng đảm bảo hàm mục tiêu gần với lời giải tối ưu.

Chương 4

THỰC NGHIỆM

4.1 Mục đích thực nghiệm

Trong phần này, luận văn trình kết quả thực nghiệm nhằm đánh giá hiệu quả của giải pháp phòng ngừa xâm nhập được đề xuất. Nội dung của thực nghiệm bao gồm:

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

Dữ liệu được tiến hành thực nghiêm bao gồm dữ liệu của hai mạng xã hội Flickr và BlogCatalog. Đây là các mạng xã hội phổ biến có tính chất cộng đồng và nhóm cộng đồng và tổ chức.

- Flickr: Là mạng xã hội với chức năng chính là duy trì kết nối giữa người dùng, lưu trữ và chia sẻ hình ảnh và duy trì cộng đồng trực tuyến. Dữ liệu của mạng xã hội này được Tang [61] thu thập thiết lập chế độ ẩn danh gồm: $80,513$ người dùng và $5,899,882$ liên kết bạn bè. Trong đó có 195 nhóm người dùng đại tham gia và cùng một tổ chức hoặc cùng sở thích. Trong dữ liệu này, luận văn chọn ra hai nhóm người dùng là U_1 và U_2 có số người dùng tương ứng là 101 và 895.
- BlogCatalog: Là mạng xã hội kết nối các blogger trên toàn thế giới và gần như hầu hết blogger đều tham gia và mạng này để quảng bá cho blog của

mình. Dữ liệu về mạng này được Tang [60] thu thập gồm: 10,312 người dùng và 333, 983, trong đó có 39 nhóm, tổ chức người dùng. Trong dữ liệu này, luận văn chọn ra hai tổ chức là U_3 và U_4 có số người dùng tương ứng là.

Các bộ dữ liệu tiến hành thực nghiệm được biểu diễn dưới dạng đồ một thị vô hướng không có trọng số.

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

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

Để đánh giá hiệu quả của lời giải của bài toán MTO, trong việc phòng ngừa sự xâm nhập, luận văn mô phỏng tấn công của Socialbot tới người dùng cụ thể trong tổ chức bằng phương pháp trong [4] sau đó đưa ra tỷ lệ thành công số bạn chung của người dùng đích chấp nhận yêu cầu kết bạn.

Thực nghiệm được tiến hành với dữ liệu mạng quy mô lớn, do đó các chương trình được tiến hành trên máy tính có tốc độ tính toán để đảm bảo hiệu xuất và thời gian chạy thực nghiệm. Cụ thể, cấu hình máy tính như sau: Chipset: Intel (R) 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 3 [4]. Do việc xây dựng các hoạt động của Socialbot [4] trên mạng xã hội thực đòi hỏi cần nhiều thời gian và quy trình phức tạp. Do đó, luận văn này chỉ mô phỏng lại sự tấn công của Socialbot trên dữ liệu về mạng xã hội. Các kết quả này vẫn đảm bảo tính khách quan của kết quả tấn công và. Thứ nhất, do việc tấn công sử dụng thuật toán trên tương tự với phương pháp trong [4, 5, 6]. Thứ hai, dữ liệu mạng xã hội là dữ liệu khách quan, đồng nhất với mạng xã hội thực ở tại thời điểm thu thập. Thứ ba, sử dụng thống kê về kết quả tấn

công trong [4] để đưa ra các xác suất phù hợp. Việc tạo ra Socialbots được giả lập bằng cách tạo ra một đỉnh mới trong mạng và tạo các liên kết (cạnh) khi kết bạn thành công.

Algorithm 3: 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

Các thủ tục và các biến trong phương pháp này được mô tả như sau:

- $OrgPublicGraph$: 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.

Để bắt đầu tấn công xâm nhập, Socialbots S lấy dữ liệu về mạng xã hội chứa các người dùng trong tổ chức O. Sau đó, S chọn ra 10 người dùng trong tổ chức O một cách ngẫu nhiên. Tiếp theo, S tìm bạn của người dùng đích sau đó gửi yêu cầu kết bạn đối với tất cả người dùng này. Cuối cùng S gửi yêu cầu kết bạn với người dùng đích trong tổ chức.

