SybilShield: Một doanh nghiệp hỗ trợ mạng lưới xã hội - Đặt nền móng bảo vệ đa cộng đồng trước Sybil

Tóm lược – Thiếu trung tâm tin cậy, các hệ thống phân phối đã và đang nhận phải nhiều mối đe dọa an ninh nghiêm trọng từ sự tấn công của Sybil, nơi một kẻ thù giả mạo danh tính của nhiều hơn một node và cố gắng để kiểm soát hệ thống. Bằng cách sử dụng các mối quan hệ tin tưởng thực tế giữa người sử dụng, đề án bảo vệ dựa trên mạng xã hội đã được đề xuất để giảm thiểu tác động của các cuộc tấn công mạng – Sybil attack. Những giải pháp chủ yếu được xây dựng trên giả định rằng đồ thị mạng xã hội có thể được phân chia thành hai khu vực có liên kết lỏng lẻo - một kết nối chặt chẽ khu vực phi Sybil và một khu vực có sự tấn công của Sybil. Mặc dù một giả định như thế có thể giữ trong sự sắp đặt nhất định, các nghiên cứu đã chỉ ra rằng các kết nối xã hội thực thế giới có xu hướng phân chia người sử dụng vào nhiều thế giới nhỏ liên kết với nhau thay vì một khu vực rộng lớn kết nối thống nhất duy nhất. Với thực tế này, khả năng áp dụng của các chương trình hiện có sẽ bị suy yếu đáng kể, chưa đủ khả năng để phân biệt ngườ sử dụng trong vùng có Sybil với những người khác trong các vùng phi Sybil nhỏ bé.

Bài báo đã chỉ ra vấn đề này và giới thiệu SybilShield - giao thức đầu tiên bảo vệ và chống lại cuộc tấn công Sybil bằng việc sử dụng cấu trúc mạng lưới xã hội trong thế giới thực. Chương trình của chúng tôi thúc đẩy các nhà xã hội học tin rằng số cắt cạnh giữa một cộng đồng phi Sybil và một cộng đồng Sybil, đại diện cho các mối quan hệ tin tưởng con người thành lập, là nhỏ hơn nhiều so với các cộng đồng phi Sybil. Với sự giúp đỡ của các node đại lý, SybilShield làm giảm đáng kể tỷ lệ nhận diện nhầm của người dùng phi Sybils giữa vô số cộng đồng, trong khi xác định hiệu quả các điểm có Sybil. Kết quả phân tích chứng minh tính ưu việt của SybilShield. thí nghiệm của chúng tôi trên một đồ thị mạng xã hội thế giới thực với 100.000 node cũng xác nhận tính hiệu quả của SybilShield.

