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

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

Hà Nội – Năm 2016

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 :

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

NGƯỜI HƯỚNG DẪN KHOA HỌC: TIẾN SĨ NGUYỄN ĐẠI THỌ

Hà Nội – Năm 2016

LỜI CAM ĐOAN

Tôi xin cam đoan: Luận văn này là công trình nghiên cứu thực sự của cá nhân tôi. Các số liệu, những kết luận nghiên cứu được trình bày trong luận văn này trung thực do tôi thực hiện không sao chép kết quả của bất cứ ai khác. Trong quá trình nghiên cứu tôi có tham khảo các bài báo và công trình nghiên cứu liên quan, tôi cũng đã trích dẫn đầy đủ trong luận văn. Tôi xin chịu trách nhiệm về nghiên cứu của mình.

Học viên

Nguyễn Lan Hương

LỜI CẢM ƠN

Đầu tiên tôi xin gửi lời cảm ơn chân thành đến các thầy, cô trường Đại học Công nghệ - Đại học Quốc gia Hà Nội đã nhiệt tình giảng dạy và hướng dẫn tôi trong thời gian học tập tại trường.

Tiếp đó, tôi xin bày tỏ lòng biết ơn sâu sắc tới thầy **TS.Nguyễn Đại Thọ** đã nhiệt tình hướng dẫn, tích cực phân tích, lắng nghe và phản biện giúp tôi hiểu và đi đúng hướng để có thể hoàn thành luận văn này.

Tôi cũng xin gửi lời cảm ơn đến **TS. Lê Đình Thanh** đã tham gia định hướng giúp tôi trong quá trình nghiên cứu, đánh giá kết quả thu được đảm bảo tính khoa học và tin cậy.

Mặc dù đã rất cố gắng để hoàn thiện luận văn này song không thể không có những thiếu sót, tôi mong nhận được sự góp ý và nhận xét từ các thầy, cô và các bạn đọc.

Học viên

Nguyễn Lan Hương

TÓM TẮT

Thông tin vị trí là thông tin quan trọng đối với nhiều ứng dụng trong các mạng cảm biến không dây (WSN). Khi các nút cảm biến được triển khai trong môi trường thù địch, rất dễ bị tấn công do đó thông tin vị trí cảm biến không đáng tin cậy và cần phải được xác nhận trước khi chúng có thể được sử dụng bởi các ứng dụng dùng nó. Các hệ thống xác minh trước đó hoặc là yêu cầu triển khai dựa trên nhóm kiến thức về khu vực cảm biến, hoặc phụ thuộc vào phần cứng chuyên dụng đắt tiền, chúng không phù hợp để sử dụng cho các mạng cảm biến chi phí thấp. Trong luận văn này, chúng tôi nghiên cứu sử dụng các Anchor là những node tin cậy được trang bị GPS nằm rải rác trong mạng WSN làm trung tâm trong quá trình xác minh thông tin vị trí các node có phần cứng hạn chế nằm trong phạm vi truyền tin của nó. Việc xác thực thông tin vị trí này sẽ cho phép thực hiện định tuyến an toàn giải quyết bài toán an ninh trong thuật toán vượt biên (Perimeter Forwarding) vượt vùng void của giao thức GPSR. Chúng tôi đề xuất sử dụng phương pháp k- đường dự phòng thay vì chỉ chọn một đường duy nhất theo phương pháp quy tắc bàn tay phải. Giải pháp đề xuất này cung cấp ít nhất một con đường định tuyến tới đích ngay cả trong trường hợp các node trên biên bị tấn công. Trong quá trình thử nghiệm k –path, chúng tôi thấy rằng hiệu quả thuật toán là chưa cao, cụ thể tỉ lệ các gói tin bị mất rất nhiều. Mặc dù vậy, thử nghiệm cũng đạt các kết quả nhất định như thấy rõ sự ảnh hưởng của chỉ số độ tin cậy trong định tuyến phục hồi thế hệ trước.

Từ khóa: Định vị, xác minh, tại chỗ, khu vực, an ninh mạng cảm biến không dây, định tuyến địa lý, xác thực vị trí.

ABSTRACT

Location information is information that is important for many applications in wireless sensor networks (WSNs). When the sensor nodes are deployed in hostile environments, the location information is very vulnerable. Therefore, the sensor location information is not reliable and should be verified before they can be used by applications that use it. The previous verification system or deployment requirements based on knowledge of the regional group sensor, or dependent on expensive dedicated hardware, so they are not suitable for use in sensor networks chi low cost. In this paper, we propose to use location verification which trust-based GPS Anchor node are distributed in WSN network to verify low-hardware nodes in its radio range. This step will solve issues of Perimeter Forwarding step – algorithm routes around void area – in GPSR Routing. We propose k-path method in perimeter routing instead of unique path in right hand rule as original GPRS. Its feature: we still found a routing path to destination even when a node at perimeter mode was attacked. Through the testing and received results, we found that its efficiency is not high, the percentage of packets lost a lot. However, the test also reached certain results as clear indicators of the impact of reliability in previous resilient method.

Keywords: Location verification, triangulation, wireless sensor networks, Geographic routing, Perimeter Routing, Secure WSN Protocol.

MỤC LỤC

DANH MỤC CÁC KÝ HIỆU VÀ CHỮ VIẾT TẮT

VC	Verification Center
SubVC	Sub Verification Center
GFM	Greedy Filtering using Matrix
GFT	Greedy Filtering Using Trustability-Indicator
WSN	Wireless sensor network
WSNs	Wireless sensor networks
RF	Radio Frequence
GR	Greograph Routing
RGR	Resilient Geographic Routing
ToA	Thời gian đến
TDoA	Thời gian khác nhau khi đến
XOR	Phép toán Xor
DV-hop	Distance Vector –hop
DV- distance	Distance Vector –distance
GPS	Global Positioning System – Hệ thống định vị toàn cầu
AD	Active Difference Metric
PD	Passive Difference Metric
AS	Asymmetry Metric
CN	Consistent-Neighbor Metric
ECR	Estimated communication range
CBS	Trạm cơ sở bảo mật (covert base stations)
MBS	Trạm cơ sở di động
FS	Tập chuyển tiếp (Forwarding set)
RSS	Tín hiệu vô tuyến
BS	Base station – trạm cơ sở
LAD	Localization Anomaly Detection
PLV	Phương pháp xác minh thông tin vị trí sử dụng xác suất
PMF	Hàm xác suất khối
AoA	Angle of Arrival

DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

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 …

Mạng cảm biến không dây có rất nhiều các ứng dụng tiềm năng. Bởi vì bản chất của ứng dụng điều khiển trên nó, các cơ sở hạ tầng của một cảm biến mạng không dây dễ dàng thay đổi dẫn đến một loạt các lớp và kiến trúc đa dạng. Dưới đây sẽ mô tả các đặc điểm chính của cảm biến không dây, chú ý rằng không phải tất cả các mạng cảm biến không dây đều có đầy đủ các đặc điểm này.

- Nút (tài nguyên có giới hạn): Để kích hoạt tính năng lấy mẫu hiệu quả về chi phí trong thế giới thực, cảm biến có những hạn chế về mặt hình thức, yếu tố và chi phí. Kết quả là, các nút cảm biến thường được đánh giá cao qua giới hạn xử lý, bộ nhớ và khả năng giao tiếp. Bản chất giám sát không dây thường ngầm định là nó không có quyền truy cập vào các nguồn năng lượng tái tạo. Do đó, hiệu quả năng lượng là quan trọng cho việc mở rộng thời gian làm việc của mạng.
- Dữ liệu định hướng hoạt động: Các đầu vào trong một mạng cảm biến không quan trọng đối với riêng nó, thay vào đó, chúng được dùng như một công cụ để lấy mẫu thế giới vật chất xung quanh chúng. Như vậy, định địa chỉ cá nhân không phải là quan trọng (như là trường hợp của dữ liệu mạng). Cảm biến có thể được giải quyết bằng vai trò của nó, hoặc ứng dụng khác có khả năng xác định. Ví dụ, người quan sát có thể yêu cầu nhiệt độ trong một khu vực nhất định chứ không phải cho nhiệt độ ở một cảm biến cụ thể.

- Mô hình truyền thông mới: Các mô hình truyền thông điển hình trong mạng tùy biến không dây truyền thống là điểm tới điểm. Ngược lại, trong mạng cảm biến không dây, lưu lượng truy cập dữ liệu thường chảy từ nhiều nguồn đến một điểm thu gom dữ liệu như là thu thập hoặc chuyển tiếp để đáp ứng yêu cầu truy vấn, hoặc là kết hợp dữ liệu liên quan.
- Quy mô lớn: Kích thước của mạng cảm biến không dây thay đổi theo các ứng dụng. Hãy hình dung rằng một số mạng sẽ bao gồm số lượng lớn của cảm biến. Điều này làm cho việc tổ chức, lập trình và gỡ lỗi gặp khó khăn.
- Yêu cầu thời gian thực: Đối với một số ứng dụng, tính kịp thời của việc nhận dữ liệu làm tăng thời gian khó khăn trong truyền tải. Dữ liệu thu nhận được muộn là vô dụng, và truyền dữ liệu như vậy có thể làm giảm hiệu suất của toàn mạng.

Chức năng chính của một WSN là để phát hiện và báo cáo các sự kiện mà có thể được so sánh và phản ứng nếu vị trí chính xác của các Sự kiện này đã được biết đến. Ngoài ra, trong bất kỳ WSN, các thông tin vị trí của nút đóng một vai trò quan trọng trong việc tìm hiểu bối cảnh ứng dụng. Có ba ưu điểm nhìn thấy để biết thông tin vị trí của các nút cảm biến. Đầu tiên, thông tin vị trí là cần thiết để xác định vị trí của một sự kiện quan tâm. Ví dụ, vị trí của một kẻ xâm nhập, vị trí của một tín hiệu dẫn đường, hoặc vị trí của xe tăng đối phương trên chiến trường là cực kỳ quan trọng cho việc triển khai cứu hộ và cứu trợ quân. Thứ hai, thông tin vị trí tạo điều kiện cho các ứng dụng dịch vụ, chẳng hạn như các dịch vụ hướng dẫn vị trí có đưa ra thông tin về các bác sĩ, thiết bị y tế, nhân viên trong một bệnh viện thông minh gần đó, ứng dụng giám sát mục tiêu. Thứ ba, thông tin vị trí có thể hỗ trợ chức năng hệ thống khác nhau, chẳng hạn như định tuyến địa lý kiểm tra sự phủ sóng của mạng, và các thông tin dựa trên truy vấn vị trí. Do đó, với những lợi thế và nhiều hơn nữa, việc các nút cảm biến tự nhận biết vị trí của nó trở thành tiêu chuẩn của nhà sản xuất trong WSNs ở tất cả các lĩnh vực ứng dụng cung cấp dịch vụ dựa trên vị trí.

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. Một khi bị bắt, một nút có thể trở thành kẻ thù. Hiện tại đối thủ có thể làm xáo trộn các nút cảm biến bằng cách tiêm mã độc hại, buộc nút hoạt động sai lệch, chiết các thông tin mã hóa được tổ chức bởi các nút để bỏ qua rào cản an ninh như xác thực và xác minh,... Mặt khác, các đối thủ có thể khởi động các cuộc tấn công từ bên trong hệ thống như là một tên gián điệp, và hầu hết các hệ thống hiện có sẽ thất bại khi đối mặt với các cuộc tấn công bên trong nó.

1.1.2 Vấn đề an ninh trong WSN

Các dạng tấn công

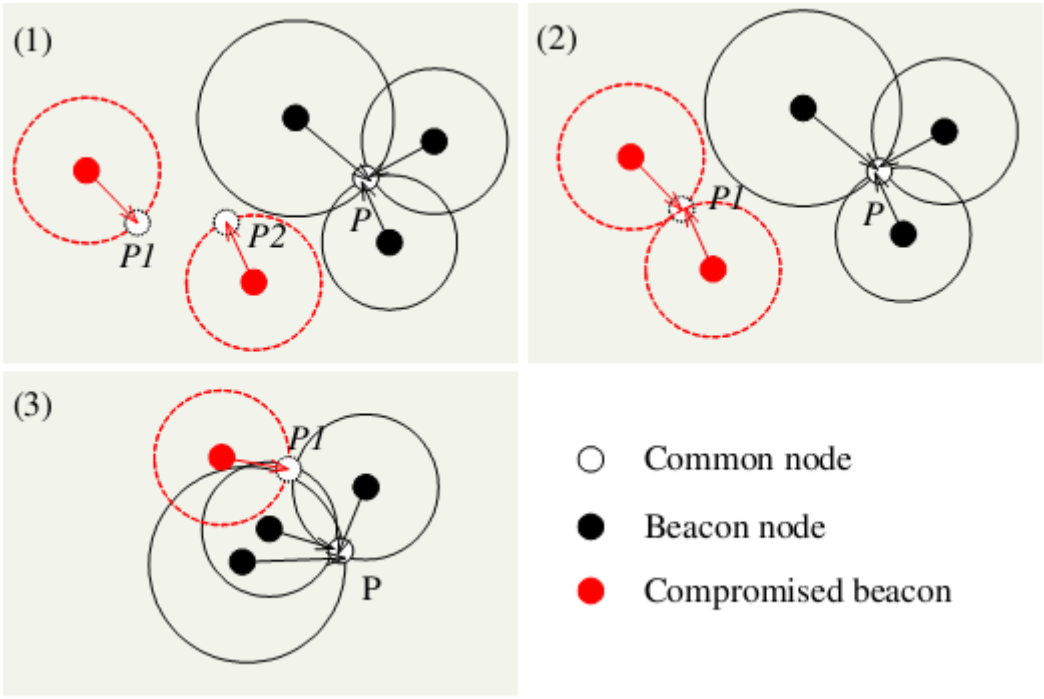
Nhiều cuộc tấn công có thể được đưa ra trong hệ thống định vị và hệ thống xác minh thông tin vị trí.

- ***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. Trong trường hợp bước nhảy đơn, nếu phép đo được dựa trên RSSI, kẻ tấn công có thể tăng hoặc giảm công suất truyền của người gửi khi người gửi đang bị tổn hại (khi người gửi là một nút bình thường, kẻ tấn công có thể đưa tín hiệu của nó và phát lại với sức mạnh truyền tải thấp hơn hoặc cao hơn). Nếu đo lường là dựa trên ToA và TDoA, kẻ tấn công có thể trì hoãn việc truyền tải các gói dữ liệu. Trong trường hợp đa bước nhảy, để làm sai lệch phạm vi đo, những kẻ tấn công có thể làm giảm hoặc tăng số lượng bước nhảy trong hệ thống DV-hop, và làm giảm hoặc tăng khoảng cách trong mỗi bước nhảy đơn trong các hệ thống DV-distance [2]. Lưu ý rằng cuộc tấn công này có ảnh hưởng trên cả hai hệ thống định vị và hệ thống xác minh vị trí. Ví dụ, làm giảm phạm vi đo lường giữa nút A và B có thể bóp méo các vị trí ước tính của B nếu A là một nút Anchor, và cũng có thể làm cho sai một tin mà B có trong một khu vực nhất định nếu A là một Virtual Center (VC).
- ***Sự mạo danh***: Trong cuộc tấn công này, kẻ tấn công đóng vai các nút khác trong mạng. Ví dụ, trong hệ thống định vị, những kẻ tấn công có thể mạo

danh các nút Anchor để phát sai thông tin vị trí. Trong các hệ thống xác minh vị trí, kẻ tấn công có thể mạo danh một nạn nhân để thực hiện các xác minh tin rằng nhân chứng là ở vị trí của kẻ tấn công. Tấn công này có thể bị đánh bại bằng cách xác thực.

- ***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 – một hố - và phát lại thông tin [3]. Những kẻ tấn công có thể trực tiếp thực hiện tấn công (tức là, tiếp nhận và phát lại các gói tin với đài tin và đường hầm theo một kênh riêng), hoặc khởi động với hai nút bị tổn hại (ví dụ, một tiếp nhận và một cho phát lại, các đường hầm là hoàn thành bằng cách định tuyến trong WSN). Các cuộc tấn công replay là để cố đợi nghe các gói tin (ví dụ, các gói tin chuyển tiếp nghe từ đèn hiệu), có thể được coi là một cuộc tấn công zero-wormhole với đường hầm dài. Trong hệ thống định vị, tấn công lỗ sâu làm cho tín hiệu dẫn đường xuất hiện tại nơi khác và làm cho các thông tin thu thập được đưa vào định vị sai. Trong các hệ thống xác minh vị trí, các cuộc tấn công chuyển các gói tin của nạn nhân đến địa điểm khác và làm cho người xác minh tin rằng là nó ở vị trí giả.
- ***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). Kẻ tấn công có thể thay đổi vị trí một phần tham chiếu trong toàn bộ vị trí tham chiếu. Theo mức độ thông minh, các cuộc tấn công có thể được phân thành ba loại: thiếu sự phối hợp các cuộc tấn công, tấn công thông đồng, và các cuộc tấn công gây ô nhiễm. Kịch bản này được thể hiện trong hình 1. Trong các cuộc tấn công không được điều phối, vị trí tham chiếu khác nhau để đánh lừa nút thông thường đến các vị trí giả

khác nhau. Trong cuộc tấn công thông đồng, tất cả các vị trí tham chiếu giả mạo để đánh lừa các nút thông thường, ngẫu nhiên nhưng cùng vị trí sai. Cuộc tấn công này là mạnh hơn, tuy nhiên nó là vẫn có thể bị đánh bại khi vị trí tham chiếu bình thường là số đông. Trong cuộc tấn công gây ô nhiễm, tất cả các vị trí tham chiếu giả mạo để đánh lừa các nút chung với một vị trí đặc biệt được chọn là sai, điều này cũng phù hợp với thành phần bình thường của vị trí tham chiếu. Cuộc tấn công này là một trong những trường hợp mạnh nhất, nó có thể xác định thành công vị trí ngay cả khi tham chiếu bình thường là đa số.



