IV. Mở đầu.

Sylby Guard là người đầu tiên sử dụng mạng xã hội để bảo vệ sự tấn công của Sylbi trong hệ thống được phân phối, cái mà dẫn đầu trong việc khai thác những tài nguyên fast mixing cho phát hiện của Sylbi. Sylbi Guard cho ra hai abor đảm: Số nhóm Sykbi đến g là hữu hạn; the effective size of Sybil groups are bounded below w, i.e. a node will accept at most g · w Sybil nodes.

Dựa trên cùng giả thuyết và trực giác nói ở trên, Sylbi sử dụng những cách bất kì thử lại được và sự tương giao để phân biệt những điểm giao thuộc Sylbi và không thuộc Sylbi. Nếu lối đi từ một điểm giao đúng giao với lối đi từ một đối tượng khác, đối tượng đó được gắn mác là không thuộc Sylbi. Lưu ý rằng mỗi điểm giao tạo ra một bảng lộ trình liên tục cái mà trong đó mỗi cạnh vào hướng tới một cạnh ra theo một sự đo vẽ riêng.

Cụ thể là, để quyết định một nút giao S có chất lượng tốt không, nút thử lại V tạo ra một w-hop lối đi bất kì, lối đi đó chính là quyết định luật được hình thành dựa theo những lối vào đã lưu của những nút giao w cố định. Trong khi đó, S bắt đầu với một lối đi w-hop bất kì. V chấp nhận S nếu hai đường giao nhau. Chú ý rằng số nút giao được chấp nhận dưới giao thức Sylbi Guard sẽ tăng với sự tăng lên của w. Từ một quan điểm khác, w phải đủ lớn để đảm bảo các giao điểm được tạo ra có khả năng lớn và được hình thành một cách riêng biệt từ những đường bất kì xuất phát từ V và S. Cụ thể hơn là, w sẽ có lợi khi ở trong một khoảng hợp lí, không quá to mà cũng không quá nhỏ. Như Yu đã phân tích, với mận xã hội với thời gian không cố định, với nghịch lí ngày sinh được tổng quát, hai nút giao không thuộc Sylbi với những mẫu √ n từ vùng không thuộc Sylbi có khả năng cao là sẽ có một giao điểm. Để thiết kế độ dài phù hợp cho những đường bất kì, Sylbi ước lượng bằng cách lấy các mẫu từ vùng không thuộc Sylbi của những nút n và bằng việc dùng những lối đi bất kì O( √ n log n).

Trong khi cung cấp một hướng đi đầy hứa hẹn cho những bảo vệ của Sylbi, Sylbi đã chịu đựng nhiều giới hạn. Như trên, việc đặt nền móng cho cấu trúc mạng xã hội của Sylbi rất khó giải quyết. Trong mạng xã hội thực nơi bao gồm ít đối thủ lớn và nhiều những cộng đồng vừa và nhỏ, khả năng của Sylbi bị giảm đi. Lí do là, một điểm để thử lại có thể dễ dàng đánh dấu điểm nghi vấn có chất lượng cao s vì Sylby nhầm lẫn khi phân biệt cộng đồng Sylby và cộng đồng không thuộc Sylbi, việc này làm tăng tỉ lệ tích cực sai. Vis cũng tuyên bố vấn đề này trong [8] bằng những dự án có sẵn về những bảo vệ của Sylbi 7, 10-12, qua những cấu trúc cộng đồng khác nhau. Nhưng phần 8 không đưa ra giải pháp cho vấn đề này. Bằng việc đề cập tới SylbiGuard, giao thức của chúng ta về SylbiShield đạt được sự chính xác cao với tỉ lệ tích cực sai tương đối thấp giữa nhiều cộng đồng trong những mạng xã hội thực.

V. Giao thức SylbilShield

A. Tống quát.

SylbiShield bảo vệ mạng xã hội thế giới thực với cấu trúc đa cộng đồng chống lại cuộc tấn công của Sybil. Với nút giao xác thực v để quyết định danh tính của nút giao nghi vấn S, cả V và S đều trước tiên thể hiện dạng được sửa đổi của đường bất kì. V chấp nhận S nếu đường bất kì của chúng có những điểm giao nhau. Nêu không thì V từ chối thừa nhận S. Kể cả khi S bị từ chối bới sự kiểm chúng của một đường bất kì, nó vẫn không thể đảm bảo rằng S phải là một nốt thuộc Sybil. Để tránh gắn nhãn nhầm những nghi vấn xác thực là Sybil, SybilShield sử dụng các tác nhân của V để kiểm tra lại danh tính của S trong bước thứ hai, cái này được gọi là bước thử tác nhân. Trong bước thử bằng tác nhân, các tác nhân được tìm kiếm cùng với các cạnh của V, được lựa chọn kĩ càng để cho ra ngoài khoảng của V. Tác nhân hợp lệ thể hiện những đường bất kì để xem liệu các giao điểm có tồn tại giữa các đường bất kì của S. S nhận được các bình chọn từ các tác nhân với các giao điểm. A ngưỡng t là một bộ cho V để quyết định việc chấp nhận S nếu lượng tác nhân bình chọn cho S không nhỏ hơn i. Ký hiệu của tờ này đã 1 phần được định nghĩa trong bảng I.

B. Random Route.

Đường bất kì đã được đưa ra trong phần 12. Chúng ta đề cập đến nó và xây dựng bước đầu của giao thức, như được thể hiện trong Algorithm 1. Với những đường bất kì trong cộng đồng xác thực, V chấp nhận S nếu các đường bất kì của chúng có ít nhất một giao điểm. Cho mỗi bước nhảy dọc đường bất kì, bước nhảy tiếp theo của nó được lựa chọn một cách nghiêm ngặt tùy theo bảng lộ trình bất kì đã được tính toán trước của bước nhảy hiện thời hơn là chọn 1 trong số cái ở gần một cách bất kì và đồng đều. Các bảng lộ trình được tính toán bằng sự hoán vị bát kì, chỉ ra phép phản xạ một đối một từ những cạnh vào đến những cạnh ra. Vì mạng xã hội được thừa nhận là tĩnh, không có điểm nút hay cạnh được them vào hay bỏ ra khỏi biểu đồ. Thế nên, đồ thị của mội điểm sẽ được giữ nguyên và không cần phải cập nhật.

Chúng ta chú ý rằng biểu đồ đã được biết để có những tài nguyên sau: tài nguyên hội tụ: nếu các đường bất kì khác nhau đi qua một nút giao nhất định qua một cạnh vào, chúng sẽ có cùng cạnh ra hướng tới bước nhảy tiếp theo.