ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

NGUYỄN LAN HƯƠNG

XÁC MINH VỊ TRÍ CHO ĐỊNH TUYẾN ĐỊA LÝ AN TOÀN TRONG CÁC MẠNG CẢM BIẾN KHÔNG DÂY

Ngành : Công nghệ thông tin
Chuyên ngành : Truyền dữ liệu và mạng máy tính
Mã số :

TÓM TẮT LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

NGƯỜI HƯỚNG DẪN KHOA HỌC: TIẾN SĨ NGUYỄN ĐẠI THỌ

Hà Nội – Năm 2016

MỞ ĐẦU

Việc biết vị trí của các nút cảm biến là rất quan trọng đối với nhiều ứng dụng như giám sát môi trường, mục tiêu tấn công, và định tuyến địa lý. Vì mạng cảm biến không dây có thể được triển khai trong môi trường thù địch, vị trí của cảm biến phải chịu các cuộc tấn công độc hại. Ví dụ, kẻ tấn công và nút cảm biến có thể thỏa hiệp để đưa thông tin vị trí sai; chúng cũng có thể làm gián đoạn tín hiệu truyền tải về khoảng cách giữa các bộ cảm biến gây nhiễu cho các phép đo đạc. Do đó, các vị trí ước tính trong quá trình định vị không phải luôn luôn đúng.

Theo những nghiên cứu trước đây đã phân loại các thuật toán xác minh vị trí vào hai loại, cụ thể là xác minh tại chỗ và xác minh khu vực. Xác minh tại chỗ là để kiểm tra xem vị trí thực sự của một cảm biến tương tự như vị trí dự kiến của nó (hoặc có lỗi rất nhỏ). Để có được kết quả mong muốn, các thuật toán xác minh tại chỗ sử dụng kiến thức triển khai các cảm biến trong khu vực hoặc sử dụng một số phần cứng chuyên dụng để xác định khoảng cách. Vì hiện tại các thuật toán xác minh thường phụ thuộc vào phần cứng khá là tốn kém, và không có sẵn trong các hệ thống cảm biến không dây chi phí thấp, nên rất cần có một thuật toán xác minh gọn nhẹ được thiết kế sao cho hiệu quả có thể thực hiện việc xác minh tại chỗ.

Bên cạnh việc xác minh tại chỗ, một số nỗ lực nghiên cứu cũng được dành cho việc thiết kế trong các thuật toán xác minh vị trí vùng. Sastry, xác định các khái niệm về xác minh trong khu vực đầu tiên [1]. Họ cũng đề xuất một giao thức được đặt tên là "*Echo*" để xác minh, nếu một bộ cảm biến bên trong một khu vực vật lý chẳng hạn như một căn phòng, một tòa nhà, hoặc thậm chí là một sân vận động thể thao. Dựa vào kết quả xác minh, nó có thể quyết định liệu phân công các cảm biến có truy cập đến một số tài nguyên trong khu vực vật lý đó không. Tuy nhiên, nó không thể được sử dụng trực tiếp cho các ứng dụng dựa trên sự xác minh khác, bởi vì vùng xác minh có thể không rõ ràng và cần phải được xác định một cách cẩn thận bằng cách phân tích chức năng của các ứng dụng. Việc xác minh như vậy làm tăng chi phí và đòi hỏi thêm những nỗ lực khi triển khai. Trong hệ thống có sử dụng một Anchor tin cậy có trang bị GPS để xử lý dữ liệu một cách tập trung, nên khi mật độ mạng dày hơn sẽ xảy ra tình trạng quá tải do dữ liệu xử lý vượt khả năng của Anchor. Vì vậy, luận văn nghiên cứu và bổ sung thêm các kịch bản tấn công để đánh

giá khả năng của các Anchor và VC. Phần trọng tâm của luận văn là áp dụng cơ chế xác minh an toàn này vào trong xác minh node bị tấn công trong thuật toán vượt biên Perimeter Forwarding và tránh đường thông qua k-đường dự phòng. Về bố cục, các phần của luận văn được tổ chức như sau:

Chương 1: Chúng tôi trình bày Tổng quan về cơ sở của đề tài: lý do chúng tôi chọn đề tài, mục tiêu cụ thể của đề tài, những vấn đề của bài toán xác minh thông tin vị trí, định tuyến an toàn và đưa ra định hướng nghiên cứu sẽ chọn.

Chương 2: Chúng tôi trình bày về các nghiên cứu Xác minh thông tin vị trí trong mạng cảm biến không dây, các giải pháp hiện có, ưu nhược điểm của các giải pháp.

Chương 3: Chúng tôi nghiên cứu các giải pháp định tuyến phục hồi dựa trên thông tin vị trí.

Chương 4: Chúng tôi trình bày phương pháp giải pháp định tuyến k đường phục hồi đưa ra các hạn chế gặp phải trong quá trình xây dựng và đánh giá kết quả đạt được khi mô phỏng lại các kịch bản tấn công cho định tuyến phục hồi an toàn với sự thay đổi các chỉ số độ tin cậy, phân tích khía cạnh an ninh của giải pháp.

Phần cuối: Tổng kết và đưa ra kết luận, những hướng nghiên cứu cần thực hiện thêm trong tương lai.

CHƯƠNG I: TỔNG QUAN VỀ CƠ SỞ CỦA ĐỀ TÀI

1.1 Mạng cảm biến không dây (WSN)

Mạng cảm biến không dây (WSN) là một công nghệ mới chỉ một tập hợp số lượng lớn các thiết bị cảm biến sử dụng liên kết không dây phân phối trong không gian tự trị nhỏ và hợp tác với nhau để giám sát, phản ứng với điều kiện môi trường. Sau đó gửi các dữ liệu thu thập được tới một trung tâm chỉ huy sử dụng các kênh không dây. Mạng cảm biến không dây thường được ứng dụng trong nhiều lĩnh vực bao gồm cả quân sự, thương mại, dân sự, công nghiệp và khoa học. Ví dụ, giám sát cảnh báo thiên tai, hỗ trợ kiểm tra sự di chuyển và các cơ chế sinh học của côn trùng hoặc các loài sinh vật nhỏ, giám sát chiến trường, trinh sát vùng và lực lượng địch, ứng dụng trong ngôi nhà thông minh …

1.1.1 Những thách thức trong WSN

WSNs không giống như các mạng khác, do thường được triển khai hoạt động để giám sát và trong môi trường thù địch hay gặp phải vì mưa, tuyết, độ ẩm và nhiệt độ cao. Khi thì sử dụng cho các ứng dụng quân sự như phát hiện bom mìn, giám sát chiến trường, hoặc theo dõi mục tiêu, điều kiện tiếp tục xấu đi. Trong môi trường hoạt động độc đáo như vậy, WSNs phải hoạt động tự chủ và do đó nó phải đối mặt với những thách thức. Một kẻ thù có thể nắm bắt và thỏa hiệp với một hay nhiều bộ cảm biến.

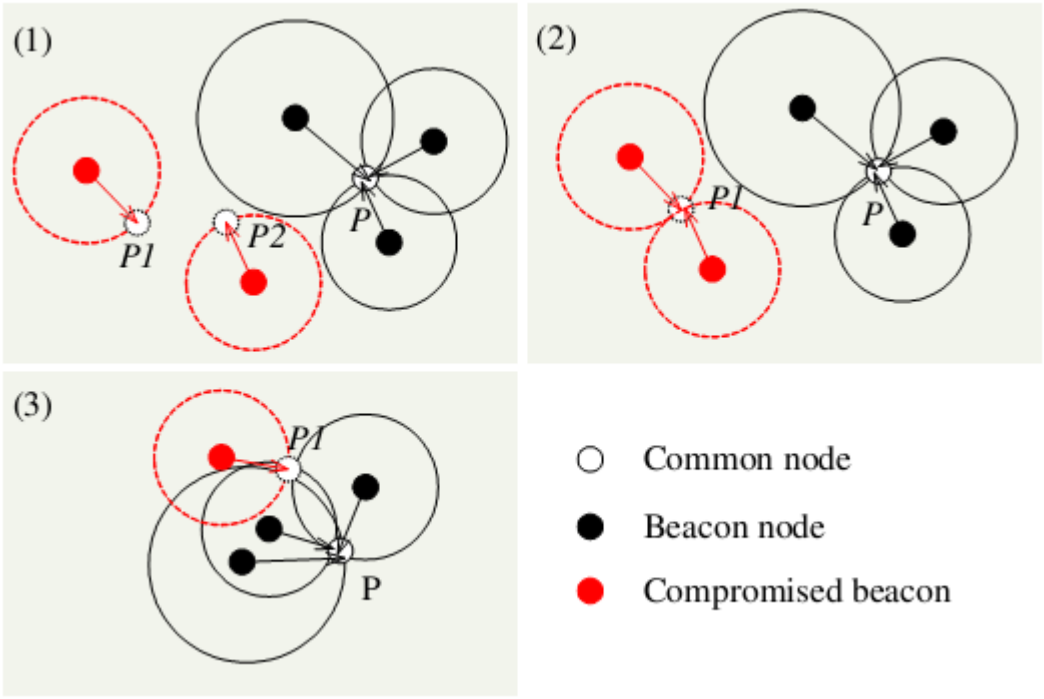
1.1.2 Vấn đề an ninh trong WSN

Các dạng tấn công

Nhiều cuộc tấn công có thể được đưa ra trong hệ thống định vị và hệ thống xác minh thông tin vị trí.