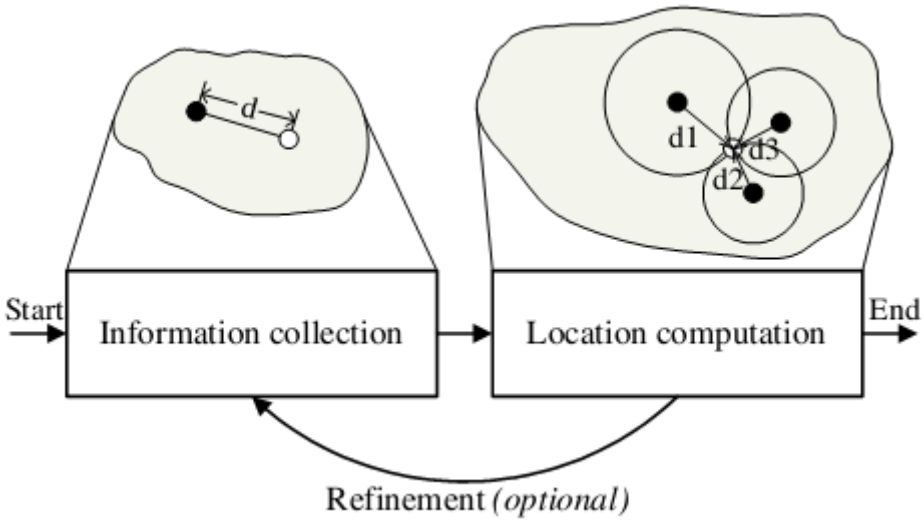
Hình 1. Ba kiểu của tấn công tham chiếu vị trí: (1) uncoordinated, (2) collusion, và (3) pollution attacks. Trong hình chỉ P là vị trí thực.

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:

- Thu thập thông tin: Các thông tin cho định vị được thu thập, trong đó có thể bao gồm các kết nối, khoảng cách và góc độ, cũng như các vị trí thông báo. Khoảng cách giữa các nút trong bước nhảy đơn có thể được đo bằng chỉ số nhận cường độ tín hiệu (RSSI), thời gian đến (ToA), hoặc thời gian khác nhau khi đến (TDoA); khoảng cách giữa các nút đa bước nhảy có thể được đo bằng phương pháp DV-hop hoặc DV-khoảng cách [2]. Các góc có thể được đo bằng góc đến (AoA).
- Sự tính toán định vị: Các địa điểm được tính toán với các thông tin thu thập được. Nhiều thuật toán đã được đề xuất. Các thuật toán đơn giản bao gồm trilateration, multilateration, và triangulation. Ngoài ra, các thuật toán phức tạp hơn cũng được đề xuất, ví dụ như, MDS-MAP cho định vị toàn bộ mạng và RobustQuad để đối phó với các phép đo nhiễu.



Hình 2 Sự định vị của các nút cảm biến

Các bước lọc tùy chọn là cho máy tính lặp đi lặp lại vị trí với các vị trí mới được tính (ví dụ, các nút được định vị sẽ trở thành các nút Anchor mới [7]) hoặc với phương pháp tính toán mới (ví dụ, trong [3], [4], phương pháp mới sẽ được thực thi sau khi có vị trí nút ban đầu).

Các hệ thống định vị có thể được phân thành nhiều loại dựa trên miền phạm vi tự do. Trong các hệ thống dựa vào khoảng cách thì khoảng cách hoặc góc giữa các nút cần phải được đo trong bước thu thập thông tin. Hệ thống Range-free không yêu cầu như vậy. Do đó, các hệ thống miền phạm vi tự do thường không yêu cầu bất kỳ

phần cứng bổ sung. Các hệ thống định vị cũng có thể được phân loại dựa vào nút trung tâm và cơ sở hạ tầng trung tâm. Trong các hệ thống cũ các nút cảm biến tự tính toán vị trí của chúng.

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.

Mô hình đối thủ trong định vị an toàn được mô tả: Mục tiêu của kẻ thù là làm cho các nút (ví dụ, tại nút định vị trung tâm) hoặc trong sở hạ tầng (tức là, trong cơ sở hạ tầng trung tâm định vị) có vị trí ước tính sai. Kẻ thù có thể thỏa hiệp với các nút (bao gồm cả các nút thông thường và các cảnh báo).

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. Nếu hệ thống định vị có trạm cơ sở hạ tầng trung tâm, cơ sở hạ tầng sẽ tin tưởng các vị trí dự toán, bởi vì vị trí được tính bằng cách riêng của mình (các vị trí cũng có thể không chính xác, nhưng đảm bảo sự định vị là duy nhất nó có thể làm). Tuy nhiên, nếu hệ thống định vị có nút trung tâm, các cơ sở hạ tầng sẽ không chỉ đơn giản là tin tưởng các vị trí dự toán. Bởi vì ngay cả các địa điểm thu được thông qua định vị an toàn, các nút có thể bị tổn hại và cố ý báo cáo sai vị trí. Việc thêm phần cứng chống giả mạo cho các vị trí báo cáo một cách trung thực là một cách tiếp cận mới; Tuy nhiên nó sẽ làm tăng chi phí của các nút và được chứng minh có vấn đề trong thực tế.

Vì vậy, khi hệ thống định vị trí có nút trung tâm thì xác minh vị trí là cần thiết để xác minh các địa điểm tuyên bố của cảm biến. Trong các hệ thống xác minh vị trí, các nút cảm biến được xác nhận gọi là *nhân chứng* và các nút có cơ sở hạ tầng được gọi là *người xác minh*. Chúng tôi lưu ý rằng trong một số kịch bản để xác minh rằng các nút cảm biến bên trong một khu vực nhất định (nhưng không chính xác tại một vị trí) là đủ. Ví dụ, xác minh rằng một nút nằm bên trong một quán cà phê để

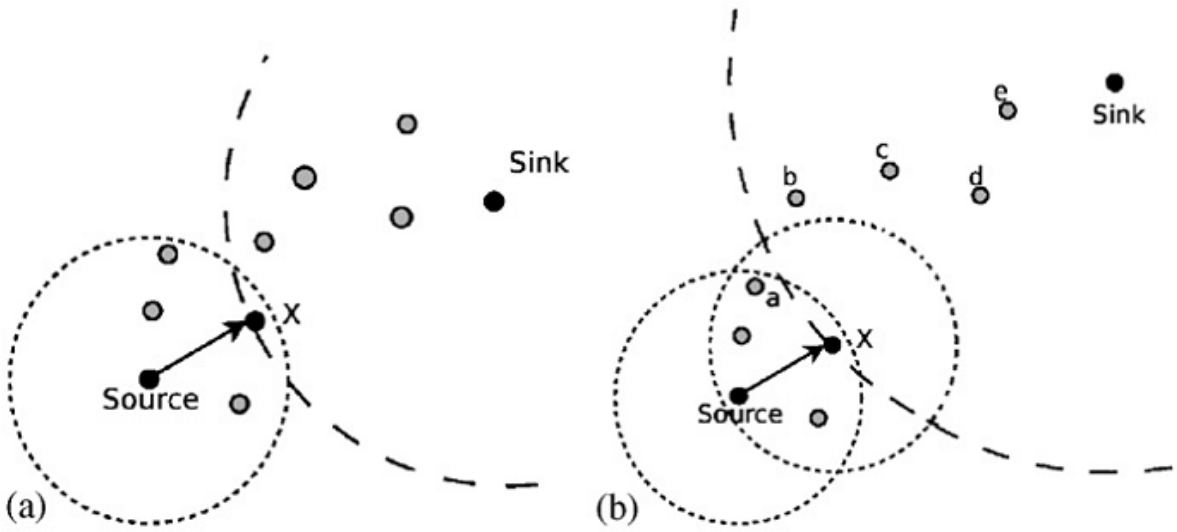
đánh giá trình độ chuyên môn cho một số dịch vụ. Dưới đây là mô tả ngắn gọn các mô hình đối thủ trong xác minh vị trí.

Mô hình đối thủ: Mục tiêu của kẻ thù là làm cho việc xác minh không thành công. Tức là, tuyên bố vị trí đúng từ các nhân chứng bình thường được xác nhận là không chính xác và bị từ chối, nhưng tuyên bố vị trí sai từ các nhân chứng bị xâm nhập là xác nhận chính xác và được chấp nhận.

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.

GR không phải lúc nào cũng thành công trong pha tham lam như mô tả ở trên. Khi một nút chuyển tiếp, ví dụ nút X trong hình 3(b) không có hàng xóm trong một bước nhảy gần với sink hơn nó, nó có thể không tiếp tục chuyển tiếp gói tin đó nữa.

Kết quả là, gói tin bị mắc kẹt trong một phạm vi nhất định, nơi mà FS là rỗng thì được gọi là một khoảng trống. Trong trường hợp như vậy, thường có một cơ chế bổ sung (ví dụ, định tuyến bề mặt hoặc quay lui về phía beacon được sử dụng để định tuyến xung quanh một khoảng trống và càng nhiều những tối ưu. Vì ngày càng có nhiều và nhiều những ứng dụng dựa trên GR được đề xuất nên sự an toàn của GR càng trở nên cấp thiết hơn.

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 [4] [1] [3] đề xuất, tuy nhiên khi áp dụng vào trong giải thuật GPSR thì chỉ có [5] đề cập qua và cũng trên quan điểm dựa theo nguyên tắc triangulation [6] 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 [5] còn bỏ ngỏ. Nói cách khác, trong thuật toán định tuyến GPSR mà [5] 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.

Để ngăn chặn việc làm sai lệch thông tin vị trí tới các nút cảm biến, Sastry đã đề xuất một kế hoạch xác minh vị trí [1] mà trong đó các nút cảm biến cần phải gửi yêu cầu vị trí của mình cho một người xác minh rằng chuỗi sau là một yêu cầu thách thức đối với nút. Khi nút nhận tín hiệu thách thức, nó ngay lập tức phải trả lời xác minh thông qua kênh siêu âm, với một khoảng thời gian đã bao gồm trong bản tin thách thức. Để xác minh vị trí, người xác minh đo độ trễ giữa các thách thức và phản hồi. Nó so sánh độ trễ đo được với độ trễ ước tính theo các vị trí được thông báo và tốc độ âm thanh. Tuy nhiên, phương pháp này đòi hỏi phần cứng đặc biệt, trong khi việc xác minh vị trí đã tuyên bố liên quan tới một người xác minh duy nhất. Hơn nữa, một phản hồi ngay lập tức luôn là không thể, ví dụ, do quá tải hoặc gói tin bị thất lạc. Kết quả là, các nút trung thực có thể được xác thực là không cần thiết.

Ke Liu [5] đề xuất một phương pháp khác để xác minh vị trí. Ý tưởng chính là để đảo ngược quá trình định vị như vậy một nút cảm biến không đáng tin cậy thì không được phép tạo ra ước tính vị trí riêng của nó. Kế hoạch đề xuất có thể được sử dụng cho các phương pháp định vị dựa trên tam giác bao gồm cả những người sử dụng tín hiệu vô tuyến (RSS), thời gian đến (ToA), thời gian khác nhau khi đến (TDoA) và AoA đã được thảo luận ở trên. Trong kế hoạch đề xuất, sự định vị được khởi tạo bằng việc có một bộ cảm biến truyền một yêu cầu định vị tới các nút Anchor trong vùng lân cận. Yêu cầu này được chấp nhận bởi nhiều nút Anchor (lớn hơn 3). Mỗi nút Anchor sản ra một khoảng cách ước tính (nếu sử dụng RSS hoặc TDoA) hoặc góc (nếu sử dụng AoA) dựa trên các yêu cầu nhận được từ nút cảm biến. Các Anchor trao đổi thông tin này với các nút khác để tạo ra một vị trí ước tính an toàn thông qua các tính toán tam giác. Vị trí ước tính sau đó được cung cấp cho các nút cảm biến kèm theo một chứng nhận. Như vậy các thông tin vị trí được chứng nhận có thể được trao đổi an toàn với các nút khác. Với cách này, có thể không cho phép một nút cảm biến không đáng tin cậy từ việc truyền thông tin vị trí sai. Ngoài

ra, chú ý rằng phương pháp tiếp cận của Ke Liu có thể được sử dụng để xác minh một vị trí ngay cả khi nó không được sử dụng thuật toán định vị bằng các nút cảm biến.

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. Ví dụ, khi RSS được sử dụng, khoảng cách được ước tính dựa trên cường độ tín hiệu đo được. Một nút có thể cố gắng để làm sai lệch bằng cách truyền một mức năng lượng thấp hơn hoặc cao hơn để xuất hiện gần nó hơn hay xa nó hơn. Một cuộc tấn công tương tự có thể cố gắng với một kế hoạch định vị TDoA cơ sở trong đó một nút là cần thiết để truyền tải một RF và một xung siêu âm. Một nút độc hại có thể cố gắng tấn công bằng cách gửi các xung siêu âm RF vào những thời điểm khác nhau. Khi AoA được sử dụng cho sự định vị, các thao tác truyền tín hiệu có thể là khó khăn như một nút không thể ngụy trang góc tới nút khác trừ khi nó có ăngten thông minh.

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. Các hướng truyền có thể được thiết kế để được nhận bởi một hoặc nhiều tín hiệu, nhưng không phải là những nút khác. Có hai phiên bản của cuộc tấn công này: đồng thời và tuần tự. Trong nhiều phiên bản tuần tự, các gói tin định vị khác nhau được gửi một cách trực tiếp tới các nút định vị khác nhau vào cùng một thời điểm. Tấn công này có thể được ngăn chặn bằng cách đồng bộ các Anchor định vị với sự chấp nhận được về chiều dài một gói tin Beacon. Các nút định vị có thể phát hiện sự chênh lệch thời gian của đồng hồ mà đang có trong các tấn công nối tiếp. Các phiên bản đồng thời xử lý bằng việc truyền nhiều yêu cầu cùng lúc và trực tiếp, sử dụng sóng vô tuyến tới các nút định vị khác nhau. Trong khi tấn công này không thể phát hiện dựa trên

sự chênh lệch đồng hồ, mức xác thực MAC có thể được sử dụng để phát hiện việc truyền phát từ các tín hiệu radio khác nhau.

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. Hiệu quả của cuộc tấn công loại này có thể được làm giảm bằng cách yêu cầu các nút cảm biến có các Anchor định kỳ đổi chứng nhận của chúng với chi phí định vị được tăng lên so với trước. Ngoài ra, các nút tin cậy như các nút vị trí có thể lấy mẫu truyền tin của các nút không tin cậy và ước lượng khoảng cách của các nút này với chính nó. Việc làm cho tương thích khoảng cách ước tính này với vị trí tuyên bố của nút có nhiều điểm thuận lợi như có thể cung cấp phát hiện động các tấn công di động. Trong một cuộc tấn công có liên quan khác, một nút có thể có được một vị trí được xác nhận và vượt qua nó tới một nút khác thông qua một kênh phát ngược trở lại. Tấn công này có thể được bảo vệ thông qua xác thực hoặc các cơ chế phòng vệ khác được nêu ở trên.

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. Chúng tôi giả định phạm vi giao tiếp tất cả các cảm biến có cùng bán kính. Mỗi bộ cảm biến truyền ID của nó trong phạm vi giao tiếp của mình, và tình cờ nghe một cách thụ động ID của cảm biến khác. Chúng tôi nói cảm biến A có thể quan sát cảm biến B, nếu A có thể nhận được thông báo ID từ B. Chú ý rằng sự gián đoạn về môi trường và tồn tại hoán vị để quan sát

khu vực không phải là luôn luôn đối xứng. Ví dụ, cảm biến B có thể không quan sát cảm biến A trong khi A quan sát được B.

Chúng tôi xem xét cả hai mô hình tấn công thụ động và chủ động. Kẻ tấn công thụ động có thể nghe trộm thông tin liên lạc của cảm biến, hoặc tạo ra các wormhole [2] giữa hai cảm biến cách xa nhau. Do đó, các cảm biến sẽ nhầm lẫn tin rằng họ là những hàng xóm. Kẻ tấn công chủ động có thể thỏa hiệp cảm biến và gửi thông tin sai sự thật tới các hàng xóm. Hơn nữa, theo nguyên tắc của [7] giả định rằng những kẻ tấn công biết hệ thống xác minh, do đó họ có thể cố khởi động các cuộc tấn công khai thác sự yếu kém của hệ thống. Giả định duy nhất về kẻ tấn công trong một khu vực là những kẻ tấn công không lớn hơn so với những nút lành tính.

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 [8] [1] [9] và xác minh vị trí đơn [9] [7] .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* (đối với việc đánh bại các gian lận). Đầu tiên, *nhân chứng* (P) gửi một cam kết trên một chuỗi bít m_i để V xác minh (ví dụ, gửi giá trị băm, bởi một sự va chạm hàm băm, các chuỗi bít), và V chuẩn bị một chuỗi α_i. Thứ 2, mức thấp của khoảng cách biên thay đổi bắt đầu: V gửi bít α_i tới P, và P gửi bít $\beta_i = \alpha_i \oplus m_i$ tới V ngay sau khi anh ta nhận α_i. Thứ 3, P mở ra những cam kết và gửi chữ ký $sign(\alpha||\beta)$ tới V, và V tính một biên bên trên khoảng cách của nó tới P dựa trên thời gian trễ tối đa giữa việc gửi đi một bít α_i và nhận bít β_i trở lại. khoảng cách biên như vậy sử dụng tín hiệu RF (tần số Radio) yêu cầu phần cứng chuyên dụng (vì chúng ta cần phải đo thời gian với sự chính xác nano giây).