I.Phần giới thiệu

“Sybil attack” [1] là một cuộc tấn công nổi tiếng trong hệ thống phân phối, nơi mà một người sử dụng độc hại tạo ra nhiều tính trạng giống nhau không có thật (hoặc các node Sybil) như chúng muốn, giả dạng như những thực thể khác nhau, và sau đó bắt đầu các cuộc tấn công thông qua những tính trạng giả, làm cho bản thân không thể lần ra . Với các “node Syril” gồm một phần lớn các node còn lại trong hệ thống, các đối thủ có khả năng kiểm soát cả hệ thống. Ví dụ về các “Sybil attack” đã được quan sát thấy trong thế giới thực, bao gồm các hành vi thông đồng trong các ưu đãi dựa trên chia sẻ tập tin mạng Maze trong mạng ngang hàng [2], thao tác các cuộc thăm dò bằng cách bỏ phiếu nhiều lần với nhiều tính trạng [3], [4], gây rối loạn cấp bậc của nội dung hoặc các trang trên YouTube [5] và [6] Google, và những trang khác. Các giải pháp hiện cho các “Sybil attack”có thể được thường chia thành phòng thủ tập trung phòng thủ và phi tập trung. Với một cơ quan tin cậy, hệ thống phòng thủ tập trung xác nhận danh tính của thông tin duy nhất được cấp cho khách hàng. Trong khi công việc trước đây [1], [3], [7] - [9] đã chỉ ra rằng nó là tốn kém và không thực tế để triển khai các giải pháp tập trung vào các hệ thống phân phối, các nhà nghiên cứu lần lượt khám phá những phương pháp phòng thủ phi tập trung khó khăn hơn. Tuy nhiên, vẫn chưa có giải pháp toàn cầu mà hoàn toàn loại bỏ các mối đe dọa của “Sybil attack” . Tất cả các giải pháp hiện nay chỉ để giảm thiểu tác động của “Sybil attack”. Gần đây, đã có một sự quan tâm ngày càng tăng trong lợi dụng đặc điểm chung của các mạng xã hội để ngăn chặn “Sybil attack” [7], [9] - [12]. Tại trung tâm của các chương trình dựa trên mạng xã hội nằm trong ý tưởng cơ bản của các node phân vùng trong mạng thành hai khu vực - một khu vực phi Sybil và một khu vực Sybil - bằng cách cân tin tưởng trưng bày trong đồ thị xã hội với sự giúp đỡ của các nền tảng cơ bản [8]. Tuy nhiên, [13], [14] nói rằng một đồ thị mạng xã hội thực sự có thể được chia thành nhiều cộng đồng khác nhau. Vì vậy, nó là không phù hợp cho công việc trước khi xây dựng đề án trên cơ sở giả định rằng ngoại trừ các khu vực Sybil chỉ có một cộng đồng lớn chặt chẽ cho tất cả những người sử dụng chân thật. Hơn nữa, trong những phòng thủ “Sybil attack” dựa trên mạng xã hội, Sybil của được phát hiện theo giả định thuật toán rằng số lượng các cuộc tấn công cạnh giữa Sybil và node phi Sybil bị hạn chế [15]. Tuy nhiên, Viswanath et al. trong [8] cho thấy rằng nó cũng có thể cho phi Sybil phụ đồ thị để có một cắt thưa thớt giữa mỗi khác, bất kể các cạnh đa hợp gián tiếp giữa chúng, trong đó tiếp tục khẳng định cấu trúc đa cộng đồng của mạng xã hội. Trong một mạng xã hội như vậy, nó là một thách thức để phân biệt giữa người sử dụng phi Sybil và Sybil vì mỗi người sử dụng các hệ thống phân phối không có kiến thức về cấu trúc liên kết của toàn bộ mạng lưới. Kết quả là, các thông tin cho một người sử dụng để quyết định danh tính của một người dùng khác trong mạng bị hạn chế. Do đó, các node trong một cộng đồng có thể nhầm nút-Sybil không trong một cộng đồng khác cho Sybils với xác suất cao do kết nối trực tiếp giới hạn giữa hai cộng đồng, mà còn tạo ra khó khăn trong việc phân biệt đối xử Sybils từ phi Sybils thành công. Kết quả là, các thông tin cho một người sử dụng để quyết định danh tính của một người dùng khác trong mạng bị hạn chế. Node Sybil có thể dễ dàng ngụy trang mình như là một cộng đồng phi Sybil bằng cách thiết lập một số lượng nhỏ các liên kết mục tiêu cẩn thận để cộng đồng có chứa các node tin cậy, do đó gây nhầm lẫn cho việc phát hiện Sybil. Bị thúc đẩy bởi các vấn đề trên, chúng tôi giới thiệu SybilShield, một giao thức phòng ngự Sybil mới phát hiện Sybil và hạn chế các tác hại “Sybil attack” trong bối cảnh của đồ thị xã hội đa cộng đồng. Thiết kế của chúng tôi thúc đẩy các thuộc tính cấu trúc sau đây của đồ thị mạng xã hội: các node trong cộng đồng Sybil thưa thớt kết nối với tất cả các cộng đồng phi Sybil do thiếu sự tin tưởng; cộng đồng thật là chặt chẽ liên kết nói chung kể từ khi người sử dụng trung thực là phần lớn trong hệ thống, nhưng liên kết nối của họ có thể được nắm bắt. Trong thời gian xác minh, lá chắn Syril đầu tiên biến đổi các “quá trình đi bộ ngẫu nhiên” trong đồ thị và sử dụng node giao thông giữa các lớp như vậy để hạn chế số lượng đặc tính Sybil được chấp nhận. Nếu người cung cấp không được chấp nhận ở bước này, SybilShiled tận dụng lợi thế do các đại lý áp dụng, ví dụ, các node chọn từ cộng đồng không bao gồm những người bao gồm người xác minh và người cung cấp, để xác nhận liệu nhận dạng bị các người cung cấp, người yêu cầu là hợp pháp, là phi Sybil hay không. Những đóng góp chính của công việc của chúng tôi bao gồm: (1) Chúng tôi trình bày các giải pháp đầu tiên do “Sybil attack” trong các mạng xã hội đa cộng đồng, trong khi các chương trình bảo vệ mạng xã hội khác dựa trên mạng lưới Sybil giả định không đúng rằng đồ thị mạng xã hội cơ bản chỉ bao gồm một khu vực phi Sybil và một khu vực Sybil; (2) Chúng tôi đánh giá SybilShield bằng cách phân tích và thí nghiệm trên các mẫu từ mạng xã hội MySpace, cho thấy rằng chương trình của chúng tôi có thể phát hiện Sybils hiệu quả. Bên cạnh đó, trong SybilShield tỷ lệ nhận diện nhầm, đại diện cho tỷ lệ phần trăm của các “honest node” bị nhầm là Sybils, giảm đáng kể so với việc áp dụng trước đó giải pháp cho các mạng xã hội đa cộng đồng, giúp cải thiện độ chính xác.