- ***Tấn công thay đổi phạm vi***: Trong cuộc tấn công này, kẻ tấn công có thể làm giảm hoặc tăng số đo phạm vi giữa các nút bất kỳ.
- ***Sự mạo danh***: Trong cuộc tấn công này, kẻ tấn công đóng vai các nút khác trong mạng.
- ***Tấn công lỗ sâu***: Trong cuộc tấn công này kẻ tấn công tạo ra các gói dữ liệu tại một vị trí trong mạng và thỏa hiệp với một nút khác sau đó chúng chuyển thông tin cho nhau thông qua một đường hầm và phát lại thông tin [2].

- ***Tấn công Sybil***: Trong cuộc tấn công này, kẻ tấn công đã thu nhiều nút, và sau đó nó có thể là nút thỏa hiệp để giả dạng như một số các nút khác tại cùng thời gian. Ví dụ, trong hệ thống định vị, một nút thỏa hiệp có thể giả dạng như một số các cảnh báo (danh tính của họ là tổn hại bởi những kẻ tấn công), và gửi thông tin sai lệch.
- ***Tấn công tham chiếu vị trí***: Trong cuộc tấn công này, kẻ tấn công có thể làm cho các đèn hiệu phát sóng các địa điểm giả, và/ hoặc có thể bóp méo khoảng cách giữa các cảnh báo và các nút thông thường (nghĩa là, có thể chứa các cuộc tấn công thay đổi phạm vi).

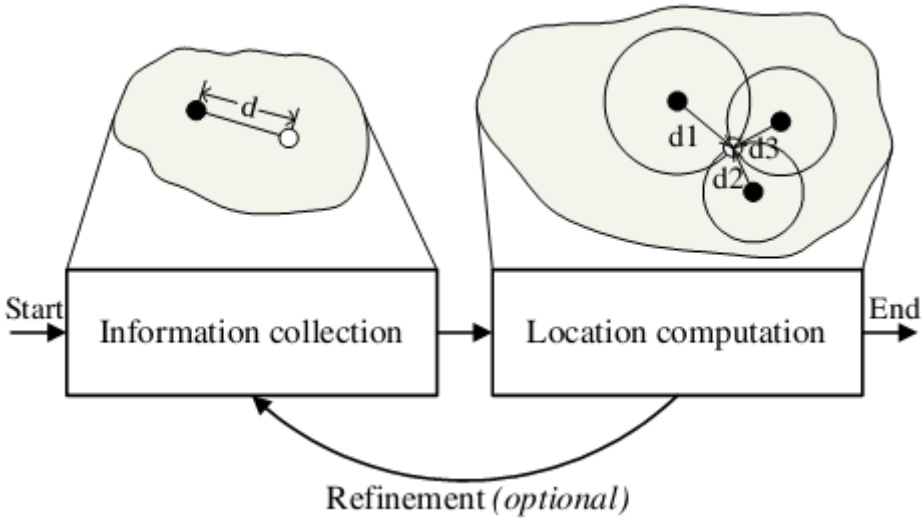


Hình 1. Ba kiểu của tấn công tham chiếu vị trí: (1) uncoordinated, (2) collusion, và (3) pollution attacks. Trong hình chỉ P là vị trí thực.

1.1.3 Những khái niệm cơ bản trong xác minh thông tin vị trí trong WSN

Sự định vị

Thông thường các mạng cảm biến có chứa hai loại nút: các nút thông thường và các nút Anchor. Các nút thông thường không biết vị trí của họ, và các nút Anchor biết vị trí của chúng (ví dụ, bằng GPS). Sau đó, quá trình định vị để ước tính các vị trí của các nút thông thường. Bình thường quá trình định vị có thể được chia thành hai bước (với một bước lọc tùy chọn), như trình bày trong hình 2:



Hình 2 Sự định vị của các nút cảm biến

Định vị an toàn

Định vị an toàn là làm cho quá trình định vị vẫn đúng khi có các cuộc tấn công. Nó có thể yêu cầu thêm phần cứng để làm thất bại các cuộc tấn công. Việc phân loại các hệ thống định vị an toàn cũng có thể thực hiện theo phân loại các hệ thống định vị chung như trên.

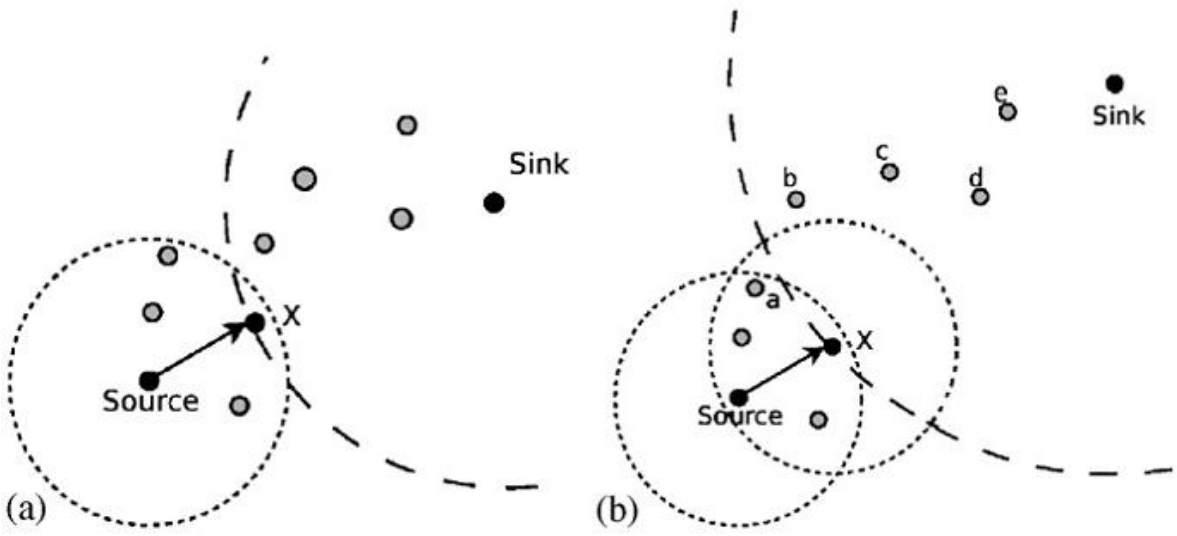
Xác minh vị trí

Khi các cơ sở hạ tầng đang quản lý mạng dựa trên sự báo cáo vị trí của cảm biến, ví dụ, xử lý dữ liệu ràng buộc với các địa điểm hoặc chứng thực dựa trên vị trí của chúng, cảm biến có thể không tin tưởng những vị trí báo cáo. Chúng ta hãy xem xét các trường hợp trong hai loại hệ thống định vị.

1.1.4 Định tuyến vị trí trong mạng cảm biến không dây

Định tuyến vị trí truyền thống (Geographic routing - GR)

GR thường bao gồm hai phần: chuyển tiếp địa lý và định tuyến bổ sung cho việc tránh khoảng trống, còn được gọi là định tuyến bề mặt hay định tuyến vành đai. Chuyển tiếp địa lý là một thuật toán định tuyến tham lam dựa trên vị trí địa lý. Đối với một nút đã cho, tất cả hàng xóm của một bước nhảy (one-Hop) gần với đích thuộc tập chuyển tiếp (FS) cho đích đó. Như đã được hiển thị trong hình 3(a), các nút chuyển tiếp một gói dữ liệu đến hàng xóm trong FS và gần đích nhất. GR là hấp dẫn vì nó chỉ đòi hỏi các nút để duy trì vị trí của các hàng xóm của chúng trong một bước nhảy. Ngoài ra, các quyết định định tuyến có thể được thực hiện một cách địa phương và tự động như đã nói trước đó.



Hình 3: Ví dụ về định tuyến địa lý: (a) X là hàng xóm gần nguồn với sink; (b) các khoảng trống: X là vị trí ngắn nhất.