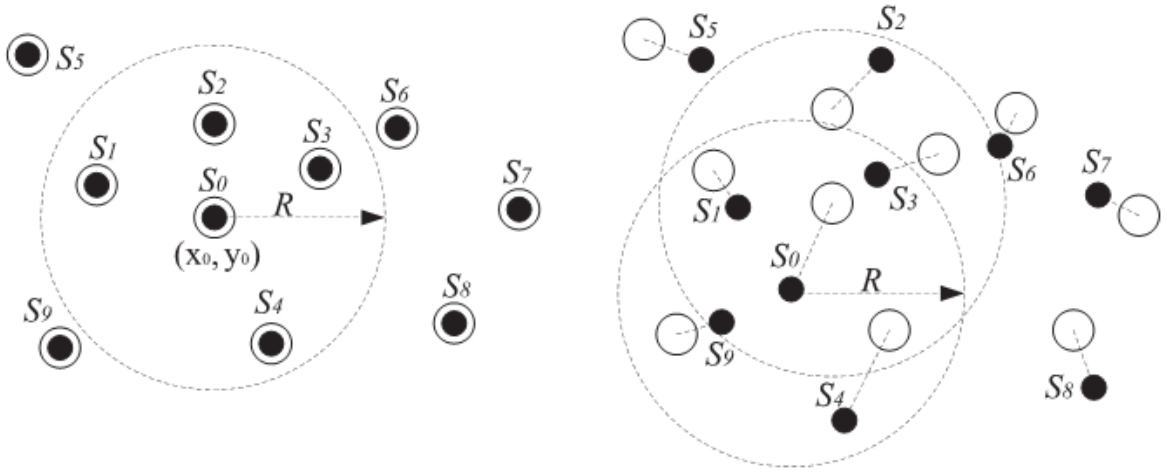
Vora đề xuất một phương pháp mới để đạt được cùng một mục tiêu như [10]. Họ chia người xác minh vào *acceptors* và *rejectors*. Các *acceptor* được triển khai

trong khu vực bảo vệ và *rejectors* được triển khai tại ranh giới của khu vực. Quá trình xác minh theo từng bước bắt đầu khi nút nhân chứng tăng cường độ tín hiệu của nó và phát đi một tín hiệu, cho đến khi một nút xác minh nghe tín hiệu và phản ứng. Các nút xác minh chấp nhận các *nhân chứng* nếu không có bất kỳ *rejectors* nào nghe thấy nó trong quá trình này.

Dưới đây,chúng tôi nghiên cứu hai thuật toán có thể thực hiện cho xác minh tại chỗ. Thuật toán đầu tiên được gọi là Greedy Filtering using Matrix (GFM - Lọc tham lam sử dụng ma trận). Thuật toán thứ hai được đặt tên là Greedy Filtering using Trustability-indicator (GFT- Lọc tham lam sử dụng chỉ số tin cậy). Cả hai thuật toán không sử dụng thống nhất các vị trí được ước tính của cảm biến và quan sát xung quanh. Các số liệu này có thể được sử dụng trong các tình huống khác nhau theo yêu cầu của ứng dụng.

2.4.1.1. Thuật toán lọc tham lam sử dụng ma trận - GFM

Trong phần này, chúng tôi sẽ thảo luận về các thuật toán xác minh GFM. Bước đầu tiên trong quá trình xác minh, mỗi bộ cảm biến phát sóng ID của nó trong phạm vi giao tiếp và khi đó nó cũng nghe được các ID của các cảm biến khác. Như một ví dụ, hình. 5a cho thấy một kịch bản mà cảm biến được định vị một cách chính xác không có sai số định vị. Các vòng tròn đậm và các vòng tròn rỗng biểu diễn tương ứng các nút cảm biến đúng và các vị trí được ước tính. Vị trí đúng của nút cảm biến S_0 là $L = (x_0, y_0)$ và phạm vi truyền của nó là vòng tròn nét đứt lớn. Bởi vì các nút cảm biến S_1, S_2, S_3, S_4 có trong phạm vi truyền của nút cảm biến S_0, các thông điệp ID của chúng có thể được truyền đến S_0. Do đó, việc quan sát khu vực của nút cảm biến S_0 là $O_0 = (S_1, S_2, S_3, S_4)$. Sau đó mỗi nút cảm biến gửi quan sát khu vựcvà các ước tính vị trí tới VC. VC sẽ phân tích tất cả thông tin thu thập được từ các nút cảm biến và phát hiện nếu ở đây có bất kỳ một sự không phù hợp nào.



Hình 5. Ảnh chụp một khu vực các nút cảm biến

Trực giác là khi các cảm biến được định vị một cách chính xác với các lỗi định vị nhỏ, thì mỗi quan sát khu vực của họ nên phù hợp với các vị trí được ước tính. Ví dụ, trong hình 5a tất cả các cảm biến được định vị với lỗi ZERO. Khoảng các giữa vị trí được ước tính và S_1 là nhỏ hơn bán kính R, cái mà phù hợp với thực tế là họ có thể quan sát mỗi nút khác. Dựa vào trực giác này, thuật toán GFM tổ chức tất cả thông tin trong ma trận để tìm thông tin mâu thuẫn.

a. Xây dựng ma trận

Giả sử có tất cả n nút cảm biến trong khu vực này được ký hiệu bởi $S_1, \dots, S_n$. Để thuận tiện, chúng tôi giả định cảm biến S_i là số nguyên i trong đó $i \in \{1, \dots, n\}$. Trong thuật toán GFM, 5 ma trận hình vuông $n \times n$ được tính dựa trên thông tin được báo cáo từ các cảm biến.

- *Ma trận quan sát (Observation)*. Ma trận này được tính bằng việc sử dụng các quan sát khu vực của nút cảm biến. Các phần tử trong ma trận này là 1 hoặc 0 phụ thuộc vào vị trí các cảm biến có thể quan sát cảm biến khác, cụ thể là

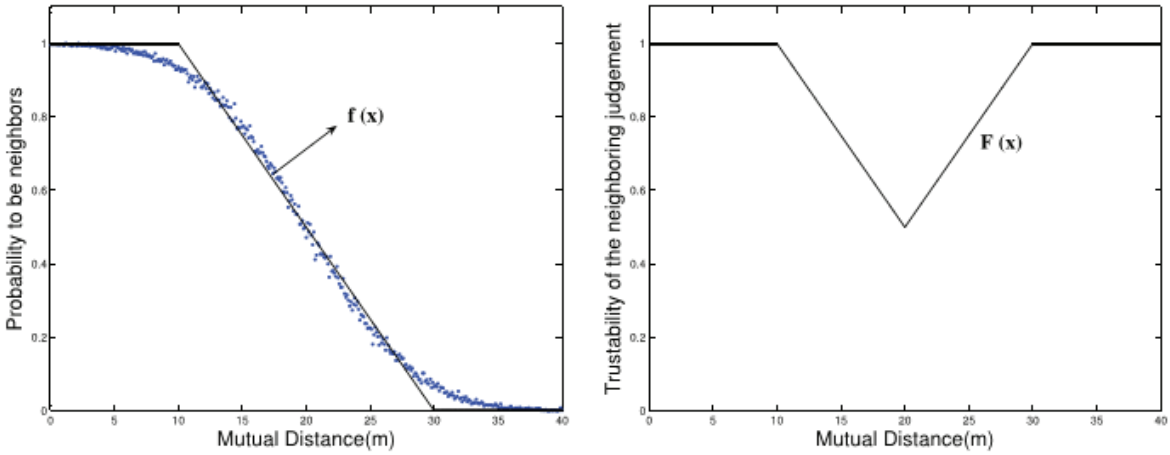
$$M_o(i,j) = \begin{cases} 1, nếu\ nút\ cảm\ biến\ S_i\ quan\ sát\ thấy\ S_j \\ 0, ngược\ lại \end{cases} \quad (2)$$

Trong đó, $i, j \in \{1, \dots, n\}$ là chỉ số hàng và cột. Chú ý do sự gián đoạn về môi trường mà hai bộ cảm biến không thể quan sát nhau ở cùng một thời gian nên ma trận M_0 không phải là một ma trận đối xứng.

- *Ma trận ước lượng (Estimation)*. Ma trận này được tính bằng việc sử dụng các vị trí được ước tính của nút cảm biến. Nếu khoảng cách giữa các vị trí được ước tính của S_i và S_j là nhỏ hơn R, bán kính của phạm vi truyền, thì phần tử ở hàng i và cột j sẽ là 1, ngược lại, nó sẽ là 0, cụ thể:

$$M_e(i,j) = \begin{cases} 1, nếu\ d_{ij} \leq R \\ 0, nếu\ d_{ij} > R \end{cases} \quad (3)$$

Trong đó d_{ij} biểu diễn khoảng cách giữa các vị trí được ước tính của các cảm biến S_i và S_j.



(a) Statistical results (b) Weight function F(x)

Hình 6. Hàm trọng lượng

- *Ma trận khác biệt (Difference matrix)*. Ma trận này được tính bằng phép XOR giữa ma trận quan sát và ma trận ước tính.

$$M_d = M_o \bigoplus M_e \quad (4)$$

Trong đó $\oplus$ là ký hiệu biểu diễn phép toán XOR. Các phần tử *nonzero* trong ma trận này được tạo ra bởi sai số định vị của nút cảm biến. Ví dụ, khi $M_o(i,j) = 1$ và $M_e(i,j) = 0$ thì $M_d(i,j) = 1$. Trong ví dụ này, nút cảm biến S_i quan sát nút cảm biến S_j, mà ngụ ý khoảng cách giữa chúng vị trí đúng thực sự là trong phạm vi truyền sóng. Tuy nhiên vì sai số định vị, khoảng các giữa các vị trí được ước tính của chúng là lớn hơn bán kính phạm vi truyền. Hình 5b trình bày thêm các mâu thuẫn như vậy được tạo ra. Trong hình, các vị trí đúng của cảm biến được miêu tả như vòng tròn đặc đậm, và các vị trí được ước tính của họ được mô tả như những vòng tròn rỗng. Chúng ta có thể quan sát các vị trí được ước tính S_0 và S_2của phạm

vi truyền sóng, nhưng vị trí thực của chúng không như vậy, vì vậy chúng không thể quan sát lẫn nhau. Wei đã sử dụng ma trận M_d để phát hiện các sai số định vị lớn. Tuy nhiên trước đó, chúng ta cần nghiên cứu rằng khi cảm biến được định vị với các lỗi nhỏ (lỗi nhỏ hơn một sự bất thường mức D – anomaly degree), thì làm thế nào để thấy được sự không phù hợp trong ma trận M_d.

- *Ma trận trọng lượng*: Trong thử nghiệm này, Wei ngẫu nhiên triển khai 100 nút cảm biến trong khu vực, phạm vi truyền sóng của nút cảm biến là $R = 20m$ và sự bất thường chấp nhận được là $D = 10m$. Tất cả các cảm biến được định vị với các lỗi mà sự phân phối thống nhất trong phạm vi [0, 10m]. Sau đó, tính xác suất mà hai cảm biến nằm trong phạm vi giao tiếp, với khoảng cách giữa các vị trí được ước tính của S_i và S_j là d_{ij}. Kết quả được trình bày trong hình 6a, Wei quan sát thấy rằng khi d_{ij} phát triển từ 0 đến 40m, xác suất giảm từ 1 đến 0. Và biểu diễn những điểm phân tán bằng cách sử dụng một hàm đơn giản $f(x)$. Hơn nữa, chúng tôi lấy hàm khác $F(x)$ đặt tên là hàm trọng lượng (weight function) bằng việc sử dụng $f(x)$

$$F(x) = \begin{cases} f(x), nếu\ x \le R, \\ 1 - f(x), nếu\ x > R \end{cases} (5)$$

Như đã biểu diễn trong hình 6b, giá trị của hàm $F(x)$ chỉ ra xác suất mà bộ cảm biến báo cáo thông tin là phù hợp. Một cách chính xác hơn khi $x = d_{ij}$ là lớn hơn (nhỏ hơn) $R = 20m$, $F(x)$ là xác suất khoảng cách giữa các vị trí thực sự của chúng là lớn hơn (nhỏ hơn) R. Chúng tôi cũng có thể xem xét các giá trị của $F(x)$ như là trọng lượng của sự phù hợp và có được ma trận M_w bằng việc sử dụng hàm trọng lượng, cụ thể là:

$$M_w(i,j) = F\left(d_{ij}\right), (6)$$

Trong đó $i, j \in \{1, 2, \dots, n\}$ và d_{ij} là khoảng cách giữa các vị trí được ước tính S_i và S_j.

- *Ma trận mâu thuẫn (Inconsistency matrix)*. Chúng tôi nhân mỗi phần tử trong ma trận khác biệt với phần tử tương ứng trong ma trận trọng lượng, và có được ma trận mâu thuẫn M_{inc}

$$M_{inc} = M_d \bigodot M_w, (7)$$

Trong đó ⊙ biểu thị phép nhân ma trận. Chúng tôi sử dụng ma trận này để lọc tham lam các vị trí mà là nguyên nhân gây ra mâu thuẫn lớn hơn các vị trí khác. Chú ý rằng với một cảm biến S_i trong đó $i \in \{1, 2, \dots, n\}$, những mâu thuẫn được mang bởi nút cảm biến này được biểu diễn bởi các phần tử *nonzero* trong hàng thứ i và cột thứ i của ma trận M_{inc}. Trên đây chúng tôi định nghĩa một vài số liệu mà được sử dụng trong quá trình lọc.

b. Số liệu cho việc lọc các vị trí bất thường

- *Số liệu về hoạt động khác biệt*

$$AD_i = \sum_{k=1}^{n} M_{inc}(i,k), \ (8)$$

Trong đó $i \in \{1, 2, \dots, n\}$. Với 1 cảm biến S_i, số liệu AD_i là tổng các phần tử trong hàng thứ i của ma trận M_{inc}. Số liệu này định lượng sự không thống nhất giữa quan sát khu vực của cảm biến S_i và các vị trí được ước tính.

- *Số liệu khác biệt động (Passive Difference Metric)*

$$PD_i = \sum_{k=1}^{n} M_{inc}(k,i), \ (9)$$

Trong đó $i \in \{1, 2, \dots, n\}$. Với 1 cảm biến S_i, số liệu PD_i là tổng các phần tử trong cột thứ i của ma trận M_{inc}. Số liệu này định lượng sự không thống nhất giữa sự quan sát của các cảm biến trên S_i (cụ thể, nút cảm biến S_i được quan sát một cách bị động) và các vị trí được ước tính của các cảm biến.

- *Số liệu không đối xứng (Asymmetry Metric)*

$$AS_i = \sum_{k=1}^{n} |M_{inc}(i,k) - M_{inc}(k,i)|, (10)$$

Trong đó $i \in \{1, 2, \dots, n\}$. Trong môi trường không tấn công các quan sát của cảm biến không đối xứng do xáo trộn môi trường. Tuy nhiên, nếu không đối xứng như vậy là lớn hơn một ngưỡng (một trường hợp cực đoan là một bộ cảm biến có thể quan sát tất cả các hàng xóm của nó, nhưng không ai trong số những hàng xóm có thể quan sát thấy nó), thì đó có thể là một sự giả mạo.

- *Số liệu hàng xóm phù hợp*

$$CN_i = \sum_{k=1, k\neq i}^{n} M_o(k,i) \times M_e(k,i), (11)$$

Trong đó $i \in \{1, 2, \ldots, n\}$. Số liệu này đếm số hàng xóm phù hợp của một bộ cảm biến. Ở đây, chúng ta xác định một cảm biến S_k là một hàng xóm phù hợp của cảm biến S_i, nếu nó có thể quan sát S_i và nó ước tính vị trí có trong phạm vi giao tiếp của vị trí được ước tính S_i.

c. Thủ tục lọc tham lam

Trong mục này, chúng tôi mô tả các thuật toán GFM tính toán tất cả ma trận trên và sử dụng các số liệu lọc để lọc một cách tham lam các vị trí bất thường.

Thuật toán lọc tham lam theo ma trận GFM

Tính toán ma trận M ;
Tính toán tham số AD, PD, AS cho tất cả các sensor;
While(sensor Si tồn tại có thể kiểm tra)
If ADi > AD – threshold
Loại Sk có ADk lớn nhất
Else if Pdi > PD – threshold
Loại Sk có PDk lớn nhất
Else if ASi < AS – threshold
Loại Sk có ASk lớn nhất
Thiết lập giá trị 0 cho vị trí thứ k (hàng, cột) ở ma trận Me, Mo, Minc
Tính toán lại AD, AS, PD cho tất cả các sensor
While (sensor Si có điều kiện thỏa mãn CNi < CN – threshold)
Loại bỏ các Si nếu nó không đủ điều kiện có đủ số láng giềng cần thiết
Kiểm tra lại danh sách các sensor còn lại mà không bị loại bỏ.

Hình 7. Thuật toán GFM

Thủ tục được thể hiện trong hình 7. Ở vòng đầu tiên, VC tính ma trận M_{inc} và các số liệu AD_i, PD_i và AS_i cho tất cả $i \in \{1, 2, \ldots, n\}$. Nếu có bất kỳ cảm biến có giá trị số liệu vượt quá ngưỡng của số liệu này, VC thu hồi các cảm biến có giá trị số liệu lớn nhất (gọi là nút S_k), và tập tất cả các zero ở hàng thứ k và cột thứ k trong các ma trận M_e, M_o và M_{inc}. Quá trình này lặp đi lặp lại cho đến khi không có các cảm biến nhiều hơn có thể được lọc ra. Sau đó số liệu CN_i được xem xét:

các cảm biến mà không có đủ số hàng xóm phù hợp thì bị thu hồi. Cuối cùng, các cảm biến còn lại được chấp nhận bởi VC như là các cảm biến được định vị một cách chính xác.