Phần còn lại của bài viết này được tổ chức như sau. Phần II đánh giá các công việc liên quan. Phần III trình bày các mô hình và giả định. Tổng quan về công việc sơ bộ được đưa ra trong phần IV. Chúng tôi mô tả thiết kế của SybilShield chi tiết trong Phần V. Mục VI cho thấy hiệu quả của SybilShield, phân tích và thí nghiệm lý thuyết, tiếp theo là kết luận nhận xét tại Mục VII.

II. CÔNG VIỆC CÓ LIÊN QUAN

Bảo vệ chống lại các “Sybil attack” đã thu hút sự quan tâm liên tục kể từ khi “Sybil attack” đầu tiên được xác định bởi Douceur [1]. Hiện các chương trình phòng thủ Sybil có thể được phân thành các loại sau [3]: đáng tin cậy chứng nhận quyền trung ương, kiểm tra tài nguyên, và tận dụng mạng tin tưởng. Theo [1], chứng chỉ tin cậy của chính quyền trung ương là giải pháp phổ biến nhất để chống “Sybil attack”, và cũng là phương pháp duy nhất để triệt để quét sạch những ảnh hưởng tiêu cực của nó. Tuy nhiên, trong hệ thống phần tử quy mô lớn, nó là không thực tế cho các cơ quan trung ương để từng đặc tính cho tất cả các thực thể. Ngoài ra, nếu các cơ quan trung ương trở thành mục tiêu cho những kẻ tấn công và thất bại, toàn bộ hệ thống sẽ bị thiệt hại.