1.2 Định hướng và mục tiêu của đề tài

Những nghiên cứu về vấn đề an ninh định tuyến trong WSN đã được nhiều các bài báo tập trung khai thác như chúng tôi cũng đã nói ở phần 1.1. Phần cốt lõi trong an ninh định tuyến là phải "xác minh được vị trí" có an toàn không trước khi chuyển sang phần "định tuyến". Khái niệm xác minh thông tin vị trí của chúng tôi được định nghĩa là xác định thông tin vị trí mà một node trong mạng WSN gửi đi đến các node khác có thực sự đúng nằm ở vị trí đó hay không. Việc này rất quan trọng để xác định được các node bị tấn công Wormhole, mạo danh làm sai lệch vị trí hay không…và từ đó quyết định gửi hoặc không gửi thêm thông tin đến các node này. Nghiên cứu về lĩnh vực xác minh này cũng đã có những bài báo [3] [1] [2] đề xuất, tuy nhiên khi áp dụng vào trong giải thuật GPSR thì chỉ có [4] đề cập qua và cũng trên quan điểm dựa theo nguyên tắc triangulation [5] cho một mạng Ad-hoc nói chung. Hơn nữa, hầu hết các bài báo nghiên cứu về xác minh thông tin vị trí chỉ là các phương pháp tập trung vào xác minh mà không gắn với quá trình định tuyến. Điều này vô tình làm quá trình định tuyến vẫn tồn tại các lỗ hổng dẫn đến tấn công làm mạng WSN không thể chuyển được dữ liệu ra ngoài. Dựa trên cách vận dụng sử dụng phương pháp áp dụng các thuật toán xác minh làm đầu vào trong quá trình định tuyến, chúng tôi đã tiếp cận theo hướng này. Ngoài ra, chúng tôi vận dụng phương pháp xác minh vị trí để tìm k đường dự phòng trong thuật toán định tuyến tìm đường biên khi mạng WSN xuất hiện các vùng void – một trường hợp mà công

trình [4] còn bỏ ngỏ. Nói cách khác, trong thuật toán định tuyến GPSR mà [4] nghiên cứu có hai pha riêng biệt, phần Greedy Forwarding đã được đảm bảo an toàn thông qua cơ chế RGR, nhưng phần xác minh thông tin vị trí và đảm bảo an toàn cho định tuyến vòng Perimeter Forwarding khi mạng bị tấn công thì chưa thực hiện được. Chúng tôi tập trung giải quyết vấn đề này. Như vậy có hai vấn đề chính cần thực hiện trong nghiên cứu đề tài:

- Xác định phương pháp xác minh thông tin vị trí của node khi quá trình định tuyến chuyển sang chế độ void: Đánh giá tính hiệu quả của phương pháp cũ và tiến hành thay bởi phương pháp xác minh mới phù hợp với điều kiện của bài toán.

- Đảm bảo an toàn cho quá trình định tuyến theo đường biên Perimeter Forwarding.

1.3 Phạm vi của đề tài

Chúng tôi lựa chọn định hướng giải quyết một trường hợp đặc biệt của định tuyến trong mạng WSN là xác minh thông tin vị trí để định tuyến an toàn trong mạng WSN khi có xuất hiện void nên chỉ tập trung trình bày những vấn đề liên quan đến trường hợp này, những vấn đề liên quan đến định tuyến an toàn sẽ được nhắc đến nhưng không phải là trọng tâm. Do hạn chế về sử dụng thiết bị cũng như một mô hình mạng toàn diện có đầy đủ các dạng tấn công mới nhất nên chúng tôi chỉ chọn mô phỏng qua NS2 và đánh giá với những kịch bản tấn công có xuất hiện void điển hình.

CHƯƠNG II: XÁC MINH THÔNG TIN VỊ TRÍ TRONG MẠNG CẢM BIẾN KHÔNG DÂY

2.1 Xác minh thông tin vị trí

Xác minh thông tin vị trí là việc xác định thông tin vị trí mà một node trong mạng WSN gửi đi đến các node khác có thực sự đúng nằm ở vị trí đó hay không.

2.2 Các cuộc tấn công có thể xảy ra và biện pháp đối phó

Thao tác truyền sự định vị

Trong khi một nút không liên quan tới vị trí riêng của nó trong kế hoạch được đề xuất, nó có thể cố gắng làm ảnh hưởng đến sự định vị bằng cách khai thác các cơ chế định vị cơ bản.

Tấn công dạng gói Unicast

Một cuộc tấn công có thể cố gắng để ngăn chặn sự đồng thuận giữa các Anchor bằng cách lừa chúng với truyền tin Unicast khác nhau. Ví dụ, một nút độc hại có thể gửi các yêu cầu trực tiếp tới các nút Anchor khác nhau bằng việc sử dụng một mức năng lượng khác nhau cho việc truyền mỗi yêu cầu.

Tấn công di động

Trong tấn công này, một nút độc hại có thể được chứng nhận vị trí hợp lệ và sau đó chúng di chuyển đến vị trí mới. Do đó, thông tin vị trí được xác nhận không còn đúng nữa. Tấn công này có thể không dễ dàng ngăn chặn, bởi vì vị trí là chính xác tại thời điểm xác minh.

Phá hoại các nút định vị

Kế hoạch được mô tả với nhiều giả định rằng sự định vị các nút Anchor là được tin cậy và không bị làm tổn hại. Đầu tiên, một cuộc tấn công thao tác truyền tin quảng bá được thử. Thứ hai, ít nhất một nút Anchor có một lỗi hoặc nó đã bị xâm nhập.

2.3 Các giả sử và mô hình hệ thống

Trong hệ thống của chúng tôi, tất cả các nút cảm biến có thể ước lượng vị trí của chúng bằng cách sử dụng bất kỳ các chương trình định vị hiện có. Những vị trí này được gọi là vị trí ước tính của cảm biến hoặc vị trí tuyên bố, và khoảng cách giữa các vị trí ước tính của cảm biến và vị trí thực sự của nó được gọi là *sai số định*

vị. Phạm vi giao tiếp của một cảm biến được một vòng tròn có tâm tại đúng vị trí của bộ cảm biến và có một bán kính nhất định.

2.4 Các phương pháp xác minh thông tin vị trí mới

Dựa trên những mục tiêu xác minh, chúng tôi phân loại các giải pháp xác minh vị trí thành hai loại: xác minh trong khu vực [6] [1] [7] và xác minh vị trí đơn [7] [8]. Loại 1 là để xác minh rằng cho dù các nút *nhân chứng* đang ở trong một khu vực nhất định. Loại 2 là để xác minh rằng cho dù các nút *nhân chứng* nằm tại các vị trí nhất định.

2. 4.1 Xác minh tại chỗ

Một số giải pháp được đề xuất dựa trên kỹ thuật biên khoảng cách. Brands và Chaum đã đề xuất đầu tiên về khoảng cách biên để làm cho các *nhân chứng* không thể làm giảm khoảng cách của nó tới *người xác minh*.

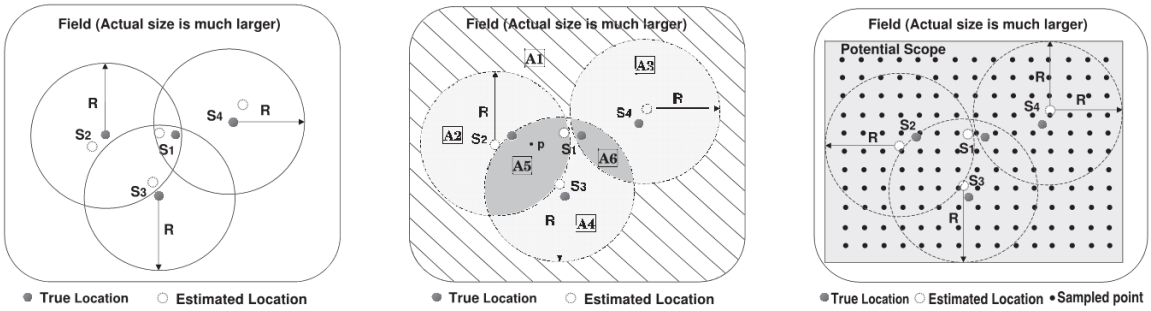
2.4.2 Sự xác minh vị trí đơn

Căn cứ vào số lượng các nút xác nhận tại một thời gian, chúng ta có thể tiếp tục phân loại các thuật toán xác minh thành hai loại: xác minh hàng loạt [5], [6], [8] và xác minh nút đơn [9], [10]. Loại xác minh thứ nhất là để xác minh một lô các nút tại một thời điểm, và sau này là để xác minh từng nút một.

Xác minh hàng loạt: Trong [18] Wei đề xuất hai thuật toán chạy ở một Trung tâm xác nhận (VC) để xác minh các vị trí của các nút: GFM và TI. GFM là để phát hiện vị trí cảm biến bất thường dựa trên sự không thống nhất trong bốn ma trận nguồn

2.4.3 Xác minh vùng In-Region

Trong phần này, Wei đề xuất một thuật toán đơn giản mà VC có thể sử dụng để thực hiện trong khu vực xác minh. Thuật toán này cũng sử dụng quan sát lân cận của cảm biến. Về cơ bản, nếu hai cảm biến quan sát nhau, và các VC coi họ là một cặp "xác nhận" hàng xóm. Sau đó, VC xuất phát một phân phối xác suất mỗi cảm biến, mà chỉ ra làm thế nào để cảm biến là mỗi điểm trong khu vực này. Chức năng phân phối có thể là liên tục hay rời rạc. Ở các phiên bản liên tục, trong khu vực tin cậy được tính bằng cách lấy tích phân của chức năng phân phối trong khu vực xác minh. Ở phiên bản rời rạc, trong vùng tin tưởng là tổng của các xác suất của tất cả các điểm trong việc xác minh khu vực.