Trong thủ tục trên, ngưỡng cho số liệu khác nhau có thể được thu hồi thông qua đào tạo bằng việc sử dụng dữ liệu thử nghiệm. Trong mô phỏng của Wei, việc triển khai các cảm biến ngẫu nhiên trong một khu vực hình vuông và khoanh vùng chúng với ít lỗi hơn mức độ bất thường. Sau đó Wei tính toán tất cả các ma trận và các giá trị của AD_i, PD_i, AS_i và CN_i cho tất cả các cảm biến. Giá trị ngưỡng được xác định theo mong muốn tỷ lệ cảnh báo sai. Ví dụ, nếu ứng dụng đòi hỏi tỷ lệ cảnh báo sai nên được nhỏ hơn 5%, sau đó, thiết lập các ngưỡng cho số liệu AD, PD và AS ở 95% và ngưỡng cho số liệu CN ở 5%. Với giá trị của bán kính phạm vi truyền, mật độ nút, tính chính xác của các thuật toán định vị được sử dụng trong khu vực và các tham số môi trường, chúng ta có thể xây dựng các thí nghiệm cho phù hợp và có được các giá trị trên ngưỡng.

2.4.1.2 Lọc tham lam sử dụng chỉ số tin cậy – GFT

Trong phần này, chúng ta thảo luận về các thuật toán xác minh GFT. Trong Thuật toán GFT, VC tính một chỉ số cho khả năng tin cậy mỗi bộ cảm biến và cập nhật giá trị của chỉ số trong nhiều lần. Trong mỗi vòng, nếu chỉ số của cảm biến là cao hơn ngưỡng, các cảm biến được chấp nhận như là một vị trí chính xác của cảm biến. Lặp đi lặp lại như vậy dừng lại khi chỉ số tất cả các cảm biến ổn định. Cuối cùng, các cảm biến có chỉ số giá trị thấp hơn ngưỡng được phát hiện và thu hồi.

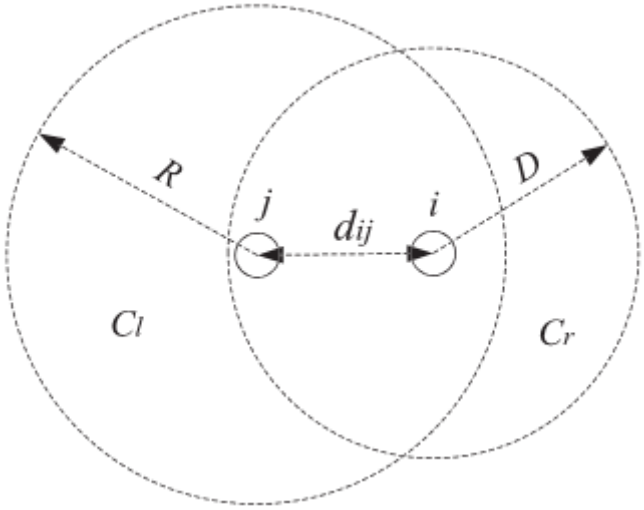
a. Tính chỉ số cho khả năng tin cậy

Chỉ số tin cậy của cảm biến S_i ($i \in \{1,2,..,n\}$) được tính trong nhiều cận. Ban đầu, tất cả các chỉ số được thiết lập từ 0.5 tới cận 0. Trong cận $k > 0$, chỉ số của cảm biến S_i được ký hiệu bởi I_i^k và được tính:

$$I_i^k = \frac{\sum_{S_j \in N_i} T_{ij}^k . I_j^{k-1}}{\sum_{S_j \in N_i} I_j^{k-1}} \quad (12)$$

Trong đó N_i biểu thị tập các nút cảm biến có thể quan sát cảm biến S_i. Với mỗi cảm biến S_j trong tập này, ký hiệu I_j^{k-1} biểu thị chỉ số của S_j ở vòng trước. vì vậy, thực sự I_i^k được tính bằng bình quân các chỉ số của tất cả các chỉ số của hàng xóm

trong vòng trước. Trong đó, trọng lượng T_{ij}^{k} được tính dựa trên mối quan hệ địa lý giữa S_i và S_j. Trong phần sau, chúng ta thảo luận làm thế nào để tính trọng lượng phụ thuộc vào cảm biến S_j có là một hàng xóm của S_i.



Hình 8. Tính toán chỉ số tạm thời

b. Tính toán của trọng lượng

Mỗi cảm biến có thể quan sát S_i, nếu các vị trí được ước tính có trong phạm vi truyền của vị trí được ước tính của S_i, sau đó cảm biến này được xem xét là một hàng xóm phù hợp; ngược lại nó được coi là một hàng xóm không phù hợp.

- *Tính trọng lượng bằng việc sử dụng hàng xóm phù hợp*. Chúng ta thảo luận làm thế nào để tính T_{ij}^{k} bằng việc sử dụng một hàng xóm phù hợp. Như đã biểu diễn trong hình 8, khoảng cách giữa các vị trí được ước tính của cảm biến S_i và S_j là d_{ij}; R là bán kính của phạm vi truyền; D là sự bất thường chấp nhận được. việc xác minh nơi mà lỗi vị trí của cảm biến S_i nhỏ hơn D bằng cách xác minh vị trí đúng của S_i trong vòng C_r. Do đó, chúng ta tính được xác suất sau đây:

$$P(S_i \in C_r) = P(S_i \in C_r | S_i \in C_l).P(S_i \in C_l) + P(S_i \in C_r | S_i \notin C_l).P(S_i \notin C_l)$$
$$\approx P(S_i \in C_r | S_i \in C_l).P(S_i \in C_l) = (S_o/S_l).f(d_{ij}), \quad (13)$$

Trong đó sự xấp xỉ sau vì xác suất có điều kiện $P(S_i \in C_r | S_i \notin C_l)$ là rất nhỏ. S_0 biểu diễn diện tích của khu vực đang chồng chéo, và S_l biểu thị diện tích của đường tròn C_l. Hàm $f(x)$ là hàm được xác định trong hình 6a. Bởi vì các hàng xóm phù hợp giúp nâng cao khả năng tin cậy của cảm biến S_i, chúng ta tăng chỉ số trước của S_i bằng tổng trong (13) và lấy thêm trọng lượng T_{ij}^{k} như sau:

$$T_{ij}^{k} = I_i^{k-1} + P(S_i \in C_r). (14)$$

- *Tính trọng lượng bằng cách sử dụng các hàng xóm không phù hợp*. Chúng ta tính xác suất mà nút S_i có thể không được xác minh, cụ thể là, xác suất mà vị trí đúng của nút cảm biến S_i nằm ngoài vòng tròn C_r trong hình 8

$$P(i \notin C_r) = 1 - (S_o/S_l). f(d_{ij}). (15)$$

Để đối diện của các hàng xóm phù hợp, các hàng xóm không phù hợp nên làm giảm khả năng tin tưởng của vị trí nút cảm biến S_i, do đó, chúng ta giảm chỉ số trước của S_i bởi số liệu trong phương trình trên và tính trọng lượng như sau.

$$T_{ij}^{k} = \max\{I_i^{k-1} - P(S_i \notin C_r), 0\}. (16)$$

Trong mỗi vòng, các VC tính toán trọng lượng bằng cách sử dụng cả hai hàng xóm phù hợp và không phù hợp của một bộ cảm biến, sau đó cập nhật chỉ số của cảm biến sử dụng (12).

c. Thủ tục lọc tham lam

Khởi tạo giá trị tin cậy đặt cho tất cả các sensor trong mạng;
For k=1 to N
For mỗi sensor Si
Cập nhật giá trị tin cậy Si từ I(k-1) đến Ik
If Ik > threshold
Chấp nhận sensor Si và dừng update giá trị
If Ik – I(k-1) < 0.05
Dừng update giá trị tin cậy cho Si vòng tiếp theo
Kiểm tra các sensor với giá trị tin cậy lớn hơn ngưỡng quy định

Hình 9 Thuật toán GFT

Như thể hiện trong hình 9, trong mỗi vòng, các VC cập nhật mỗi chỉ số tin cậy của cảm biến, sau đó xác nhận cảm biến bất kỳ nếu chỉ số tin cậy của nó lớn hơn ngưỡng. Nếu chỉ số của cảm biến thay đổi với số lượng không đáng kể trong hai lần lặp liên tiếp, thì VC nhận ra rằng chỉ số đã hội tụ và dừng cập nhật giá trị của nó. Ngưỡng có thể thu được thông qua đào tạo về dữ liệu thực nghiệm. Chúng tôi chạy thuật toán GFT trong môi trường không tấn công và tính toán chỉ số cho tất cả các cảm biến. Sau đó, chúng tôi thiết lập các ngưỡng theo tỷ lệ báo động giả mong

muốn. Nếu tỷ lệ các báo động giả là 0,5 %, thì 99,5 % số nút cảm biến nên có chỉ số lớn hơn ngưỡng, cụ thể là, các ngưỡng sẽ được thiết lập với tỷ lệ phần trăm 0,5 % của tất cả các chỉ số thu được trong môi trường không tấn công.

2.4.1.3 Sự so sánh giữa các thuật toán GFM và GFT

Cả hai thuật toán dựa trên những mâu thuẫn giữa các mối quan hệ địa lý cảm biến theo vị trí tuyên bố của họ và những ngụ ý của các quan sát khu vực của mình. Tuy nhiên, hai thuật toán là khác nhau trong các số liệu mà chúng sử dụng và quá trình lọc.

Đầu tiên, GFM khám phá những mâu thuẫn trực tiếp bởi so sánh các yếu tố trong hai ma trận. Tức là, các ma trận ước tính và ma trận quan sát; trong khi GFT phát hiện bất thường vị trí gián tiếp dựa trên các chỉ số chỉ ra những mâu thuẫn. Thứ hai, các thuật toán GFM lọc ra các vị trí tồi ngay sau khi một trong những giá trị số liệu không được chấp nhận theo các ngưỡng. Cảm biến không thu hồi sẽ được xác nhận trong vòng cuối. Trong thuật toán GFT, thay vì những tuyên bố vị trí tốt được chấp nhận đầu tiên, và sau nhiều lần thì các chỉ số của cảm biến còn lại trở nên ổn định, các cảm biến với chỉ số dưới ngưỡng sẽ bị thu hồi. Bởi vì như vậy sự khác biệt, hiệu suất của chúng cũng khác nhau trong các tình huống nếu mức độ bất thường và tỷ lệ báo động sai là khác nhau. Trong kết quả mô phỏng của chúng tôi, chúng tôi sẽ cung cấp thêm phân tích và hướng dẫn để VC có thể lựa chọn các thuật toán phù hợp.

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 [6], [8], [7] và xác minh nút đơn [11], [12] .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. Bốn ma trận đại diện cho quan sát của hàng xóm và các hàng xóm này tính theo vị trí ước tính. Các tác giả cũng đề xuất bốn số liệu tính toán trên bốn ma trận đặc trưng cho cảm biến bất thường. Trong TI, một quá trình lặp đi lặp lại được chạy

để cập nhật các giá trị chỉ số của mỗi nút. Trong quá trình như vậy mỗi nút quan sát một nút i giá trị chỉ số tính toán từ các mối quan hệ địa lý đánh giá liệu các nút i có vị trí bất thường. TI nhận được Kết quả xác minh và dừng cập nhật các chỉ số của một nút nếu chỉ số của nó phát triển vượt quá ngưỡng hay hội tụ.

Trong [17] Hwang . đề xuất một thuật toán cho mỗi nút để phát hiện các nút ảo trong khu vực của mình. Ở đây, thuật toán chạy một quá trình cho mỗi lần nhất định. Trong mỗi lần chạy, đầu tiên các nút tạo ra một bản đồ vị trí sử dụng ngẫu nhiên hai hàng xóm phân biệt. Sau đó, trong mỗi bản đồ như vậy, tác giả tìm ra tập con phù hợp lớn nhất. Các phương pháp phát hiện kiểm tra mỗi nút cho dù phạm vi đo phù hợp với phạm vi tính toán sử dụng vị trí của nút trong bản đồ. Cuối cùng, các tập con lớn nhất trong tất cả các lần chạy được chọn, và nó chứa tất cả các nút phù hợp trong khu vực của nút.

Xác minh nút đơn: Trong [9] Du . LAD đề xuất giải pháp sử dụng thông tin triển khai để phát hiện vị trí bất thường. Xem xét các cảm biến với việc triển khai dựa trên nhóm, mỗi nút có thể được giả định theo phân phối hai chiều Gaussian, trong đó tập trung vào việc triển khai điểm của nhóm là nút. Sau đó, các tác giả đã đề xuất ba số liệu cho mỗi nút để phát hiện sự bất thường: các số liệu về sự khác biệt *Diff*, *Add-all*, và các số liệu xác suất. Lấy số liệu *Diff* đại diện cho sự khác biệt giữa thực tế quan sát và quan sát dự kiến (một quan sát là một vector, trong đó giá trị i đại diện cho số hàng xóm trong nhóm i). Các giá trị ngưỡng của các số liệu chỉ ra sự bất thường thu được thông qua đào tạo. Chú ý rằng LAD được thực hiện bởi mỗi nút đó; Tuy nhiên nó là dễ dàng được thực hiện tại BS (trạm cơ sở).

Trong [12] Capkun . cũng đề xuất sử dụng trạm cơ sở bảo mật (CBS) và trạm cơ sở di động (MBS) để báo cáo xác minh vị trí của các nút. Trong trường hợp CBS, các nút để được xác nhận sẽ phát đi một tín hiệu RF và một tín hiệu âm thanh. Sau đó, CBS có thể tính toán khoảng cách giữa các CBS và các nút dựa trên TDoA. Vì mỗi CBS biết vị trí của nó, là khoảng cách tính toán được so sánh với các khoảng cách tính bằng cách sử dụng các vị trí báo cáo và vị trí của CBS. Nếu sự khác biệt vượt một ngưỡng, các vị trí báo cáo bị từ chối. Trong trường hợp MBS, cũng tương tự. MBS đầu tiên đòi hỏi các nút phát sóng RF và tín hiệu âm thanh sau khi đạt thời gian T_R. Sau thời gian đó, các MBS đã di chuyển đến một vị trí khác không được

biết đến bởi các nút, do đó nó có thể kiểm tra các vị trí báo cáo tương tự như một CBS.

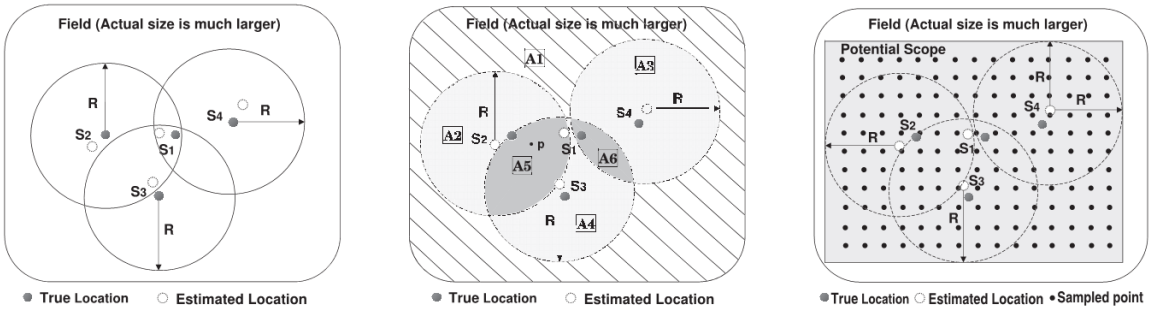
Trong [16] Ekici đề xuất một phương pháp xác suất (PLV) để xác minh vị trí của một nút. Một số nút xác minh đáng tin cậy biết vị trí của họ được triển khai trong mạng. Việc xác minh bắt đầu khi, nút đưa thông tin vị trí của nó làm ngập lụt trong mạng, với một trường đếm tổng số bước nhảy. Sau đó, mỗi nút xác minh có thể nhận được số lượng bước nhảy giữa các nút và kiểm tra, xác nhận và tính toán khoảng cách giữa chúng. Dựa trên hai giá trị, mỗi nút xác minh tính hai xác suất: một là khẳng định rằng một cặp giá trị như vậy không xảy ra, và một xác suất khác đại diện cho độ tin cậy của khẳng định. Cuối cùng, một nút trung tâm thu thập thông tin từ tất cả các nút kiểm tra và đưa ra các quyết định cuối cùng là chấp nhận hay từ chối.

	Batch-Verification	**Single-node Verification**	**Additional Hardware**
In-Region		Brands ; Echo ; Vora	Brands ; Echo ; Vora
Single-Location	Hwang	LAD ; CBS, MBS ; Leinmuller , PLV	CBS, MBS ; PLV

Hình 4 Sự so sánh các hệ thống xác minh thông tin vị trí

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. Các thuật toán được mô tả trong hình 11. Chúng tôi sẽ thảo luận các kỹ thuật chi tiết hơn trong phần sau.