Luận văn đưa ra một xác xuất chấp nhận kết bạn của Socialbot S đối với mỗi người dùng là: p_{accept}. Sử dụng phương pháp thống kê kết quả trong [4], ta thu được kết quả: $p_{accept} = 0.325$.
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

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. Ta thấy rằng đối với 4 tổ chức, kết quả này giao động trong khoảng [34.04 ; 39.22], trong đó thấp nhất là 34.04 đối với tổ chức U_2, cao nhất là 39.02 đối với tổ chức U_3. So sánh với tỷ lệ 37.09% và 33.33% đối với hai tổ chức O_1 và O_2 [4], tỷ lệ mô phỏng tấn công đảm bảo số lượng bạn chung đồng ý kế bạn của kẻ tấn công là tương đồng.

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

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

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

Đối với mỗi tổ chức Socialbot giả lập đó có một số lượng bạn chung nhất định với người dùng đích trong tổ chức. 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

Dữ liệu tiến hành thí nghiệm được biểu diễn dưới dạng đồ thị vô hướng không có trọng số. Để thu được trọng số từ dữ liệu, tác giả sử dụng phương pháp lấy trọng số trong [38]. Theo đó, trọng số của mỗi cạnh $(u, v) \in E$ được tính 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	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

Đối với mỗi tổ chức, thực nghiệm tiến hành xây dựng các cộng đồng an toàn tương ứng. Các tham số cần thiết lập cho mỗi tổ chức gồm gồm: Số người dùng trung gian T để tính độ đo Φ, số bước lặp k và ngưỡng an toàn θ.

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: Thiết lập tham số cho mỗi tổ chức

Tham số và kết quả xây dựng Cộng đồng an toàn cho mỗi tổ chức được trình bảy trong bảng 4.7.

Các tham số trên được đưa ra dựa trên kết quả thống kê đối với một phần dữ liệu nhỏ của mỗi mạng. Tham số T phụ thuộc vào cấu trúc mạng là số bậc trung bình của mạng. Trong chương 3 ta đã nhận định rằng, độ phức tạp của tính độ đo tăng khi số bậc càng lớn. Do đó, trong khuôn khổ thực nghiệm, luận văn chọn $T = \{1, 2\}$.

Do dữ liệu mạng xã hội lớn nên việc tính toán trong việc xây dựng Cộng đồng an toàn là rất lớn đối với mỗi tổ chức là rất lớn. Chi phí của việc tính toán này hầu hết nằm ở việc tính toán độ đo Φ. Đối với các tổ chức có số lượng người dùng nhỏ U_1 và U_3, thời gian chạy là khoảng gần 12h. Đối với tổ chức có số lượng người dùng lớn hơn là U_2 và U_4 thời gian chạy gần 24h.

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.

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

4.5 Kết luận và nhận xét

Đối với các tổ chức có số lượng người dùng nhỏ là U_1 và U_3 với các giá trị tương ứng là $\beta \leq 0.70$ và $\beta \leq 0.80$ vùng β-MTO vẫn cách ly được S_1 và S_3 với các giá trị lớn hơn không cách ly được.

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

Đối với tổ chức có số lượng người dùng lớn hơn như: U_2 và U_4 vùng β-MTO có thể cách ly được S_2 và S_4 với các giá trị β cao ($\beta = 0.85$), chỉ với $\beta = 0.9$ không cách ly được.

Kết quả này có thể do hai nguyên nhân sau: Thứ nhất, thuật toán tham lam chỉ chọn được giá trị tối ưu địa phương. Thứ hai, số lượng đỉnh trong tập U_3 nhỏ so với U_1 và U_4 do đó S_3 và S_4 đạt được độ an toàn cao đối với U_2 và U_4

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.

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 Social 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.