(a) s_1's neighborhood (b) ECRs (c) Potential Scope

Hình 10 Một hình ảnh về khu vực của nút cảm biến s_1 có 3 hàng xóm s_2, s_3, và s_4

2.5 So sánh các giải pháp xác minh vị trí

Chúng tôi liệt kê phân loại các giải pháp hiện có trong hình 4. Một số thuật toán xác minh đơn vị không cần bất kỳ phần cứng bổ sung. Tuy nhiên, trong khu vực các thuật toán xác minh thường cần thêm phần cứng để đại diện cho các khu vực được bảo vệ hoặc xác nhận.

2.6 Lựa chọn phương pháp xác minh thông tin vị trí

Trong số nhiều phương pháp xác minh thông tin vị trí, chúng tôi chọn thiết kế một hệ thống xác minh sử dụng VC để xác định xem ước tính vị trí của cảm biến có đáng tin cậy hay không.

2.7 Kết luận

Phương pháp mà chúng tôi chọn đã được phát triển nhưng là một phương pháp độc lập không được tích hợp vào để giải quyết bài toán định tuyến an toàn. Chúng tôi kế thừa những ý tưởng này vào giải quyết bài toán xác minh thông tin trước khi định tuyến và truyền tin để đảm bảo an toàn. Đóng góp chủ yếu của chúng tôi tại phần này là cố gắng tích hợp phương pháp xác minh vùng cải tiến mới để tìm cách giảm thiểu thời gian phải xác minh, từ đó tăng tốc hoặc tăng tỉ lệ chuyển phát gói tin của quá trình định tuyến an toàn.

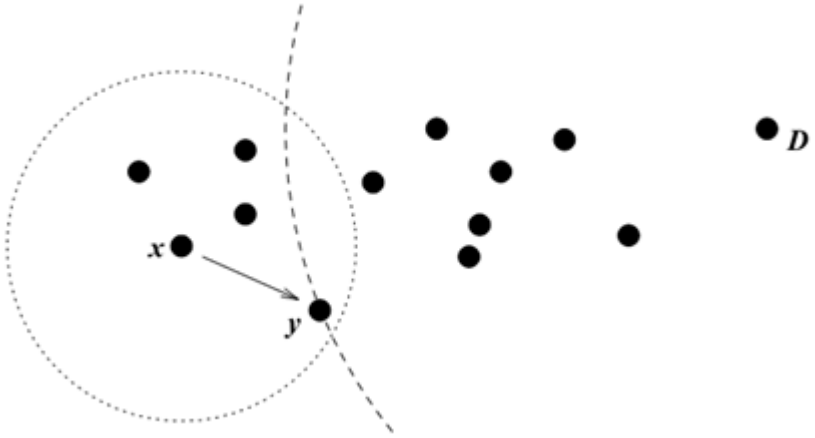
CHƯƠNG III: ĐỊNH TUYẾN PHỤC HỒI THEO THÔNG TIN VỊ TRÍ

3.1 GPSR

Dựa trên kết quả của phương pháp xác minh thông tin vị trí bên trên, chúng tôi tiến hành bước tiếp theo là sử dụng nó phục vụ quá trình định tuyến an toàn. Bây giờ chúng ta sẽ thảo luận các thuật toán định tuyến tham lam theo các trạng thái biên GPSR. Đây là thuật toán khởi nguồn được [11] đề xuất, được sử dụng rộng rãi trong WSN. Thuật toán bao gồm hai phương pháp cho việc chuyển tiếp các gói tin: chuyển tiếp tham lam, được sử dụng bất cứ nơi nào có thể, và chuyển tiếp chu vi, được sử dụng trong các khu vực chuyển tiếp tham lam không thể được.

3.1.1 Chuyển tiếp tham lam

Trong GPSR, một nút chuyển tiếp có thể làm cho một tối ưu vị trí, lựa chọn tham lam trong việc chọn một bước nhảy tiếp theo của gói tin. Cụ thể, nếu một nút biết vị trí hàng xóm của nó, sự lựa chọn vị trí tối ưu cho bước nhảy tiếp theo là hàng xóm gần nhất với đính đến của gói. Chuyển tiếp trong chế độ này lặp lại sao cho các bước nhảy địa lý gần hơn cho đến khi tới vị trí đích. Một ví dụ về sự lựa chọn bước nhảy tham lam tiếp theo được chỉ ra trong hình 16.

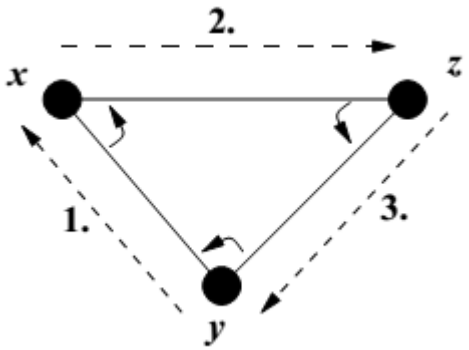


Hình 16. Ví dụ chuyển tiếp tham lam

3.1.2 Quy tắc bàn tay phải

Quy tắc bàn tay phải từ lâu được biết để vượt qua void như hình vẽ được mô tả trong hình 19. Quy luật này nói rằng khi đến nút x từ nút y, các cạnh tiếp theo đi qua là một tuần tự tiếp theo ngược chiều kim đồng về x từ mép (x; y). Biết rằng, quy tắc bàn tay phải đi qua phần bên trong của một khu vực đa giác khép kín theo thứ tự

cạnh chiều kim đồng hồ trong trường hợp này, các tam giác được giới hạn bởi các cạnh giữa các nút x, y, z, theo thứ tự $(y \to x \to z \to y)$. Quy tắc đi qua một khu vực bên ngoài, trong trường hợp này, các khu vực bên ngoài của cùng tam giác, theo thứ tự cạnh ngược chiều kim đồng hồ.



Hình 19. Quy tắc bàn tay phải

3.1.3 Đồ thị phẳng

Trong các mạng được tạo ra một cách ngẫu nhiên, nó là không thể chấp nhận cho một thuật toán định tuyến liên tục thất bại nếu chẳng may mô hình mạng rơi vào trường hợp đặc biệt – điều hoàn toàn có thể xảy ra trong thực tế - là các liên kết trên đường đi theo quy tắc bàn tay phải có sự đan chéo dẫn đến định tuyến lặp. Bởi sự bất cập của liên kết dạng đan chéo, Karp trình bày các phương pháp thay thế để loại bỏ các liên kết chéo trong mạng thông qua đồ thị phẳng.

3.1.4 Kết hợp tham lam và vành đai đồ thị phẳng

Bây giờ chúng ta trình bày đầy đủ về thuật toán định tuyến tham lam theo chu vi trạng thái, cái mà kết hợp cả chuyển tiếp tham lam (Phần 2.1) trên đồ thị mạng đầy đủ với chuyển tiếp theo vành đai dựa trên đồ thị mạng được làm phẳng nơi mà chuyển tiếp tham lam là không thể thực hiện. Nhớ lại rằng tất cả các nút duy trì một bảng láng giềng, trong đó lưu trữ các địa chỉ và vị trí của các hàng xóm trong phạm vi phủ sóng 1 bước nhảy.

3.2. Định tuyến an toàn

3.2.1 Khả năng hồi phục GR (Resilient GR)

Mặc dù việc xác minh vị trí có thể ngăn chặn một cuộc tấn công xác định dựa trên việc làm sai lệch thông tin vị trí một nút bị tổn hại hoặc nguy hiểm có thể vẫn còn có các gói tin chuyển tiếp một cách có lựa chọn làm gián đoạn việc định tuyến.

Để giải quyết vấn đề này, chúng tôi đề xuất một giao thức định tuyến đa đường theo xác suất mà được phục hồi với gói tin bị mất do lỗi hoặc do một âm mưu tấn công.

3.2.2 Quản lý độ tin cậy

Ý tưởng cơ bản của kế hoạch quản lý độ tin cậy của chúng tôi là để ưu tiên những hành vi của các nút trung thực bằng việc cho chúng sự công nhận với mỗi gói tin chuyển tiếp thành công, trong khi phạt các nút đáng ngờ được cho là nói dối hoặc phóng đại sự góp sức vào việc định tuyến. Khi một nút nằm ở vị trí của nó, nó sẽ bị loại khỏi FS ngay lập tức.