(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

a. Đánh dấu các khu vực -Scored Districts

Chú ý rằng phạm vi giao tiếp là khu vực có tâm tại vị trí của cảm biến với bán kính R. Ở đây chúng ta định nghĩa một biến thể đã đặt tên phạm vi giao tiếp được ước tinh (ECR) là một vòng tròn mà tâm tại vị trí ước tính của bộ cảm biến. VC sử dụng các ECRs của một bộ cảm biến hàng xóm để xác nhận phân chia các trường thành nhiều vùng. Mỗi khu vực đều có một số điểm mà là số các ECRs chứa khu vực này. Một ví dụ thể hiện trong hình 10b, các vòng tròn rắn và rỗng tương ứng thể hiện cho vị trí đúng và ước tính của cảm biến. Cảm biến S_1 có ba người hàng xóm xác định là các cảm biến S_2, S_3 và S_4. Do đó được chia thành sáu khu vực thuộc ba khu vực được đánh số. khu vực được ghi 0 chứa khu vực A_1; khu vực được ghi 1- có chứa các vùng A_2, A_3, và A_4; và các khu vực ghi 2- có chứa các vùng A_5 và A_6. Chúng tôi nhận thấy rằng một bộ cảm biến có thể không được đánh số cao nhất trong khu vực, vì ECRs ước tính được phạm vi giao tiếp, có thể không bao gồm vị trí thực sự của một cảm biến. Dữ liệu có thể được thu thập từ hiện trường, sau đó được sử dụng trực tiếp cho mục đích của chúng tôi. Nếu không, các mô phỏng cần được tiến hành bằng cách sử dụng các thông số mạng thích hợp. Trong mô phỏng của chúng tôi, 600 cảm biến được triển khai một cách ngẫu nhiên trong một lĩnh vực vuông 300 m x 300 m. Phạm vi giao tiếp là R=20 m. Mỗi cảm biến trung bình có 12 xóm trong của nó phạm vi giao tiếp. Sự nhiễu loạn môi trường là định lượng bằng f=10%, có nghĩa là một bộ cảm biến có 90% cơ hội nhận được một thông báo beacon từ hàng xóm. Đối với mỗi cảm biến, chúng tôi ghi lại số xác nhận hàng xóm của nó, sau đó chúng tôi chia thành nhiều khu vực được đánh số mà các khu vực được đánh số có chứa vị trí thực sự của cảm biến.

Các kết quả của tất cả các cảm biến được tóm tắt trong hình 12. Trong này bảng, chỉ số hàng là số hàng xóm xác nhận, và chỉ số cột là số của khu vực đã được đánh số. Phần tử $T(t_1, t_2) = p$ có nghĩa là trong số tất cả các cảm biến có t_1 xác nhận hàng xóm, p% trong số họ đang ở trong một khu vực ghi là t_2. Ví dụ, $T(3, 2) = 27.18$ có nghĩa là trong số tất cả các cảm biến nhận được ba xác nhận của hàng xóm, 27.18 % là các hàng xóm bên trong khu vực được ghi 2.

Tìm danh sách hàng xóm đã được xác minh cho sensor Si

Xác định trọng số vùng Di1,....Dim

For mỗi vùng Dij

Tính toán giá trị xác xuất Pr(Dij)

Tính toán PDF, PMF xác định xem là phân bố rời rạc hay liên tục

Tính toán độ tin cậy vùng;

If phân bố liên tục

Thực hiện tích phân 2 lớp sử dụng PDF

Else

Thực hiện tính xác xuất các điểm sử dụng PMF

Hình 11 Thuật toán xác minh trong khu vực

VC sử dụng bảng đào tạo hình 12 để gán trọng lượng khác nhau cho các khu vực được đánh số khác nhau. Chúng tôi vẫn sử dụng các ví dụ trong hình. 10b để giải thích các thủ tục. Trong hình, có ba vùng (khu vực được đánh số) chia cho cảm biến S_1 có điểm tương ứng 0, 1, và 2. Vì S_1 có ba hàng xóm đã xác nhận, nên VC đề cập đến hàng thứ ba trong bảng. Các trọng số tương ứng với điểm số 0, 1, và 2 là $T(3, 0) = 0.22, T(3,1) = 4.09$ và $T(3,2) = 27.18$. Dựa trên những trọng số, xác suất mà cảm biến S_1 nằm bên trong khu vực khác nhau có thể được tính toán. Ví dụ, xác suất S_1 là bên trong khu vực số 2 là 27.18/(0.22+4.09+27.18)=0.8631. Các công thức tính xác suất trong vùng được cho bởi

$$P_r(L_i \in D_{im}) = \frac{T(n_i, m)}{\sum_{k \in M_{inc}} T(n_i, k)}, \forall m \in M_{inc}, (20)$$

Trong đó D_{im} là khu vực được đánh số m, n_i là số lượng các hàng xóm đã xác nhận của s_i, và M_{inc} là tập các điểm khu vực của tất cả các khu vực đã chia cho cảm biến s_i.

b. Phân phối liên tục

Hàm mật độ xác suất (pdf) xác định mật độ xác suất mà một bộ cảm biến có thể cư trú tại các điểm khác nhau trong vùng bởi (20), chúng tôi đã tính toán xác suất trong vùng. Và chấp nhận giả định rằng xác suất phân phối trong một vùng là thống nhất. Bởi vì một cảm biến sẽ có cùng số người hàng xóm xác nhận tại hai điểm trong một vùng, do đó hai điểm có thể không được phân biệt về mặt thống kê. Dựa trên giả định này, chúng tôi có thể tính toán mật độ xác suất trong vùng bằng cách chia xác suất trong vùng theo khu vực của vùng. Ví dụ, trong hình. 9b, nếu giá trị khu vực của vùng số 2 là 12 m^2, và xác suất mà S_1 là ở vùng này là 0.8631. Sau đó các mật độ xác suất tại bất kỳ điểm nào trong vùng số 2 là 0.8631/12=0.0719. Các công thức tính hàm pdf cho cảm biến s_i có thể được đưa ra bởi:

$$pdf_i(l) = \frac{P_r(L_i \in D_{im})}{S(D_{im})}, \forall l \in D_{im}, (21)$$

Trong đó số bị chia $P_r(L_i \in D_{im})$ là xác xuất ngoài khu vực trong (20), và số chia $S(D_{im})$ là giá trị diện tích của khu vực được ghi số m là D_{im}.

c. Phân phối rời rạc

Vì nó có giá là tương đối đắt để tính toán diện tích của vùng $S(D_{im})$ trong (21). Nên chúng ta thảo luận làm thế nào để tính toán một phân bố rời rạc mà không liên quan đến độ phức tạp tính toán.

Chúng tôi nhận thấy rằng các trọng số tương ứng với các vùng được ghi là 0 (cột đầu tiên trong bảng đào tạo trong hình 12), có giá trị rất nhỏ. Trong khi đó, diện tích của vùng này là rất lớn (xấp xỉ diện tích của toàn bộ khu vực). Do đó, mật độ xác suất bên trong vùng 0 sẽ rất nhỏ. Dựa trên quan sát này, trong thuật toán của chúng tôi, VC xác định một phạm vi tiềm năng và chỉ tập trung vào phạm vi bên trong của khu vực này. Chúng ta sử dụng các ví dụ trong hình. 10c để giải thích việc xác định phạm vi tiềm năng. Với cảm biến S_1 có ba người hàng xóm xác nhận S_2, S_3, và S_4. Các ranh giới của phạm vi tiềm năng là các đường tiếp tuyến của ECRs của các cảm biến này. Rõ ràng, phạm vi tiềm năng sẽ bao gồm tất cả các vùng khác không ghi bàn.

Trong phạm vi tiềm năng, các VC thống nhất và gán xác suất khác nhau tới mỗi điểm. Và xác suất của tất cả các điểm trong một khu vực nên tổng hợp để xác

suất trong vùng được tính bằng (20). Do đó, hàm xác suất khối (PMF) của cảm biến s_i được cho bởi:

$$pmf_i(l) = \begin{cases} \frac{P_r(L_i \in D_{im})}{N(D_{im})}, l \in P_i \\ 0, ngược\ lại \end{cases} \quad (22)$$

Trong đó số bị chia $P_r(L_i \in D_{im})$ là xác xuất ngoài khu vực trong (21), và số chia $N(D_{im})$ là số lượng của các điểm lấy mẫu trong khu vực D_{im} và P_i là phạm vi khả năng của cảm biến S_i.

d. Độ tin cậy của xác minh

Độ tin cậy của xác minh là sự tự tin rằng một bộ cảm biến có thể được xác nhận trong khu vực xác minh. Nếu các phân phối là liên tục, trong khu vực tin cậy là tính bằng cách lấy tích phân 2D của xác suất hàm mật độ (21) trong khu vực xác minh.

$$P_r(L_i \in V_i) = \iint_{V_i} pdf_i(x, y)dxdy. (23)$$

Nếu việc phân phối là rời rạc, trong vùng tin tưởng, việc bổ sung các xác suất của tất cả các điểm trong việc xác minh vùng:

$$P_r(L_i \in V_i) = \sum_{l \in P_i} pmf_i(l).I(l \in V_i) \quad (24)$$

Trong đó I là chỉ số hàm mà đầu ra 1 nếu $l \in V_i$, và ngược lại đầu ra là 0.

Sau khi VC cung cấp độ tin cậy của xác minh đến trung tâm điều khiển, trung tâm sẽ so sánh độ tin cậy này với một ngưỡng ứng dụng cụ thể để đưa ra quyết định đúng đắn. Trong các ứng dụng giám sát chiến trường, cảm biến phát hiện S_i một chiếc xe tăng và vị trí của nó được xác nhận qua các VC. Sau đó, độ tin cậy của xác minh được so sánh với một ngưỡng quyết định cho một ứng dụng. Do đó,

$$\begin{cases} P_r(L_i \in V_i) \geq t \Rightarrow thỏa\ ứng\ dụng, \\ P_r(L_i \in V_i) < t \Rightarrow không\ thỏa\ ứng\ dụng, \end{cases} \quad (25)$$

Trong đó t là ngưỡng và giá trị của nó là ứng dụng cụ thể. Nếu nhiều cảm biến phát hiện các xe tăng, mỗi một xác minh có sự tin tưởng khác nhau, sau đó ứng dụng có thể đưa ra quyết định về việc liệu dự án bom sử dụng quy tắc phức tạp hơn. Ví dụ, một trong những cách tiếp cận là xem xét phần lớn các kết quả xác minh. Hoặc nếu có nhiều hơn một nửa trong số các cảm biến có sự tin cậy của xác minh

lớn hơn ngưỡng, sau đó quả bom có thể được thả. Một cách tiếp cận thứ hai là tính toán độ tin cậy trung bình của tất cả các cảm biến phát hiện nơi chứa bom, sau đó so sánh nó với ngưỡng sử dụng các chức năng trên. Chúng tôi nhận thấy việc đưa ra quyết định ứng dụng cụ thể là một vấn đề độc lập từ việc tính toán sự tin tưởng của xác minh cho mỗi cảm biến. Dựa trên các kết quả xác minh, các chiến lược khác nhau có thể được sử dụng để phục vụ mục đích của ứng dụng.

Trong hàm (25), nếu t được thiết lập cao, báo động giả có thể dễ dàng lọc ra nếu không tồn tại mục tiêu; nếu t được thiết lập thấp, sau đó xác suất cao mà hầu hết các mục tiêu có thể bị tiêu diệt. Không có vấn đề làm thế nào các ngưỡng xác định, chúng tôi mong đợi một thuật toán xác minh rằng không phải là nhạy cảm với các giá trị ngưỡng. Cụ thể, khi các ngưỡng rơi vào một phạm vi rộng lớn của các giá trị, cả hai tỷ lệ âm tính giả và tỷ lệ dương tính giả có thể được duy trì ở các mức thỏa đáng. Trong phần mô phỏng, chúng tôi đã nghiên cứu tỷ lệ phát hiện sai tích cực / tiêu cực của giá thuật toán xác minh, và nó cho thấy rằng thuật toán có hiệu suất xác minh tốt với các thiết lập ngưỡng khác nhau.

2.4.4. Phân tích sự bảo mật

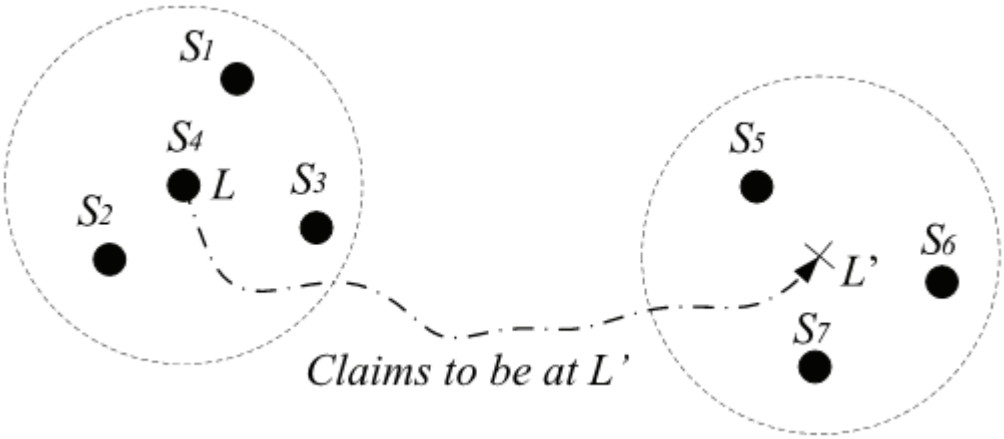
Khi WSNs được triển khai trong môi trường thù địch, phù hợp khi những kẻ thù có thể tấn công các chương trình định vị để làm cho các vị trí cảm biến ước tính sai, họ cũng có thể tấn công các thuật toán xác minh để làm cho các vị trí bất thường không được VC phát hiện.

Trong thuật toán GFM, những kẻ tấn công có thể thỏa hiệp một cảm biến và buộc nó để báo cáo quan sát khu vựcgiả là phù hợp với vị trí tuyên bố. Trong GFT thuật toán, kể từ khi các hàng xóm phù hợp có thể làm tăng chỉ số của một cảm biến, kẻ tấn công có thể tạo ra các hàng xóm phù hợp xung quanh một cảm biến nạn nhân. Trong các thuật toán xác minh trong khu vực, kể từ khi VC dựa trên những quan sát khu vực cảm biến để lấy được phân phối xác suất, kẻ tấn công có thể làm méo mó các quan sát này. Điều quan trọng là thuật toán là đủ mạnh mẽ trong sự hiện diện của tấn công nguy hiểm.

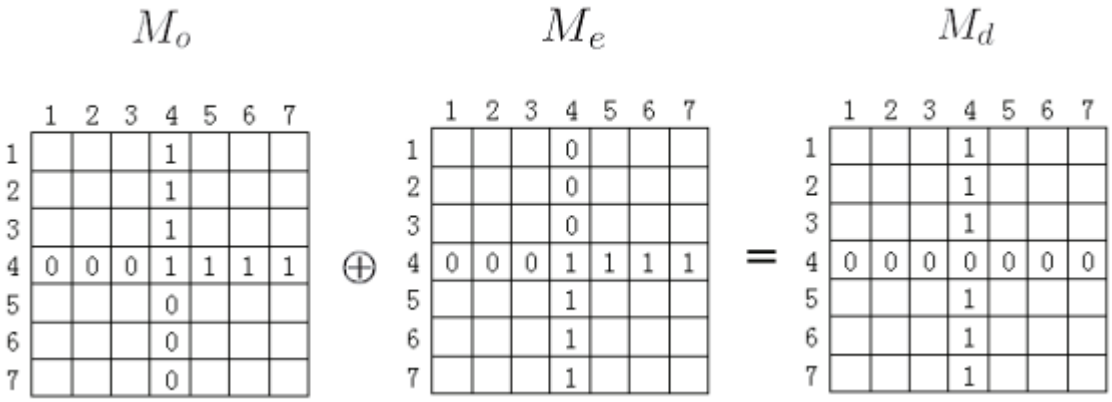
a. Phân tích an ninh cho thuật toán GFM

Cũng giống như các đối thủ có thể tấn công các chương trình định vị để làm cho các vị trí của cảm biến bị ước tính sai, họ cũng có thể tấn công các thuật toán

xác minh để làm cho các vị trí bất thường KHÔNG được phát hiện bởi các VC. Để đạt được mục tiêu này, kẻ tấn công sẽ thỏa hiệp một cảm biến và buộc nó báo cáo giả về quan sát khu vựclà phù hợp với tuyên bố vị trí. Chúng tôi minh họa một cuộc tấn công như trong hình 13. Trong hình, Cảm b iến S_4 bị xâm nhập và được định vị tại vị trí L' đó là vị trí cách xa vị trí đúng L của nó. Nếu cảm biến S_4 báo cáo quan sát đúng $O_4 = (S_1, S_2, S_3)$, thì thuật toán sẽ GFM dễ dàng tìm thấy mâu thuẫn vì các vị trí được ước tính của các cảm biến S_1, S_2 và S_3 là nằm xa vị trí L'. Để không bị phát hiện, S_4 có thể báo cáo một quan sát khu vựcgiả $O_4 = (S_5, S_6, S_7)$, trong đó bao gồm các cảm biến khu trú trong khu vực của vị trí L'.



Hình 13 Tấn công vào thuật toán GFM



Hình 14 Các ma trận của GFM dưới các cuộc tấn công

Chúng tôi sẽ sử dụng các ví dụ trên để phân tích hiệu suất của thuật toán của GFM. Trong hình 14, các phần tử trong hàng thứ 4 và cột thứ 4 của ma trận Md được hiển thị. Để đơn giản, ma trận trọng lượng Mw là không liên quan ở đây. Dựa trên ma trận này, các giá trị ma trận cho cảm biến S4 là AD4 = 0, PD4 = 6 và AS4 =

6. Các giá trị của PD4 và AS4 là rất cao, do đó, nó có thể xảy ra rằng S4 sẽ bị thu hồi.

Một kịch bản tấn công tinh vi hơn là S4 không phát ID của nó, do đó S1, S2 và S3 không thể quan sát cảm biến S4. Sau đó, các phần tử trong Md cần phải được tính toán lại một cách thích hợp, và các giá trị ma trận trở thành AD4 = 0, PD4 = 3 và AS4 = 3. Vì vậy, sự không thống nhất đã được giảm nhẹ. Tuy nhiên, để định nghĩa các hàng xóm phù hợp, các số liệu các hàng xóm phù hợp trở thành CN4 = 0, vì vậy S4 vẫn có thể bị thu hồi trong quá trình kiểm tra cuối cùng tại dòng (13) - (14) của thuật toán GFM.