Kiểm tra tài nguyên giải pháp dựa trên [16], [17] giải quyết “Sybil attack” bằng cách giả sử rằng một kẻ tấn công chỉ có thể sở hữu nguồn tài nguyên hữu hạn và có thể tạo ra một vài node Sybil với hệ thống thiết kế một cách thích hợp. Nhưng [18] cho thấy rằng trong một số hệ thống, “Sybil attack” có thể được thực hiện ngay cả với vài node Sybil. Gần đây, đã có một số lượng đáng kể của việc sử dụng sự tin tưởng tiềm ẩn trong các đồ thị mạng xã hội để nâng cao sức đề kháng chống lại các cuộc tấn công Sybil. Các đề xuất trên cơ sở của các mạng xã hội bao gồm SybilGuard [12], SybilLimit [7], SybilInfer [10], SumUp [11], Wha nau [9], SybilDefender [19], vv. Họ khám phá sự xáo trộn nhanh chóng về nguồn cung của đồ thị xã hội, và chỉ ra rằng một bước đi ngẫu nhiên trên một đồ thị tiếp cận phân phối văn phòng phẩm một cách nhanh chóng. Thủ tục xác nhận của SybilGuard,SybilLimit và SybilDefender về cơ bản dựa trên quãng đường ngẫu nhiên và va chạm của họ giữa các node trung thực. Trong khi SybilLimit tối ưu hóa các giới hạn cho việc chấp nhận các node Sybil trong SybilGuard từ O (pn) đến O (log n), SybilDefender đơn đã được xác định tỷ lệ Sybil của phương pháp tiếp cận lý thuyết ràng buộc. Tuy nhiên, SybilDefender giả định người quản trị biết câú trúc phần tử của mạng xã hội, trong đó cho thấy nó là một cơ chế tập trung và không áp dụng cho các hệ thống phân phối. SybilInfer xác định người sử dụng trong một mạng xã hội là người sử dụng trung thực hoặc Sybils theo xác suất xác định bằng suy luận Bayesian. SumUp là một hệ thống bầu chọn nội dung điều trị các node có phiếu được chấp nhận như là phi Sybils, bằng kỹ thuật tập hợp lưu lượng phiếu bầu thích ứng. Nau Wha, một giao thức định tuyến DHT Sybil bằng chứng, kết hợp “di chuyển ngẫu nhiên” với ý tưởng định danh lớp.

Trong [8], Viswanath et al. thấy rằng các chương trình quốc phòng Sybil có nền tảng mạng lưới xã hội cơ bản là các thuật toán đồ thị phân vùng, xử lý các mạng xã hội cơ bản như một đồ thị. Nghiên cứu này cũng cho thấy rằng những vệ Sybil rất nhạy cảm với cấu trúc cộng đồng liên quan đến thời gian trộn trong các mạng xã hội. Tuy nhiên, khả năng phát hiện Sybils sẽ bị suy yếu nếu nhiều cộng đồng liên kết với nhau tạo thành các khu vực phi Sybil trong đồ thị mạng xã hội thực sự. Mohaisen et al. trong [15] mô hình tin cậy như một tham số trong các hình thức khác nhau của các bước đi ngẫu nhiên thay đổi, và kiểm tra tác động đến hiệu suất của phòng thủ Sybil tương ứng. Nhưng làm thế nào để xác định sự tin tưởng và mức độ tin cậy không được chỉ định.

III. Mô hình và giả thuyết

1. Mẫu hệ thống

Chúng tôi cho rằng trong hệ thống có sử dụng n “honest user” thể hiện con người thật, và mỗi người trong số họ có chính xác một đặc tính trung thực, được ký hiệu là một node trung thực trong đồ thị mạng xã hội. Khác với phòng thủ Sybil có nền móng mạng lưới xã hội trước đây, chúng tôi giả định rằng một đồ thị mạng xã hội bao gồm các cộng đồng nhiều kích cỡ khác nhau. Để xác minh giả định của chúng tôi, chúng tôi tiến hành thí nghiệm trên một đồ thị mẫu 100,000- nút từ MySpace [20] bằng cách áp dụng phương pháp Louvain [21] cho phát hiện của cộng đồng. Kết quả thử nghiệm của chúng tôi cho thấy rằng những 100.000 nút có thể được chia thành 19 cộng đồng, với kích thước nhỏ nhất của 12 và kích thước lớn nhất của 33.877, liên kết với nhau bởi hang chục đến hàng trăm của các cạnh. Kết quả này xác nhận giả thiết của chúng tôi và cũng là phù hợp với quan sát thực hiện trong công việc trước đây [21], [22].

Nhân vật. 1 mô tả các cấu trúc liên kết mạng xã hội trong đó các “honest node” soạn nhiều nhóm các kích cỡ khác nhau, đó là sự liên kết với nhau và gọi là “honest communities” hoặc “ honest regions”. Tương ứng, cộng đồng được hình thành bởi các “node Sybil” được gọi là “Sybil communities” hoặc “ Syril regions”. Trong khi các “honest node” luôn tuân thủ các quy tắc giao thức, các “node Syril” có thể cư xử ngẫu nhiên hoặc thậm chí theo cách ngược lại.