3.2.3. Phân tích và điều chỉnh an ninh (Security analysis and trade-offs)

Bằng các thông điệp chứng thực và mã hóa, chúng ta có thể ngăn chặn một kẻ thù bên ngoài mà không dùng khóa mật để mạo danh một nút hợp lệ hoặc giải mã bản mã. Hơn nữa, các đối thủ không thể thay đổi dữ liệu trong quá trình vận chuyển mà không bị phát hiện.

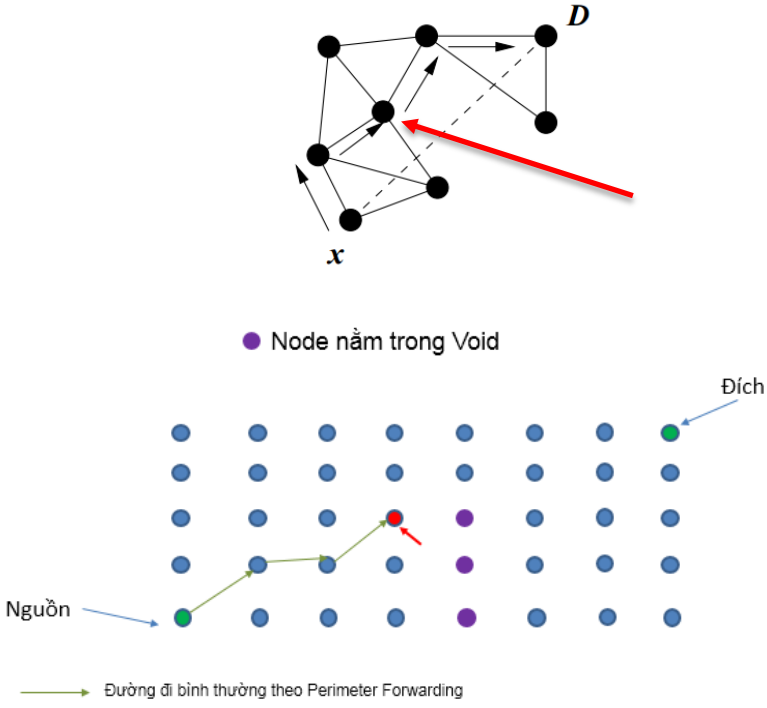
3.3 Kết luận

Trong nghiên cứu này, ngay từ đầu chúng tôi luôn mong muốn đưa ra được một giải pháp định tuyến an toàn hoàn chỉnh. Dựa trên bài báo của K.Liu [4] chúng tôi xác định được phần xác minh thông tin vị trí tác giả có sử dụng ý tưởng xác minh dựa trên phương pháp Triangulation, phương pháp xác minh tại chỗ này cũng có nhiều nhược điểm về tốc độ. Do đó chúng tôi tiến hành thay thế bằng thuật toán xác minh vùng để xác minh độ tin cậy của các node láng giềng trước khi chuyển tin. Phương pháp này sẽ được kiểm nghiệm tỉ lệ chuyển gói thành công tin cậy trong phần mô phỏng. Thêm nữa, trong quá trình thực hiện chúng tôi đã cố gắng giải quyết tình huống Perimeter Forwarding trong định tuyến an toàn bằng cách gửi broadcast đến k-láng giềng đã xác minh tin cậy sẽ trình bày chi tiết hơn bên dưới. Chúng tôi cố gằng bổ sung những phần còn hạn chế mà tác giả K.Liu [4] chưa giải quyết triệt để.Trong phần mã nguồn mô phỏng vì thế mà chúng tôi kế thừa từ mã nguồn của bài báo này để tiến hành cải tiến.

CHƯƠNG IV: GIẢI PHÁP VÀ ĐÁNH GIÁ THỰC NGHIỆM

4.1 Bài toán k-đường dự phòng trong Perimeter Forwarding

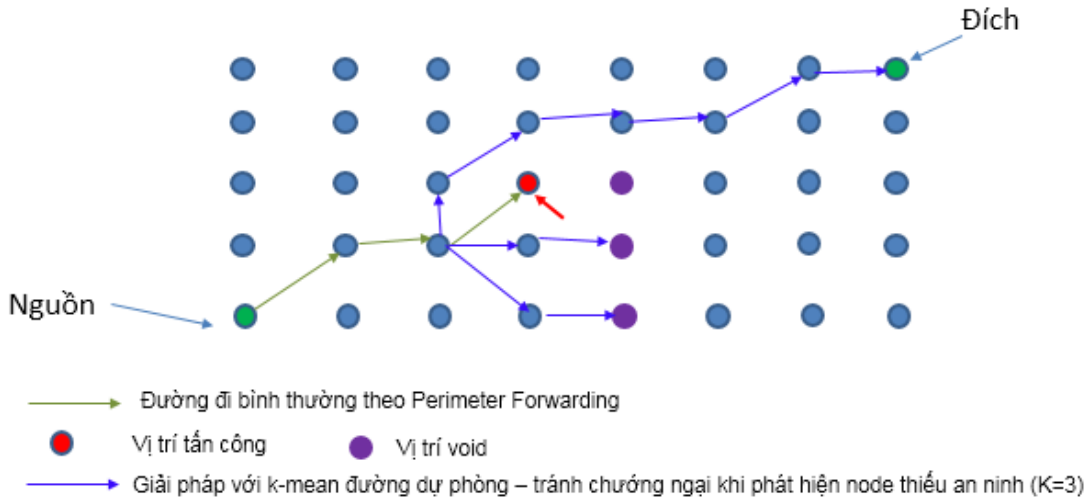
Việc xác định được thông tin vị trí đảm bảo an toàn là phần cốt lõi chính của bài toán chúng tôi đánh giá. Bài toán xác minh này chủ yếu được sử dụng để đảm bảo cho quá trình tiếp theo là định tuyến được thực hiện an toàn. Trong quá trình nghiên cứu chúng tôi phát hiện ra rằng, khi trong mạng xuất hiện hiện tượng void (từng một số node nằm trong vùng không thể chuyển được gói tin đến đích theo thuật toán GPSR thông thường) thì quá trình xác minh và định tuyến gặp trục trặc. B.Karp đã đưa ra giải pháp dùng Perimeter Forwarding để vượt void. Tức là khi gặp trạng thái void, thuật toán GPSR sẽ tắt trạng thái chuyển tiếp gói tin tham lam mà chuyển sang trạng thái dùng thuật toán vượt biên (xác định đường dựa trên quy tắc bàn tay phải và planar graph). Nhưng vấn đề lớn nhất với Perimeter Forwarding là định tuyến an toàn. Không giống như thuật toán tham lam, nó chuyển tin theo dạng broadcast và gói tin có nhiều đường để tìm đến đích, thuật toán Perimeter Forwarding chỉ chọn các điểm nằm bên trái nhất theo quy tắc bàn tay phải làm đường đi định tuyến của mình như hình bên dưới



Hình 24. Đường đi của Perimeter Forwarding bị tấn công

Như vậy nếu chẳng may một node trên đường đi này bị tấn công thì nguy cơ thông tin không chuyển được đến đích là rất cao. Giải pháp đơn giản của chúng tôi

là sử dụng nguyên tắc, khi xác minh nút theo chương 2 ở trên, node không đảm bảo tin cậy, thì chúng tôi tiến hành bật trạng thái forward đến k-đường dự phòng giúp tối đa hóa số đường đi mà gói tin có thể đi đến đích. Việc này dĩ nhiên cũng làm tăng chi phí về băng thông và năng lượng do nhiều node cùng phải làm nhiệm vụ nhưng mục tiêu vẫn đạt được là gói tin đến được đích. Việc thay đổi này khá đơn giản, trong mã nguồn của thuật toán Perimeter Forwarding, tiến hành forward đến k láng giềng đã xác thực của nó. Giá trị k có thể thay đổi tùy theo tỉ lệ gửi thành công của một vài phiên kiểm nghiệm. Giải pháp có thể minh họa theo hình bên dưới:



Hình 25: Ví dụ cho giải pháp K đường vượt void

4.2 Ý tưởng và giải thuật

Hầu hết các voids sinh ra do có các nút cực tiểu địa phương (nút cực tiểu địa phương- local minima là những nút không thể chọn được láng giềng để chuyển tiếp gói tin)[9]. Mặt khác để tránh được các Voids thì cần tránh các nút cực tiểu địa phương. Một trong các kỹ thuật để phát hiện khoảng trống là một kỹ thuật Boundhole. Bằng cách sử dụng một gói tin chuyển dọc theo biên của Voids cho đến khi quay về nút ban đầu. Như vậy Boundhole sẽ cho ta tập các nút nằm trên biên của Void.