Nhìn chung từ cuộc tấn công trong ví dụ này, chúng tôi giả định cảm biến Si báo cáo một vị trí giả L', cách xa vị trí đúng của nó L. Trong khi đó, nó báo cáo quan sát của n cảm biến trong khu vực của L và n' Cảm biến trong các khu vực của L'. Có thực sự các cảm biến m và m' trong các khu vực của L và L' tương ứng, trong đó m ≥ n và m' ≥ n'. Bởi vì n cảm biến đang không ở trong khu vực của L', số liệu về hành vi khác biệt $AD_i = n + m' - n'$. Thứ hai, vì không ai trong số các cảm biến trong khu vực của L' Sẽ quan sát cảm biến Si, số liệu vượt qua là PD_i= n+m'. Hơn nữa, các số liệu bất đối xứng là $AS_i = m - n + m' - n'$ và số liệu về hàng xóm phù hợp là $CN_i = 0$. Để hạn chế tối đa các giá trị cho ba số liệu đầu tiên, những kẻ tấn công sẽ có giá trị lớn cho n' như là n' = m' . Trong khi giá trị nhỏ hơn của n sẽ làm tăng số liệu AS, giá trị lớn hơn của n sẽ tăng số liệu AD và PD. Quan trọng hơn, vì chẳng có hàng xóm phù hợp tồn tại với cảm biến Si, nó sẽ được thu hồi tại bước kiểm tra cuối cùng của thuật toán GFM.

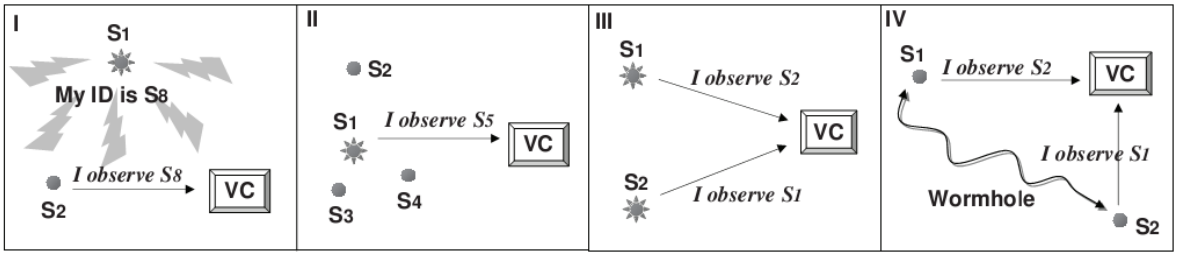
Sự mâu thuẫn có thể được loại bỏ hoàn toàn nếu cảm biến S4, S5, S6 và S7 đều bị tổn hại. Cảm biến S4 không phát ID của nó, và các báo cáo một quan sát khu vựcgiả O4 = (S5, S6, S7); Trong khi đó, cảm biến S5, S6 và S7 tất cả các báo cáo quan sát S4. Tấn công thông đồng này gây tốn kém khi khởi động và chống lại giả định của chúng tôi là phần lớn các cảm biến này là lành tính trong một khu vực địa phương. Do đó, chúng tôi kết luận rằng miễn là những kẻ thù không thể thỏa hiệp với phần lớn các cảm biến trong một khu vực địa phương, mâu thuẫn luôn luôn tồn tại và vị trí bất thường có thể được phát hiện. Kết quả mô phỏng cũng chứng minh tính hiệu quả và mạnh mẽ của các thuật toán GFM.

b. Phân tích sự an toàn của thuật toán GFT

Trong thuật toán GFT, các hàng xóm phù hợp có thể làm tăng chỉ số của cảm biến, và hàng xóm không phù hợp có thể làm giảm chỉ số tin cậy của nó. Việc biết quá trình lọc của GFT, kẻ tấn công sẽ cố tránh bị thu hồi bằng cách tạo ra nhiều hàng xóm phù hợp nhất có thể cho một cảm biến bị làm tổn hại. Để đạt được mục tiêu này, các cảm biến được nhu cầu để giữ im lặng của ID của nó bị tổn hại. Mặt khác, các cảm biến được xung quanh các vị trí dự kiến của các cảm biến cần thỏa hiệp yêu cầu bồi thường để "quan sát" cảm biến này, để họ có thể trở thành hàng xóm phù hợp của cảm biến này. Kết quả mô phỏng cũng sẽ chứng minh rằng các thuật toán GFT có hiệu suất thỏa mãn yêu cầu.

c. Phân tích sự an ninh của thuật toán xác minh vùng In-region

Khi WSNs được triển khai trong môi trường thù địch, kẻ thù cố có thể làm gián đoạn quá trình xác minh. Kể từ khi VC dựa vào "quan sát khu vực để lấy được phân bố xác suất của bộ cảm biến 'cảm biến vị trí, những kẻ tấn công sẽ cố gắng để tạo ra sai lệch quan sát xung quanh. Chúng tôi minh họa cho các cuộc tấn công có thể trong hình 15. Trong đó có bốn phụ liệu: (I) một cảm biến tổn hại phát sóng một ID không chính xác, do đó, các cảm biến khác báo cáo quan sát khu vực sai; (II) là một bộ cảm biến bị tổn hại trực tiếp báo cáo quan sát khu vựcsai; (III) hai bộ cảm biến được bản địa hoá xa nhau hợp tác và yêu cầu bồi thường để quan sát nhau; (IV) wormhole kẻ tấn công thông điệp đèn hiệu kỷ lục tại một địa điểm, đường hầm chúng thông qua một liên kết có dây và phát lại tại một vị trí khác. Do đó, các cảm biến ở hai đầu của wormhole sẽ cả hai báo cáo quan sát khác.



Hình 15. Các tấn công vào thuật toán xác minh

Trong thuật toán của chúng tôi, các VC khẳng định có mối láng giềng của hai bộ cảm biến chỉ khi họ có thể quan sát nhau. Kể từ khi hai cuộc tấn công đầu tiên (tấn công I và II) tạo ra các quan sát không cân xứng giữa các bộ cảm biến, quan sát

khu vực của họ sẽ không được xem xét bởi các VC để sử dụng tiếp. Tuy nhiên, các cuộc tấn công thông đồng và các cuộc tấn công wormhole (tấn công III và IV) đều có khả năng để tạo ra các quan sát đối xứng giữa một cặp cảm biến. Do đó, một người hàng xóm xa xôi của một bộ cảm biến có thể đóng góp một vùng khác không ghi bàn trong lĩnh vực này.

Để giải quyết những mô hình tấn công III và IV, chúng ta xem xét các cuộc tấn công dạng tunnel, nơi một số bộ cảm biến cung cấp các tài liệu tham khảo vị trí cộng tác giả và làm cho các vị trí gần nhau. Cuộc tấn công này có thể được đưa ra bằng cách ảnh hưởng đến nhiều bộ cảm biến hoặc tạo một wormhole giữa hai khu vực xa cách nhau. Trong mô phỏng, chúng ta thiết lập giá trị trong khoảng (0,50%), và các kết quả mô phỏng chứng minh tính hiệu quả của thuật toán của chúng tôi trong việc đánh bại chống lại các cuộc tấn công như vậy. Tuy nhiên, có thể có tình huống các dạng tấn công wormhole truyền tải thông điệp từ một vị trí xa với cảm biến nạn nhân, và tạo ra một nhầm lẫn rằng để cảm biến rằng hơn một nửa số người hàng xóm giả của nó có các tham khảo địa điểm phù hợp. Đánh bại chống lại các cuộc tấn công này, chúng tôi sẽ tiến hành nghiên cứu trong tương lai.

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.

Trong các hệ thống xác minh đơn vị, hệ thống xác minh nút đơn thường có hiệu quả hơn hệ thống xác minh hàng loạt khi chúng ta muốn xác minh một số nút quan trọng, ví dụ các nút thông báo sự kiện. Tuy nhiên hệ thống xác minh hàng loạt thích hợp hơn khi chúng ta muốn xác minh tất cả các nút cùng một lúc.

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. Theo yêu cầu của các ứng dụng khác nhau, hệ thống sẽ cung cấp kết quả xác minh (tại chỗ) *on-spot* hoặc (theo vùng) *in-region*. Xác minh tại chỗ là để xác minh liệu ước tính vị trí của cảm biến có khoảng cách của nó đúng

vị trí hay kém hơn so với một khoảng cách nhất định. Mặt khác, xác minh theo vùng là để xác minh xem một cảm biến có nằm trong một khu vực địa lý theo ước tính vị trí của nó là ở khu vực đó. Nếu xác minh thành công, các vị trí sẽ được công nhận bởi các VC như một vị trí chính xác. Ngược lại, nó sẽ được công nhận là một trong những vị trí sai.

Các hệ thống xác minh nên có thuộc tính sau. Đầu tiên, các thuật toán xác minh gọn nhẹ về chi phí phần cứng và chi phí tính toán. Nó không nên đòi hỏi thiết bị đắt tiền như hướng ăng ten, và bộ vi xử lý nhanh chóng mà thực hiện XOR tính toán trong phạm vi vài nano giây. Cảm biến không cần sự truyền thông lớn, cái mà sẽ nhanh chóng tiêu thụ năng lượng lưu trữ của cảm biến. Thứ hai, các thuật toán nên có hiệu quả bằng cách đạt tỷ lệ phát hiện cao và phát hiện nhầm thấp. Tỷ lệ phát hiện được định nghĩa là tỷ lệ giữa số lượng phát hiện sai vị trí và số lượng của tất cả các vị trí sai. Trong khi tỷ lệ thứ hai được định nghĩa là tỷ lệ giữa số vị trí chính xác mà bị nhầm tưởng công nhận là sai với số lượng của tất cả các vị trí chính xác. Thứ ba, như các thuật toán xác minh có thể trở thành mục tiêu của những kẻ tấn công, nó nên đủ mạnh và có khả năng để cung cấp xác minh chính thức kết quả ngay cả trong sự hiện diện của các cuộc tấn công độc hại.

Xác minh tại chỗ (On-spot) là để xác minh xem một lỗi định vị của cảm biến có ít hơn so với một khoảng cách nhất định. Đặt L_{true}và L_{est} biểu thị vị trí đúng và vị trí được ước tính của một nút cảm biến, thì sự xác minh không thành công nếu các điều kiện sau đây là đúng: $|L_{true} - L_{est}| > D$ trong đó D được gọi là ngưỡng dị thường (ngưỡng bất thường - Anomaly degree). Giá trị của D nên được thiết lập đúng cách với những cân nhắc các yêu cầu ứng dụng và giá trị của các lỗi định vị thông thường đang hiện diện trong môi trường không tấn công. Ở đây, chúng tôi xem xét D như là một tham số đầu vào và giả định giá trị của nó đã có trong hệ thống của chúng tôi.

In –region: Xác minh trong vùng là để xác minh xem một bộ cảm biến là bên trong một khu vực vật lý hay không. Khu vực này có thể khác nhau cho mỗi ứng dụng dựa trên địa điểm. Với một ứng dụng, chúng ta định nghĩa một vùng tự nhiên trong đó nếu một bộ cảm biến có thể được xác minh, sau đó mục tiêu ứng dụng có thể đạt được.

Mục đích của ứng dụng đã được điền đầy đủ $\Leftrightarrow L_i \in V_i$ (1)

Trong đó L_i là vị trí của nút cảm biến S_i và V_i là khu vực xác minh. Sau đó Wei đưa ra phương sai khác của khu vực xác minh và cũng tìm hiểu chi tiết về cách làm thế nào để xác định khu vực thích hợp.

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 thiều thời gian phải xác minh, từ đó tăng tốc hoặc tăng tỉ lệ chuyển phát gói tin của quá trình định tuyến an toàn.

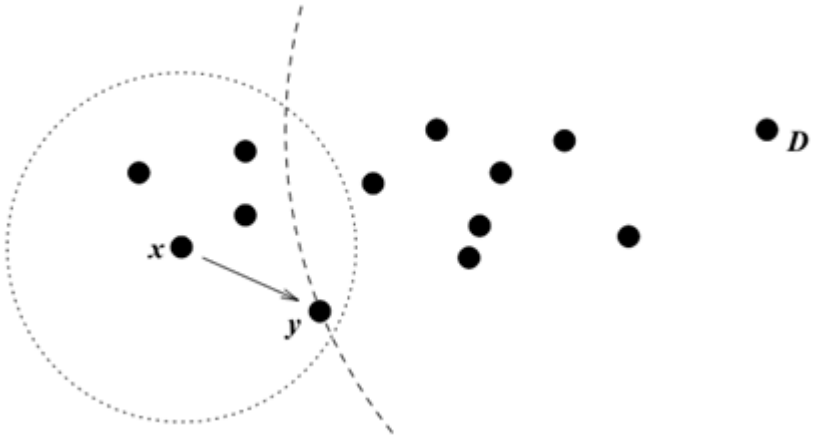
CHƯƠNG III: ĐỊNH TUYẾN PHỤC HỒI THEO THÔNG TIN VỊ TRÍ

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 [13] 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. Ở đây, x nhận một gói đã xác định đích đến D. Phạm vi truyền sóng của x vòng tròn được biểu diễn bởi vòng tròn chấm xung quanh x, và vòng cung với bán kính bằng khoảng cách giữa y và D được thể hiện là cung nét đứt với D. X chuyển các gói tin đến y, khi khoảng cách giữa y và D là nhỏ hơn so với khoảng cách giữa D và bất kỳ láng giềng nào của x khác. Quá trình chuyển tiếp tham lam này lặp đi lặp lại, cho đến khi gói tin đến D.



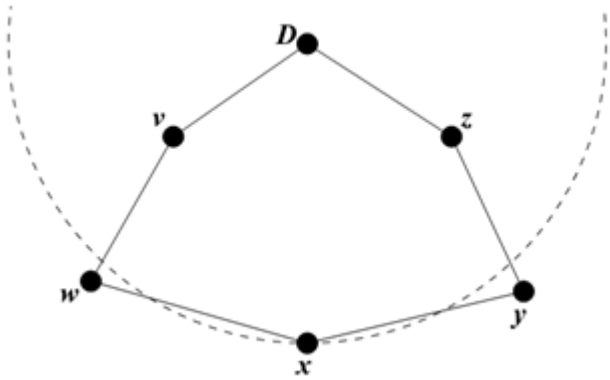
Hình 16. Ví dụ chuyển tiếp tham lam

Một thuật toán đơn giản cung cấp tất cả các nút cùng với vị trí láng giềng của họ: định kỳ, mỗi nút truyền đi một gói tin Beacon tới các địa chỉ MAC broadcast, chỉ chứa nhận dạng riêng của nó (ví dụ, địa chỉ IP) và vị trí. Karp mã hóa vị trí bằng số thực có dấu chấm động 24 byte, với các giá trị tọa độ x và y. Khi chưa nhận được một beacon từ một hàng xóm lâu hơn khoảng thời gian time-out T, một router GPSR giả định rằng người hàng xóm đã không thành công hoặc đã nằm ngoài phạm vi phủ sóng, và xóa các hàng xóm từ bảng của nó. Các lớp MAC 802.11 cũng cho dấu hiệu trực tiếp của sự thất bại truyền lại mức liên kết với các nước láng giềng; Karp đã sử dụng T = 4.5B, ba lần khoảng thời gian trễ tối đa của một beacon.

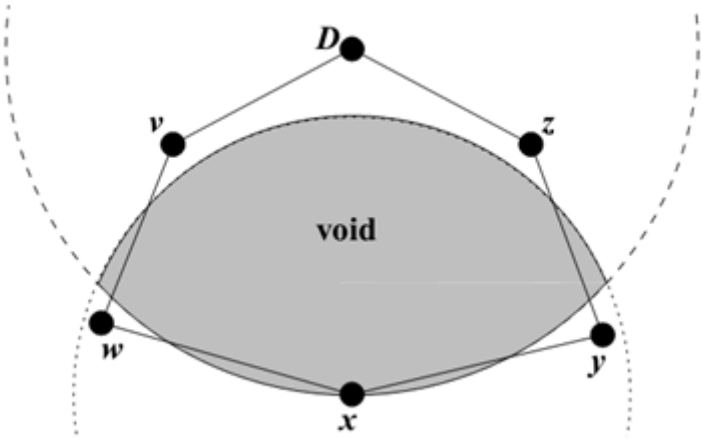
Lợi thế lớn của chuyển tiếp tham lam là sự phụ thuộc của nó chỉ về kiến thức của việc chuyển tiếp tới các hàng xóm trực tiếp của nút. Trạng thái yêu cầu là không đáng kể, và phụ thuộc vào mật độ của các nút trong mạng không dây, chứ không phải tổng số các điểm đến trong mạng. Trên mạng, nơi mà định tuyến đa bước nhảy là hữu ích, thì số lượng các hàng xóm trong phạm vi phủ sóng của một node phải ít hơn đáng kể so với tổng số các nút trong mạng. Vị trí một nút liên kết với một hàng xóm trở nên ít hơn vì hàng xóm di chuyển. Độ chính xác của các thiết lập của các nước láng giềng cũng giảm; hàng xóm cũ có thể đã rời đi và các hàng xóm mới có thể nằm trong phạm vi phủ sóng. Đối với những lý do này, sự lựa chọn chính xác của khoảng thời gian gửi beacon để giữ cho bảng hàng xóm của nút hiện thời phụ thuộc vào tốc độ di chuyển trong mạng và phạm vi phát sóng của nút. Chú ý rằng việc giữ trạng thái tôpô hiện tại cho một bán kính phủ sóng một bước nhảy cho một router là yêu cầu tối thiểu để thực hiện bất kỳ sự định tuyến nào; không có quyết định chuyển tiếp hữu ích được thực hiện mà không có kiến thức về cấu trúc liên kết đi theo một hoặc nhiều bước nhảy. Khi có bất kỳ nút gửi một gói dữ liệu, sau đó nó có thể thiết lập lại bộ đếm thời gian bên trong beacon của nó. Tối ưu hóa này làm giảm lưu lượng beacon trong khu vực của mạng chủ động chuyển tiếp các gói dữ liệu.