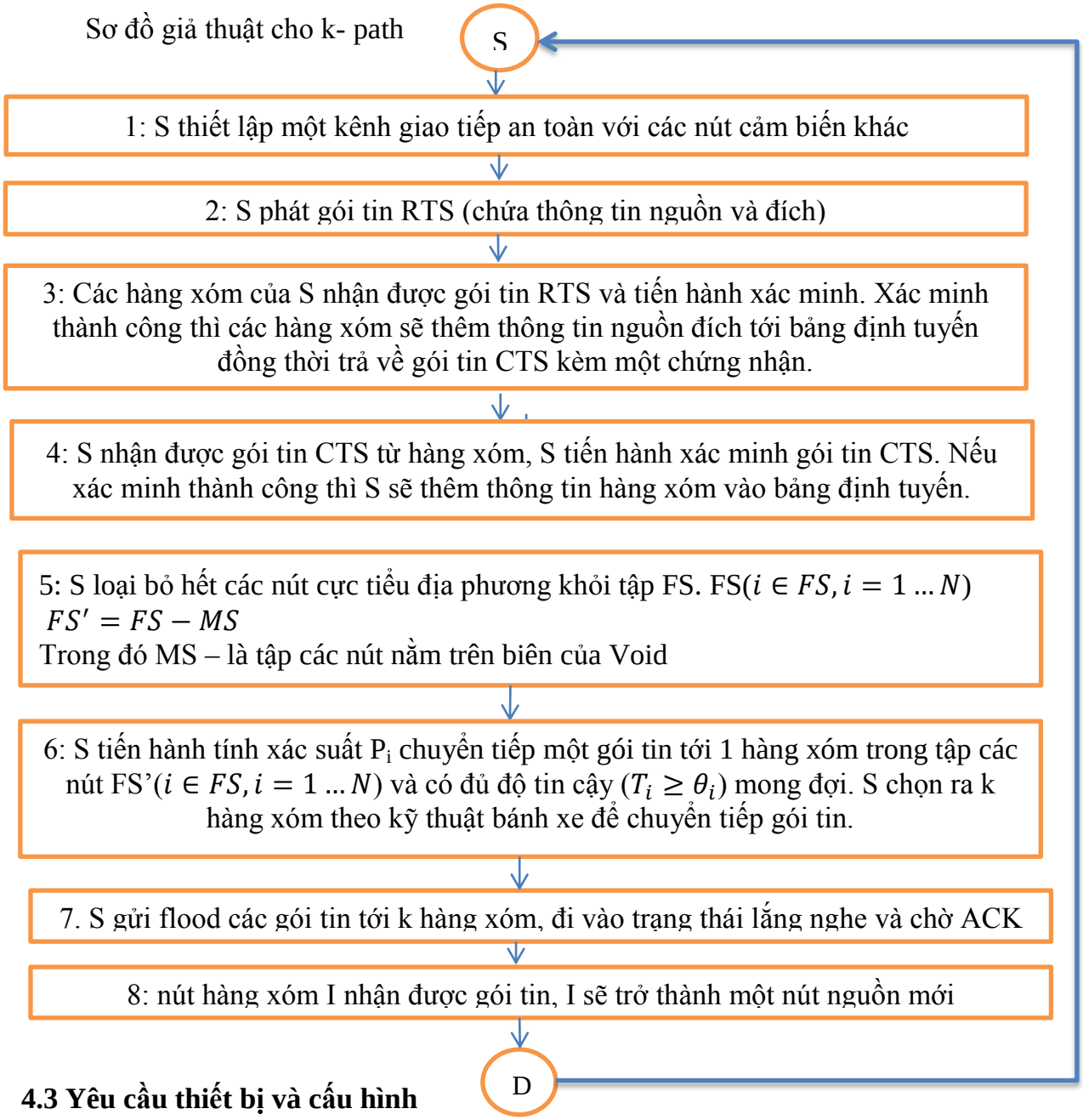
Hiện tại giải thuật RGR do Kliu đề xuất xác định FS – tập các nút hàng xóm có khả năng chuyển tiếp gói tin. Tuy nhiên một số nút vẫn có khả năng chuyển tiếp gói tin, nhưng nằm trên đường biên của Void thì không nên thuộc tuyến. Vì các lý do như sau:

- Khả năng an toàn của Nút này có thể là thấp.

- Giả sử trong trường hợp nút đủ tin cậy để sử dụng trong quá trình định tuyến. Một khi quá nhiều tuyến cùng lựa chọn nút này để chuyển tiếp gói tin thì sẽ gây đến tắc nghẽn cho nút biên như thầy Thanh có đưa ra trong Luận văn Phd.

Dựa trên giải thuật định tuyến an toàn kháng lỗi RGR đã được Kliu đề xuất như vậy để tránh việc tắc nghẽn trên đường biên và có thể vượt qua được các voids một cách an toàn thì " Các nút nằm trên biên của Void nên được loại bỏ trước khi tính xác suất chuyển tiếp một gói tin tới một hàng xóm trong tập FS".

Sơ đồ giả thuật cho k- path



4.3 Yêu cầu thiết bị và cấu hình

Tất cả các nghiên cứu thực nghiệm chúng tôi đều tiến hành trên máy tính với các chương trình mô phỏng bằng phần mềm. Thông số cơ bản của máy tính chúng tôi dùng là:

- ✓ CPU: Intel Core i5-3210M 2.5 Ghz
- ✓ RAM: 4 GB
- ✓ Hệ điều hành: Ubuntu 12.04 LTS Precis Pangolin
- ✓ Video Card onboard

Để có thể mô phỏng được tất cả các tham số về độ trễ, thời gian gửi tin, độ lớn mỗi gói, … phải có phần cứng hỗ trợ. Điều mà không khả thi nếu triển khai toàn bộ các thành phần thiết bị cần thiết như trong nghiên cứu. Vì vậy chúng tôi chọn sử dụng phần mềm mô phỏng, trong số đó NS-2.35 là công cụ mô phỏng chính. Do đây là phần mềm miễn phí, hỗ trợ tất cả các chuẩn giao thức cơ bản, hỗ trợ cache, nhiều thư viện mở rộng và có khả năng tùy biến cách thức gửi tin rất tốt.

4.4 Kịch bản mô phỏng

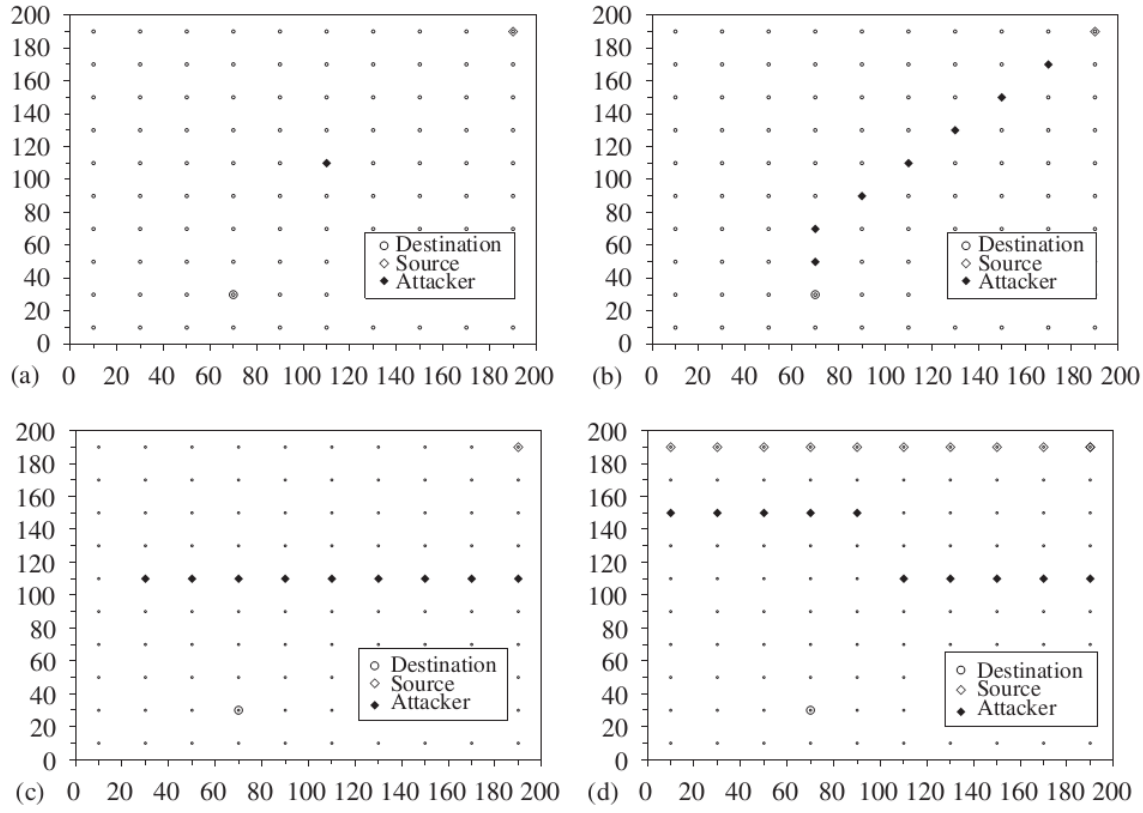
Chương trình mô phỏng được thực hiện trên NS2, là sự mở rộng của giao thức GPSR gọi là RGR (resilient geographic routing) cho mạng cảm biến không dây. Đồng thời thời cũng có một số thay đổi giao thức trong cài đặt IEEE 802.11 để phù hợp với thí nghiệm. Trong thí nghiệm này 100 cảm biến được triển khai theo lưới 10 × 10 bao phủ một diện tích 200 × 200 m2, trong đó mỗi nút được đặt tại mắt lưới (đánh số bắt đầu từ 0 đến 99, từ trái sang phải và dưới lên trên). Nút thu nhận dữ liệu cố định (hoặc đích) nằm ở phía dưới (nút 13). Bảng bên cạnh tóm tắt các tham số mô phỏng chính. Để so sánh tỉ lệ gói tin đến đích, thí nghiệm sử dụng mô hình kịch bản ở hình 25.1 gồm 10 nút tấn công (70 đến 74 và 55 đến 59) với nút phát tín hiệu ở trên cùng (nút 99)