Trong thực tế, chúng ta có thể làm cho cơ chế beacon của GPSR hoàn toàn reactive bằng việc có các nút thu hút các beacon với một broadcast cho “yêu cầu hàng xóm" chỉ khi họ có lưu lượng truy cập dữ liệu để chuyển tiếp. Sức mạnh của chuyển tiếp tham lam với tuyến đường bằng cách sử dụng các vị trí của nút hàng xóm đi kèm với một mặt hạn chế: Ở đây có các cấu trúc liên kết mà trong đó chỉ

tuyến đường duy nhất tới một điểm đến yêu cầu một gói tin tạm thời di chuyển xa hơn khoảng cách hình học từ đích [7], [16]. Một ví dụ đơn giản của một cấu trúc liên kết đó được thể hiện trong hình 17. Ở đây, x là gần đích D hơn với các hàng xóm w và y của nó. Một lần nữa, vòng cung hướng về D có bán kính bằng khoảng cách giữa x và D. Mặc dù hai con đường, $(x \to y \to z \to D)$ Và $(x \to w \to v \to D)$, tồn tại để tới D, x sẽ không chọn để chuyển tiếp đến w hoặc y sử dụng chuyển tiếp tham lam. x là một cực tiểu địa phương gần với D hơn cả. Một số cơ chế khác phải được sử dụng để chuyển tiếp các gói tin trong những tình huống này.



Hình 17. Ví dụ chuyển tiếp tham lam bị Fail. X là một cực tiểu địa phương và w,y thì xa đích D



Hình 18. X tạo nên một void tới đích D

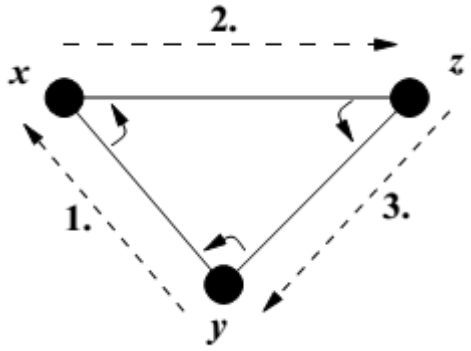
3.1.2 Quy tắc bàn tay phải

Qua hình 17, chúng tôi lưu ý rằng giao điểm của phạm vi phủ sóng của x và đường tròn D có bán kính $|\overline{xD}|$ (có nghĩa là, về độ dài của đoạn thẳng $\overline{xD}$) là các

hàng xóm rỗng. Chúng ta thấy khu vực này rõ ràng trong hình 18. Từ điểm nút x, các khu vực bóng mờ mà không có các nút là một khoảng trống (void). X tìm cách để chuyển tiếp một gói tin đến đích D ngoài rìa xung quanh khoảng trống này. Bằng trực giác, x tìm các tuyến đường xung quanh khoảng trống; nếu một đường dẫn đến D tồn tại từ x, nó không bao gồm các nút nằm trong khoảng trống (hoặc x sẽ được chuyển tiếp tham lam cho họ).

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.

Chúng tôi tìm cách khai thác những tính chất đi đường vòng để tuyến đường bao quanh các lỗ trống. Trong hình 18, việc đi qua đường vòng $(x \to w \to v \to D \to z \to y \to x)$ bởi các quy tắc bàn tay phải điều hướng xung quanh khoảng trống trong hình, đặc biệt là tới các nút gần đến đích hơn x (trong trường hợp này, bao gồm cả các điểm đến chính nó, D). Trình tự của các cạnh đi qua bởi quy tắc bàn tay phải là một vành đai.



Hình 19. Quy tắc bàn tay phải

Các trạng thái tích lũy trong các gói dữ liệu được lưu trữ bởi các nút, mà phục hồi từ vị trí cực đại trong chuyển tiếp tham lam bằng cách định tuyến đến một nút theo chu vi đã được lưu trữ gần hơn với đích. Cách tiếp cận này đòi hỏi một phương

pháp Heuristic. Heuristic này có thể cải thiện kết quả tổng thể có thể đạt được, nhưng vẫn còn hạn chế nhất định: các thuật toán không luôn luôn tìm các tuyến đường khi chúng tồn tại. Nếu xảy ra hiện tượng phân mảnh mạng(partion network) hoặc cặp cạnh đan chéo nhau thì nguy cơ quy tắc bàn tay phải sẽ bị chạy vòng và không thể thoát ra được. Để tránh hiện tượng này, người ta tìm cách loại bỏ các cặp cạnh đan chéo theo quy tắc lược hóa mạng theo cơ chế đồ thị phẳng – được trình bày sau đây.

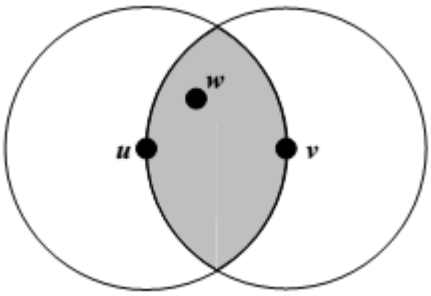
3.1.3 Đồ thị phẳng

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.

Một đồ thị trong đó không có hai cạnh chéo được biết như là một đồ thị phẳng. A tập hợp các nút với phạm vi phát sóng, nơi mà tất cả phạm vi phát sóng là giống hệt nhau, đường tròn phạm vi phủ sóng có bán kính r, có thể được xem như là một đồ thị: mỗi nút là một đỉnh, và cạnh (n; m) tồn tại giữa các nút n và m nếu khoảng cách giữa n và m, $d\ (n,m) \leq\ r$. Đồ thị có cạnh được quyết định bởi một ngưỡng khoảng cách giữa các đỉnh được gọi là đồ thị đơn vị. Trong ý nghĩa đó phần cứng mạng vô tuyến truyền thống được xem là phạm vi không gian mở (ví dụ, 250 mét với 900 MHz DSSS WaveLAN), mô hình này là hợp lý. Chúng ta cũng giả định rằng các nút trong mạng có sự khác biệt đáng kể về độ cao, vì vậy mà chúng có thể được coi là khoảng trên một mặt phẳng.

Đồ thị tương quan hàng xóm (RNG) và Gabriel Graph (GG) là hai đồ thị phẳng phổ biến. Một thuật toán để loại bỏ các cạnh từ các đồ thị mà không phải là một phần của RNG hoặc GG sẽ mang lại một mạng không có liên kết chéo. Các thuật toán nên được chạy trong một thời gian được phân chia bởi mỗi nút trong mạng, nơi một nút cần thông tin chỉ về cấu trúc liên kết địa phương như là đầu vào của thuật toán. Tuy nhiên, chiến lược này để thành công, một trong những thuộc tính quan trọng phải được thể hiện:

Việc loại bỏ các cạnh từ đồ thị để giảm bớt nó đến RNG hoặc GG không phải ngắt kết nối đồ thị; điều này sẽ chiếm phân vùng mạng.



Hình 20: Đồ thị RNG,với cạnh (u,v) nằm trong.

Với tập các đỉnh đã biết trước vị trí, các RNG được định nghĩa như sau:

Một cạnh (u; v) tồn tại giữa đỉnh u và v nếu khoảng cách giữa chúng, d (u; v), nhỏ hơn hoặc bằng với khoảng cách giữa mỗi đỉnh w khác, và nào của u và v là xa hơn từ w . Ở dạng bất đẳng thức:

$$\forall w \neq u, v: d(u,v) \leq \max[d(u,w), d(v,w)]$$

Hình 20 mô tả các quy tắc cho việc xây dựng RNG. Khi chúng ta bắt đầu với một đồ thị đơn vị được kết nối và các cạnh bị loại bỏ không phải là một phần của RNG, lưu ý rằng không làm mất kết nối của đồ thị (u; v). Chỉ loại bỏ khỏi đồ thị khi tồn tại một w trong phạm vi của cả u và v. Như vậy, loại bỏ một cạnh yêu cầu có một con đường thay thế. Mỗi thành phần kết nối trong một mạng vô tuyến thông suốt sẽ không bị ngắt kết nối bằng cách loại bỏ các cạnh không nằm trong RNG.

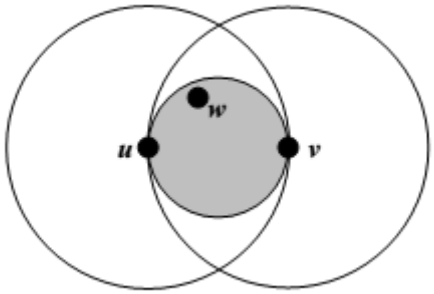
Theo cơ chế Beacon mô tả trước đây, thông qua đó tất cả các nút biết hàng xóm trực tiếp của họ, nếu u và v có thể giao tiếp với nhau, cả hai phải đều biết tất cả các nút. Bắt đầu từ một danh sách đầy đủ các hàng xóm của nó, N, mỗi nút u có thể loại bỏ các phi liên kết RNG như sau:

```
For all v ∈ N do
 For all w ∈ N do
       If w==v then continue
       Else if d(u,v) > max[d(u,w),d(v,w)] then
              eliminate edge (u,v)
             break
       end if
 end for
end for
```

GG được xác định như sau:

Một cạnh (u; v) tồn tại giữa các đỉnh u và v nếu không có đỉnh w khác có mặt trong vòng tròn có đường kính là $\overline{uv}$. Ở dạng bất đẳng thức:

$$\forall w \neq u, v: d^2(u,v) < [d^2(u,w) + d^2(v,w)]$$



Hình 21: Đồ thị GG

Hình 21 đồ thị GG, khi trung điểm của $\overline{uv}$ là tâm của vòng tròn với đường kính $\overline{uv}$, một nút u có thể loại bỏ các phi liên kết GG của nó từ một danh sách hàng xóm đầy đủ N do:

```
m = midpoint of uv
For all v ∈ N do
 For all w ∈ N do
       If w==v then continue
       Else if d(u,v) < d(u,m) then
              eliminate edge (u,v)
             break
       end if
 end for
end for
```

Việc loại bỏ các cạnh trong GG không làm mất kết nối đồ thị đơn vị đã kết nối với cùng một lý do như là trường hợp cho RNG. Cả hai thuật toán để vẽ đồ thị của mạng phát sóng tiêu tốn thời gian là $O\ (deg^2)$ tại mỗi nút, trong đó deg là mức độ chấp nhận của nút trong đồ thị có phủ sóng đầy đủ.

RNG là một tập hợp con của GG. Điều này phù hợp với các khu vực đã đổ bóng nhỏ được tìm kiếm trong GG, so với trong RNG. Hình 22 cho thấy một đồ thị đơn vị đầy đủ tương ứng với 200 nút đặt ngẫu nhiên trong một khu vực 2000 x 2000m, với phạm vi phủ sóng là 250 m; tập con GG của đồ thị đầy đủ; và các tập con RNG của đồ thị đầy đủ. Lưu ý rằng RNG và GG cung cấp mật độ khác nhau của kết nối bằng cách loại bỏ các số khác nhau của các liên kết. Nhiều lớp MAC chỉ ra

đã làm giảm nhanh hiệu quả như số lượng các trạm gửi hỗ trợ nhau có khả năng truy cập tăng [1], [5]. Hơn nữa, trong khi bất kỳ gói tin một nút truyền độc quyền theo kênh chia sẻ trong phạm vi phủ sóng của nó, các giao thức MAC nhằm giải quyết các vấn đề thiết bị đầu cuối ẩn, bao gồm 802,11 [11], MACA [14], và MACAW [2], sự xác định lan tràn một cách thận trọng tới phạm vi phủ sóng đầy đủ của cả người gửi và người nhận. Theo chế độ như vậy, bằng cách sử dụng các liên kết ít hơn trong định tuyến có thể cải thiện sự đa dạng không gian. Thông thường chúng ta phải tiến hành sắp đặt trước các node sensor theo dạng cố định trong đó có hiện tượng đan chéo xảy ra để mô phỏng hiện tượng này.

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. Bảng này cung cấp tất cả các trạng thái cần thiết cho quyết định chuyển tiếp GPSR, ngoài trạng thái trong chính các gói của chúng.

Các trường header của gói GPSR sử dụng trong chuyển tiếp theo chế độ biên được thể hiện trong Bảng 1. header của gói GPSR bao gồm một trường flag chỉ có các gói tin là trong chế độ tham lam hoặc chế độ chu vi hay đường biên. Tất cả các gói dữ liệu được đánh dấu khởi tạo ở nguồn của chúng là chế độ tham lam. Các nguồn của gói tin cũng bao gồm vị trí địa lý của các điểm đến trong các gói tin. Chỉ một nguồn của gói thiết lập trường vị trí đích; nó được giữ nguyên khi các gói được chuyển tiếp qua mạng. Khi nhận được một gói tin ở chế độ tham lam để chuyển tiếp, một nút tìm kiếm trong bảng hàng xóm của mình để đưa ra những người hàng xóm về địa lý gần đích đến của gói. Nếu người hàng xóm này là gần đến đích, nút chuyển tiếp các gói tin đến người hàng xóm đó. Khi không có hàng xóm là gần gũi hơn, các nút đánh dấu các gói tin vào chế độ biên.

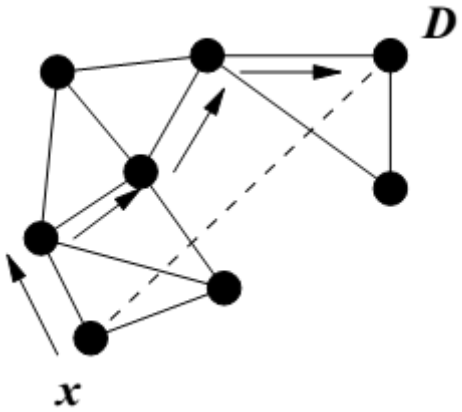
GPSR chuyển tiếp các gói tin chế độ đường biên bằng cách sử dụng một đồ thị phẳng đơn giản. Về bản chất, khi một gói tin đi vào chế độ đường biên tại nút x gắn với nút D, GPSR chuyển nó theo biên của đồ thị phẳng, mỗi trong số đó đã vượt qua bởi đường $\overline{xD}$. Một đồ thị phẳng có hai kiểu face. Mặt trong là những khu vực đa

giác khép kín bao quanh bởi các cạnh của đồ thị. Exterior face là một face không kín bên ngoài ranh giới ngoài của đồ thị. Trên mỗi face, quá trình truyền sử dụng quy tắc bàn tay phải để đạt được một cạnh mà đi qua đường $\overline{xD}$. Ở cạnh đó, quá trình truyền loại bỏ đi các face tiếp giáp được chéo với $\overline{xD}$. Xem Hình 8 cho ví dụ. Lưu ý rằng trong hình, mỗi face được truyền bị xuyên thủng bởi $\overline{xD}$ –Đầu tiên, các face 2 và cuối là các interior face trong khi thứ 3 là exterior face.

Khi một gói tin đi vào chế độ chu vi, GPSR ghi lại trong gói tin vị trí L_p, đặt vị trí nơi mà chuyển tiếp tham lam không thành công. Địa chỉ này được sử dụng tại các bước nhảy tiếp theo để xác định xem các gói tin có thể được trả về cho chế độ tham lam. Mỗi lần GPSR chuyển tiếp một gói trên một face mới, nó ghi lại trong L_f điểm trên $\overline{xD}$ được chia sẻ giữa những face cũ và mới. Lưu ý rằng L_f không phải được đặt tại một nút; $\overline{xD}$ thường là các cạnh giao, như trong hình 8. Cuối cùng, GPSR ghi e0, cạnh đầu tiên (các địa chỉ người gửi và người nhận) một gói tin vượt qua một face mới, trong gói.

Khi nhận được một gói tin theo chế độ đường biên để chuyển tiếp, đầu tiên GPSR so sánh vị trí L_p trong một gói tin theo chế độ đường biên với vị trí của nút sẽ chuyển tiếp. GPSR trả về một gói tin đến chế độ tham lam nếu khoảng cách từ nút chuyển tiếp đến D là ít hơn so với từ Lp để D. Chuyển tiếp theo chu vi này chỉ dùng để phục hồi từ một vị trí maximum; một khi các gói tin đến một vị trí gần hơn so với nơi mà tham lam chuyển tiếp trước đó không thành công với gói đó, các gói tin có thể tiếp tục chuyển tiếp tham lam tới đích mà không có bị quay trở lại vị trí maximum trước đó.

Hình 22. Bên trái là đồ thị đầy đủ của một mạng với 200 nút trong phạm vi triển khai 200x200. Ở giữa là đồ thị GG của đồ thị đầy đủ. Ở bên phải là đồ thị RNG là con của GG và đồ thị đầy đủ.



Hình 23: ví dụ về chuyển tiếp chu vi. D là đích; x là nút trong đó gói tin vào chế độ chuyển tiếp chu vi; các mũi tên là từng bước đi cho việc chuyển tiếp tham lam.

Khi một gói tin đi vào chế độ đường biên tại x, GPSR chuyển nó dọc theo face được giao cắt bởi đường $\overline{xD}$. x chuyển tiếp gói tin tới cạnh đầu tiên ngược chiều kim đồng hồ về x từ đường $\overline{xD}$. Điều này quyết định face đầu tiên mà để chuyển tiếp các gói tin. Sau đó, GPSR chuyển tiếp gói tin xung quanh face đó bằng cách sử dụng quy tắc bàn tay phải. Có hai trường hợp để xem xét: hoặc x và D có kết nối theo đồ thị phẳng, hoặc chúng không.

Khi x và D có kết nối bởi đồ thị, việc đi qua mặt tiếp giáp x theo hai hướng (chúng tôi sử dụng các quy tắc tay phải mô tả trước đây) phải dẫn đến một điểm y mà tại đó $\overline{xD}$ cắt phía xa của face. Đây là trường hợp cho dù face được đi qua là bên trong (interior) hoặc bên ngoài (exterior). Tại y, GPSR đã giảm rõ khoảng cách giữa gói tin và đích của nó, so với gói tin khởi tạo ban đầu vào chế độ đường biên tại x.