Các thông số sử dụng khi mô phỏng theo bảng dưới đây

Phạm vi phủ sóng R	30m
Băng thông	2Mbps
Gói dữ liệu	64B
Kích thước gói tin	158B
Tốc độ gửi tin	2packets/s
Độ dài hàng đợi	100packets
Chu kỳ gửi gói Hello	5s
Thời gian hoạt động	200s
Giá trị khởi tạo T_i	0.5
Công suất gửi	0.5w
Công suất nhận	0.2w

Để xem xét mô hình tấn công khác nhau, chúng tôi sử dụng 5 kịch bản khác nhau được thể hiện trong hình 26. Trong kịch bản thứ 1, chỉ có một kẻ tấn công nằm trên con đường ngắn nhất từ nguồn đến đích được xây dựng bởi GPSR. Trong kịch bản thứ 2, tất cả các nút tạo nên đường ngắn nhất đều là kẻ tấn công. Trong kịch bản thứ 3, 9 kẻ tấn công tạo thành một bức tường trên mạng và cố gắng chia cắt nguồn và đích. Với các kịch bản 1-3, chúng tôi cố định ngưỡng là 0.01.

Kịch bản 4 và 5 có cùng cấu trúc mạng. Kịch bản 4 và 5 sử dụng các giá trị ngưỡng khác nhau, tương ứng là 0.01 và 0.02. Kịch bản 5 thay đổi thêm trong điều kiện của ngưỡng. Chúng tôi cũng thay đổi tốc độ dữ liệu và số lượng của các nguồn thông tin để đánh giá kỹ lưỡng hiệu quả các tác động của quản lý độ tin cậy trong các thiết lập truyền thông khác nhau.



Hình 26 Mô hình các kịch bản mô phỏng; (a) kịch bản 1, (b) kịch bản 2, (c) kịch bản 3, (d) kịch bản 4 và 5.

4. 5 Kết quả mô phỏng

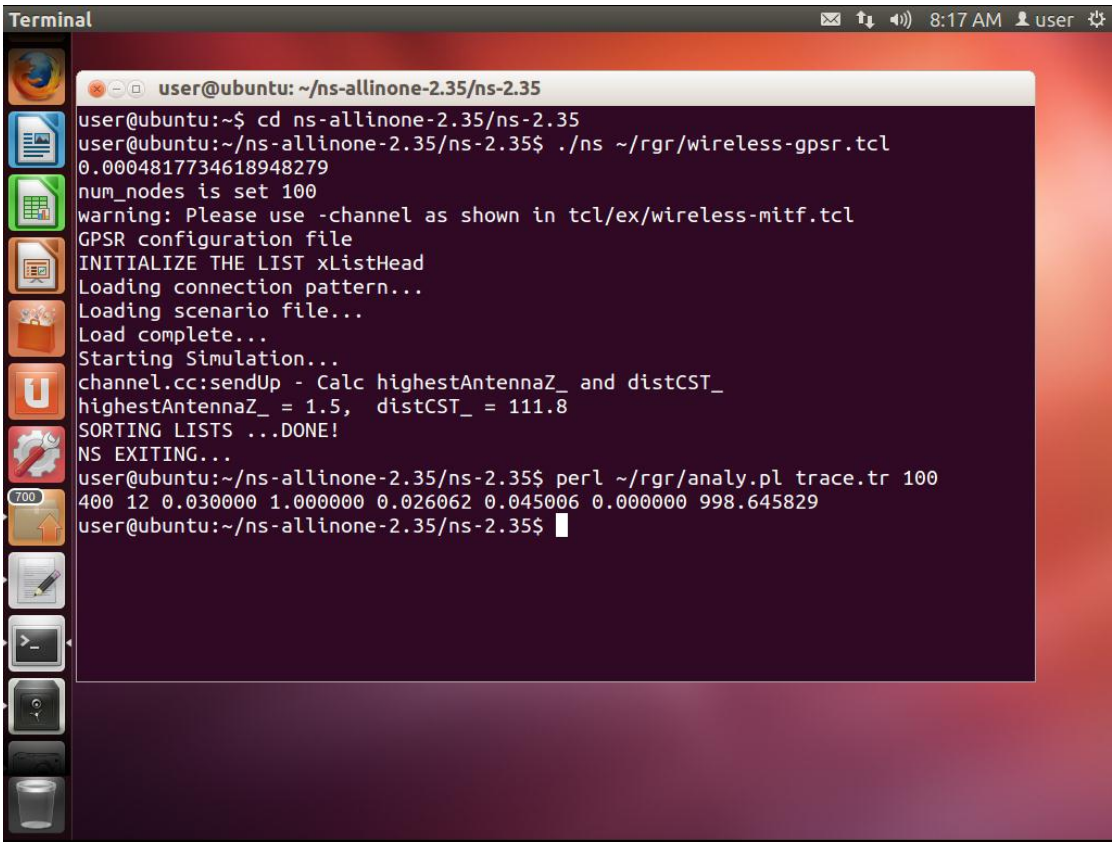
Tham số đo đạc

Với từng kịch bản sẽ tiến hành đo những tham số thể hiện đặc tính bản chất của kết quả hướng đến.

Với kịch bản xác định tính hiệu quả của phương pháp cũ với mô hình dữ liệu mới, chúng ta cần xác định được: Tỉ lệ phát hiện sai truy cập hợp pháp là tấn công trong các trường hợp truy cập thông thường = tỉ lệ truy cập thành công của người dùng bình thường khi không có tấn công. Phát hiện sai ở đây nghĩa là khi sinh ra dữ liệu của người dùng bình thường rồi tiến hành thử kết nối đến máy chủ Web thì phiên truy cập không thành công – do bị bộ lọc ngăn lại.

Với kịch bản xác định tính hiệu quả của phương pháp mới với mô hình dữ liệu mới chúng tôi tiến hành đo đạc:

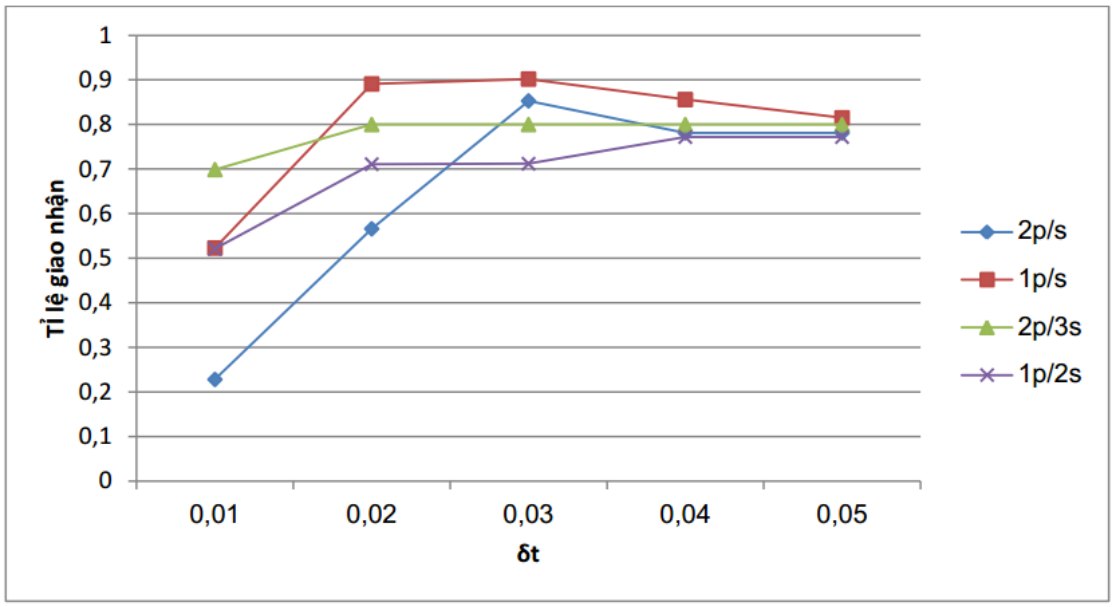
- ✓ Tỉ lệ chuyển tiếp các gói tin đến đích thành công trong các trường hợp có tấn công
- ✓ Tỉ lệ chuyển tiếp các gói tin đến đích thành công trong khi thay đổi chỉ số độ tin cậy.
- ✓ Tỉ lệ chuyển tiếp các gói tin đến đích thành công trong thay đổi chỉ số độ tin cậy và tăng số lượng nút nguồn



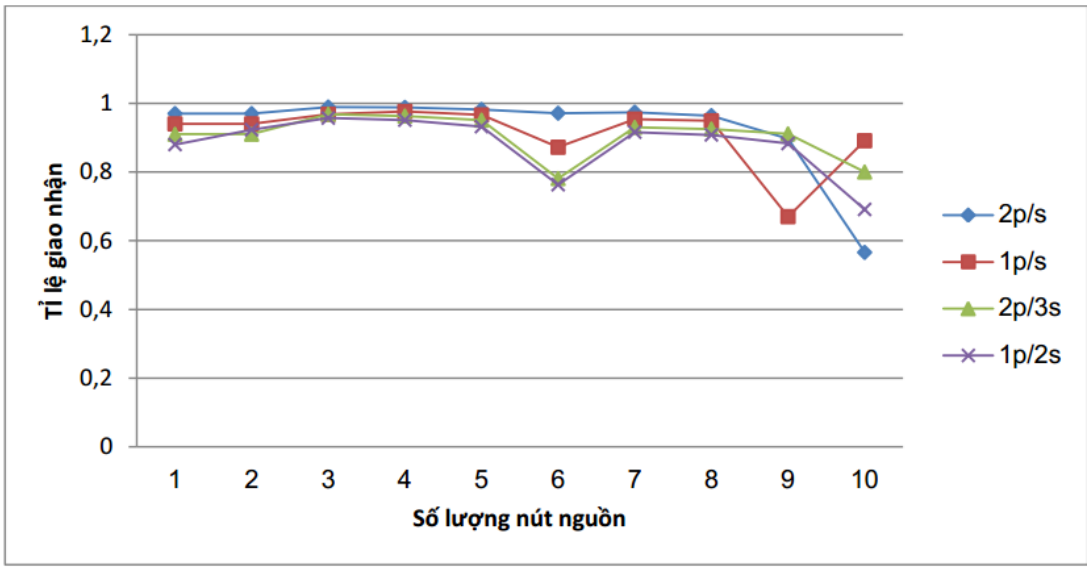
Hình 27. Kết quả chạy thuật toán định tuyến phục hồi

Bằng cách thay đổi các ngưỡng và số lượng nút nguồn gửi tin đi trên nhiều tốc độ truyền tin khác nhau chúng tôi có được kết quả như hai đồ thị dưới đây khi

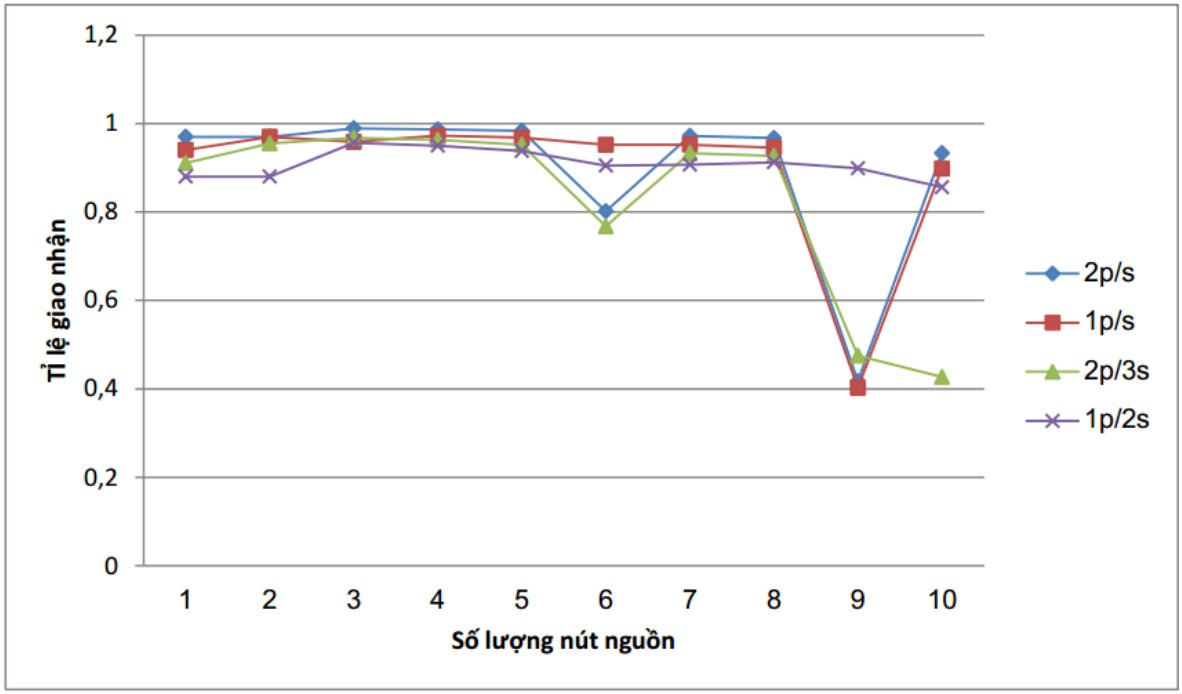
cài đặt giao thức của tác giả (RGR) (các đường khác nhau biểu thị kết quả cho mỗi tốc độ gửi gói tin).



Khi tăng số lượng nút trong mạng cảm biến



Với một nút nguồn (nút 99) gửi 2 gói tin mỗi giây, đặt ngưỡng 0.02, khi cấu hình thêm lỗ sâu (http://ds2.cs.purdue.edu/software/wormhole/wormhole.html) vào trong kịch bản (giữa nút 66 và 23),chúng tôi có thêm một số kết quả như sau :



Ở lần thí nghiệm đầu tiên có thể thấy rằng giao thức cũ hầu như không thể vượt qua tình huống tấn công. Trong khi đó giao thức được nghiên cứu đem lại khả năng thành công vượt trội đặc biệt trong trường hợp tỉ lệ δt/Δt và tốc độ phù hợp, số lượng nút nguồn cũng có một ảnh hưởng không nhỏ cần tìm hiểu.

Kết quả thử nghiệm và các vấn đề đã nghiên cứu trong luận văn này, chúng tôi đã lưu tại: rintechno.com/store/huong

4.6 Đánh giá kết quả nghiên cứu

Trong quá trình mô phỏng k-đường dự phòng các gói tin bị mất mát rất nhiều, tỷ lệ chuyển phát gói tin đến đích thành công là rất thấp. Với k = 5 thì.

Hình 28. Kết quả chạy thuật toán định tuyến phục hồi k-đường dự phòng.

Ở đây, tỷ lệ chuyển phát gói tin đến đích thành công là hoàn toàn không có. Như vậy, khả năng các gói tin không thoát được void là rất lớn. Mặc dù định tuyến phục hồi vẫn thành công ở chế độ chuyển tiếp tham lam ngay cả khi có tấn công như Keliu [10] đã thực hiện.

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

1. Kết luận

Chúng tôi đã thử nghiệm phương pháp đề xuất. Tuy nhiên hiệu quả đạt được không cao đạt được một số kết quả tốt thể hiện sự hiệu quả của phương pháp đề xuất so với một số công trình đã được công bố với những đánh giá rõ ràng. Một số thành tựu chính bao gồm:

+ Nghiên cứu các thuật toán xác minh thông tin vị trí mới làm nền tảng cho các hướng nghiên cứu tương lai.

+ Chúng tôi cũng đề xuất và xây dựng được cơ chế định tuyến mới là k-đường dự phòng cho các gói tin khi đi vào chế độ định tuyến theo chu vi.

+ Kết quả mô phỏng đánh giá sự ảnh hưởng trực tiếp của chỉ số độ tin cậy trong các công trình nghiên cứu đã công bố của các tác giả ở các tài liệu [9],[10].

2. Hướng phát triển

Vấn đề tồn tại trong quá trình thực hiện mô phỏng cũng như việc thực hiện giải pháp theo đề xuất chưa đạt được thành tựu đáng kể. Cũng như việc triển khai mô hình mạng trong thực tế còn gặp khó khăn về cơ sở nên công việc này chúng tôi sẽ tiếp tục trong một nghiên cứu tiếp theo.