Trong khi chuyển xung quanh một face, GPSR xác định nơi mà cạnh tới được chọn tiếp theo hop n cắt $\overline{xD}$. GPSR có các thông tin cần thiết để đưa ra quyết định này, như L_p và D được ghi trong gói tin, và một nút GPSR lưu trữ vị trí riêng của mình và của các hàng xóm. Nếu một nút bao quanh cạnh nơi mà các giao điểm y nói dối, GPSR đặt L_f của gói tin đến y. Tại thời điểm này, các gói tin được chuyển tiếp tới face tiếp theo đang bao quanh điểm y mà là giao cắt bởi $\overline{xD}$. Nút chuyển tiếp gói tin dọc theo cạnh đầu tiên của face tiếp theo bằng quy tắc bàn tay phải, các cạnh tiếp theo ngược chiều kim đồng hồ với chính nó từ n. Cạnh đầu tiên trên face mới được ghi lại trong trường e_0 của gói tin.

Quá trình này lặp đi lặp lại ở face thân hơn với D. Tại mỗi face, các gói tin được chuyển theo quy tắc bàn tay phải cho đến khi tìm cạnh giao cắt với $\overline{xD}$ tại một

điểm y gần hơn trường L_f của gói tin đến đích D. Cuối cùng, face có chứa D được tìm thấy, và quy tắc bàn tay phải dẫn đến D nằm trong face đó.

Khi D là không thể truy cập (ví dụ, nó bị ngắt kết nối từ các đồ thị), hai trường hợp tồn tại: các nút bị mất kết nối giả, hoặc nằm bên trong một interior face, hoặc ngoài một exterior face. GPSR sẽ chuyển tiếp gói tin theo chế độ đường biên cho đến khi gói tin đến face tương ứng. Khi đến interior hoặc exterior face này, gói tin sẽ đi một vòng không thành công xung quanh theo toàn bộ face, mà không tìm thấy một cạnh giao nhau với $\overline{xD}$ tại một điểm gần D hơn Lf. Khi gói tin đi qua cạnh đầu tiên nó phải mất trên face 2 lần thời gian, GPSR thông báo sự lặp lại của chuyển tiếp trên cạnh e0 cạnh được lưu trữ trong gói tin, và chính xác loại bỏ gói tin, vì đích đến là không thể truy cập; đồ thị chế độ đường biên được truyền đi tới một đích đến có thể truy cập không bao giờ gửi một gói tin trên cùng một liên kết trong cùng một hướng hai lần.

Lưu ý rằng GPSR sẽ chuyển tiếp tham lam một gói tin cho nhiều bước nhảy. Nếu đa số các điểm đến không thể truy cập nằm ngoài ranh giới của một địa điểm duy nhất, các gói tin không gửi được có thể tập trung tại một số địa điểm của đồ thị mạng. Hành vi này là hậu quả trực tiếp của khoảng trống trong GPSR cho lưu lượng truy cập giao thức định tuyến vượt qua nhiều bước nhảy từ một điểm đích tới một router chuyển tiếp. Vì vậy, các hệ thống định tuyến liên tục sẽ đẩy một gói tin một khoảng cách rất lớn, với kết quả trả về tiềm năng mà các gói tin sẽ bị loại bỏ bên trong đích AS. Nơi hợp lý nhất cho việc định tuyến không thể tới được xác định là tại nơi hệ thống cuối đang gửi. Các ứng dụng chạy vượt ra mạng được định tuyến GPSR, hoặc bất kỳ mạng nào khác, nên cung cấp một tải phù hợp; người gửi nên cắt giảm tốc độ truyền thông tin phản hồi của họ từ những người nhận.

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.

Để đảm bảo sự phục hồi việc chuyển tiếp địa lý, chúng ta cần phải chắc chắn rằng các nút trung gian thực sự chuyển tiếp các gói tin mà chúng phụ trách (hoặc cung cấp thông tin phản hồi nêu rõ lý do cho việc loại bỏ gói tin). Hãy xem xét các nút A-D hình thành một tuyến đường từ A đến D. Nó là khó cho A để xác minh rằng B có thực sự chuyển tiếp gói tin đến D. Nếu C không nằm trong phạm vi của A, thì C không thể cung cấp thông tin phản hồi. Hơn nữa, do tính chất định tuyến của các tương tác trong GR, A không biết nút nào trong FS của B.

Điều gì cần thiết có trong một kế hoạch xác minh việc chuyển tiếp. Một trong những phương pháp mà A có thể thực hiện là để xác minh B ít nhất có chuyển tiếp gói tin tới một nút nào đó thông qua việc lắng nghe. Khi nút A gửi một gói tin, nó đợi cho tín hiệu thừa nhận ACK từ B, trong khi lắng nghe B để quan sát xem B có chuyển tiếp gói tin hay không.

Chúng tôi lưu ý rằng thử nghiệm việc lắng nghe không phải là một kiểm tra dễ dùng với 2 lý do chính sau:

- Nút A có thể bỏ lỡ việc phát lại do một vụ va chạm với gói khác.
- Nút B có thể chuyển tiếp gói tin, nhưng tới một nút không nằm trong hướng đi hoặc thậm chí đến một nút không tồn tại. Vì A không biết các hàng xóm của B, nó không thể xác định rằng B không chuyển tiếp gói tin một cách chính xác.

Để giải quyết trường hợp đầu tiên, nghĩa là, khi một vụ va chạm xảy ra tại A, một nút cần phải theo dõi hành vi của một người hàng xóm với nhiều gói tin trước khi đánh giá độ tin cậy của nó. Để giải quyết trường hợp thứ hai, một cơ chế để kiểm tra xem các gói tin đang chuyển tiếp của B có chuyển đến đúng một bước nhảy tiếp theo hay không là cần thiết. Ở đây có một số tùy chọn có sẵn. Một lựa chọn là để truy vấn một neo với điểm đến B có chuyển tiếp một gói tin để xác định rằng nó tồn tại và nó gần với đích không. Chúng tôi lưu ý rằng kế hoạch này có thể bị đánh bại bởi 2 cuộc tấn công theo tuần tự và kiểm tra end – to – end là cần thiết cho việc xác minh mạnh hơn của hành vi chuyển tiếp gói tin. Chúng tôi không theo đuổi vấn thêm nữa. Nó xứng đáng để được nghiên cứu riêng mà chúng tôi để lại cho công việc trong tương lai. Thay vào đó, chúng tôi giả định rằng một xác minh chuyển tiếp kiểm tra các tồn tại và sử dụng nó để phù hợp với các mức độ tin cậy, vì đơn giản

chúng tôi giả định rằng các thử nghiệm lắng nghe làm hoạt động như là một kiểm tra xác minh việc chuyển tiếp.

Tùy chọn, chúng tôi có thể chia sẻ thông tin độ tin cậy mà có thể được xây dựng một cách nhanh chóng và chính xác hơn bằng cách cho phép các nút tin tưởng lẫn nhau để định kỳ trao đổi tên những người hàng xóm của họ theo một cách mã hóa an toàn để tạo thành các nhóm đáng tin cậy. Theo cách này, một nút riêng lẻ có thể nhận được nhiều thông tin tin cậy của các hàng xóm bắt nguồn từ quan điểm rộng hơn về các hàng xóm tin cậy của nó. Vì đây là một tính năng tùy chọn, các nút cảm biến có thể được cấu hình để chỉ dựa vào thông tin tin cậy riêng của mình nếu môi trường, ví dụ như một chiến trường, có nhiều thù địch.

Hai tính năng quan trọng trong giải pháp của chúng tôi là: (1) Việc sử dụng đa đường định tuyến để tăng khả năng sử dụng những con đường an toàn. Và (2) quản lý độ tin cậy rõ ràng để xác định các nút hỏng và tránh những con đường sử dụng các nút hỏng này. Mã giả của giao thức chúng ta có như sau:

1. Khi một nguồn s muốn truyền một gói tin hướng tới một điểm đích d cho lần đầu tiên, nó thiết lập một bí mật được chia sẻ với một neo địa phương và các truy vấn neo để nhận thông tin vị trí được xác nhận của những hàng xóm trong phạm vi nhất định, ví dụ như, hai lần khoảng cách truyền thông của mình. Thông tin vị trí có thể được mã hóa và xác thực bằng cách sử dụng khóa chia sẻ.
2. Nguồn bắt đầu phát đi một gói tin quảng bá, gói tin này có thể là một yêu cầu chứng thực để gửi gói tin (RTS) mà bao gồm các vị trí nguồn và đích.
3. Khi nhận được gói tin khởi tạo, một hàng xóm sẽ xác minh và xác thực tính toàn vẹn của gói tin bằng việc sử dụng khóa công khai của người gửi và thêm thông tin điểm nguồn và điểm đích tới bảng định tuyến. Ngoài ra, có sẽ trả về một chứng thực rõ ràng để gửi (CTS) gói tin tới s.
4. Các nguồn tin xác minh tính xác thực của các gói tin CTS nhận được từ hàng xóm. Nếu việc xác minh là thành công thì nó sẽ thêm ID và thông tin của hàng xóm tới bằng định tuyến trừ khi nó đã tồn tại.
5. Tính xác suất chuyển tiếp một gói tin P_i tới một hàng xóm của một bước nhảy $i \in FS$ nơi mà FS là tập các nút mà có vị trí gần với d hơn s và nó có mức tin cậy T_i là lớn hơn hoặc bằng với ngưỡng θ_i. Cụ thể, chúng tôi đặt $P_i = {T_i}/{\sum_{i=1}^{N} T_i}$, Trong đó N là phần tử của FS. (Mô tả chi tiết của T_i khởi tạo và quản lý được đưa ra trong mục 5.2) đã cho $\{P_1, P_2, \dots, P_N\}$, s chọn một cách độc lập k hàng xóm mà nó sẽ chuyển tiếp các gói tin đó với k là mức độ

được yêu cầu dư. Chúng tôi sử dụng kỹ thuật lựa chọn bánh xe rulet [14] để lựa chọn nút, vì nó không có sai lệch trong sự lựa chọn, trong khi việc xem xét ứng viên phù hợp, tức là mức độ tin cậy của nút trong cách tiếp cận của chúng tôi.

6. Các nguồn nhấn chìm gói tin một cách chọn lọc tới k hàng xóm và lắng nghe họ, trong khi chời đợi ACK từ các hàng xóm. Nếu s nghe được một hàng xóm chuyển lại một gói tin thì nó sẽ kiểm tra xem gói tin đã được chuyển đến một vị trí hợp pháp bằng cách tham chiếu tới thông tin vị trí lưu trữ của nó hoặc truy vấn neo, nếu cần thiết, để nhận được các thông tin vị trí có liên quan (lựa chọn việc kiểm tra sự xác minh chuyển tiếp có thể được sử dụng). Xác minh này có thể được thực hiện định kỳ để làm giảm chi phí lắng nghe của nó. Theo kết quả, nó cũng điều chỉnh mức độ tin cậy của những người hàng xóm.
7. Nếu s tìm thấy một nút i mà có độ tin cậy $T_i \geq \theta_2$ mà $\theta_1 < \theta_2$, thì nó trao đổi thông tin tin cậy một cách định kỳ với nút I theo một cách an toàn bảo mật để xây dựng nhiều thông tin tin cậy hơn nữa mà có thể cải tiến thông tin tin cậy riêng của nguồn và ngược lại. (Đây là một bước tùy chọn như đã thảo luận ở trên)
8. Khi nút i nhận được gói tin, nó sẽ trở thành một nguồn mới và quy trình này áp dụng đệ quy để chuyển tiếp các gói tin theo hướng d.

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. Như vậy, gói tin sẽ bị loại do sự cố định tuyến lén lút nhiều hơn hoặc chất lượng truyền thông không dây kém là nguyên nhận chính cho hình phạt. Nói chung, một nút trung thực với chất lượng liên kết tốt hướng tới các điểm đến sẽ ở lại lâu hơn trong FS để hộ trợ GR an toàn.

Khi một nút xây dựng bảng định tuyến như đã thảo luận trong mục 5.1, nó giám sát hành vi của những hàng xóm trong một bước nhảy mà nó sẽ chuyển tiếp các gói tin. (Một bảng định tuyến cũng có thể được mở rộng khi một nút cảm biến được thêm vào khu vực và vị trí của nó được xác minh). Mặc dù có thể có nhiều lựa chọn thay thế, chúng tôi xác định mức độ tin cậy của một nút hàng xóm giữa 0 và 1 tương ứng để chỉ việc không tin cậy và tin cậy hoàn toàn. Khi vị trí của nút I được

xác minh, mức độ tin cậy của nó T_i có trong tập với giá trị khởi đầu nhất định, ví dụ là 0.5.

Nếu nguồn phát hiện một nút hàng xóm i ($\in FS$) đã chuyển thành công một gói tin hướng tới d, nó sẽ làm tăng độ tin cậy của nút i:

$$T_{i_{new}} = \begin{cases} T_i + \delta t \; nếu \; T_i + \delta t \leq 1, \\ 1 \; ngược \; lại \end{cases} \quad (16)$$

Trong đó δt là kích thước bước cụ thể, ví dụ như 0.01.

Như đã thảo luận ở trên, một đối thủ trong FS có thể thả các gói hoặc chuyển tiếp nó đến một nút theo hướng sai, trong khi ACK đang được trả về. Bằng việc lắng nghe, s có thể kiểm tra một hàng xóm i đã thực sự chuyển tiếp các gói tin theo hướng d và có bằng chứng xác nhận độ tin cậy của ACK mà nó nhận được. Cụ thể, khi một nút i bị nghi ngờ làm gián đoạn việc định tuyến thì mức độ tin cậy của nó giảm:

$$T_{i_{new}} = \begin{cases} T_i - \Delta t \; nếu \; T_i - \Delta t > 0, \\ 0 \; ngược \; lại \end{cases} \quad (17)$$

Trong đó Δt là một hình phạt được xác định trước cho mỗi hành vi đáng ngờ. Hơn nữa, thông qua việc trao đổi thông tin độ tin cậy một cách định kỳ với nút j, nút s có thể tiếp tục tham chiếu độ tin cậy của nút i.

Chú ý rằng chúng tôi không loại bỏ một nút ngay lập tức khỏi FS khi nó bị nghi ngờ làm rớt một vài gói tin, bởi vì nó có thể là thành thực nhưng hiện tại bị mất chất lượng, ví dụ như một tắc nghẽn nhỏ thoáng qua. Khi nút được phục hồi từ vấn đề của mạng thì nó có thể góp sức để đảm bảo GR, trong khi độ tin cậy của nó đang được cải thiện. Nếu một nút bị các vấn đề mãn tính của mạng hoặc năng lượng còn lại ít thì nó sẽ dần dần bị loại bỏ khỏi FS.

3.3. 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. Vì vậy kẻ thù buộc phải dựa vào các cuộc tấn công mạnh để lấy khóa riêng liên quan từ khóa công khai. Hoặc nó có thể nắm bắt các nút cảm biến và trích xuất khóa.

Thuật toán quản lý độ tin cậy được cung cấp một cách đầy đủ trong một nút có thể quản lý các mức độ tin cậy của riêng nó. Trong một môi trường tương đối vô hại, ví dụ như, một toàn nhà thông minh, thông tin tin cậy có thể được trao đổi giữa các nút đáng tin cậy với sự chăm sóc cẩn thận. Như vậy, chúng ta có thể cân bằng giữa các thông tin tin cậy nhiều hơn và lỗ hổng bảo mật tiềm tàng do trao đổi thông tin.

Giá trị của ngưỡng được sử dụng để tính toán FS xác định mức độ đáp ứng của giao thức của chúng tôi với một cuộc tấn công có thể phá vỡ việc định tuyến. Nếu ngưỡng của sự lựa chọn ứng viên là cao thì một nút đáng ngờ có thể được loại bỏ trước đó; tuy nhiên, một nút không ác ý có thể bị loại sớm do vấn đề mạng làm việc như là một tắc nghẽn mạng không dây. Vì vậy, nó là cần thiết để đưa ra một giá trị ngưỡng tốt mà có thể cân bằng giữa tốc độ của việc loại trừ nút đáng ngờ và khả năng sai là dương tính. Nói chung, chúng tôi tin rằng không có giá trị ngưỡng duy nhất có thể tối ưu hóa sự cân bằng cho tất cả các ứng dụng, nhưng người ta phải chọn một giá trị thích hợp, ví dụ, bằng cách sử dụng một ngưỡng cao hơn trong một môi trường khắc nghiệt hơn. Quá trình xác minh việc chuyển tiếp (cần thiết cho việc quản lý độ tin cậy) có thể làm tiêu hao năng lượng. Để giảm mức tiêu thụ năng lượng, một nút có thể gọi ngẫu nhiên việc kiểm tra xác minh về một người hàng xóm hay không khi mức năng lượng trở nên thấp. Trong khi đó, nó có thể thu thập thông tin ổn định về độ tin cậy của các hàng xóm.

Ngoài ra, có thể có nhiều lựa chọn thiết kế với chi tiết cụ thể Δt và δt. Khi $\Delta t > \delta t$, ví dụ, chúng ta có thể giảm khoảng thời gian mà một nút bị xâm nhập trong FS để phá vỡ các giao thức. Đây là một cách tiếp cận thận trọng có thể ứng dụng nhiều để quản lý độ tin cậy trong một môi trường thù địch. Ngoài ra, nó cũng có thể quản lý được độ tin cậy theo một cách lạc quan hơn bằng việc thiết lập, ví dụ, $\Delta t \leq \delta t$ khi môi trường được coi là tương đối ổn định (lành tính- benign). Hơn nữa, kích thước tuyệt đối của Δt hay δt xác định sự cân bằng giữa tốc độ hội tụ sự tin cậy và sai là dương tính/ âm tính.

3.3 Kết luận

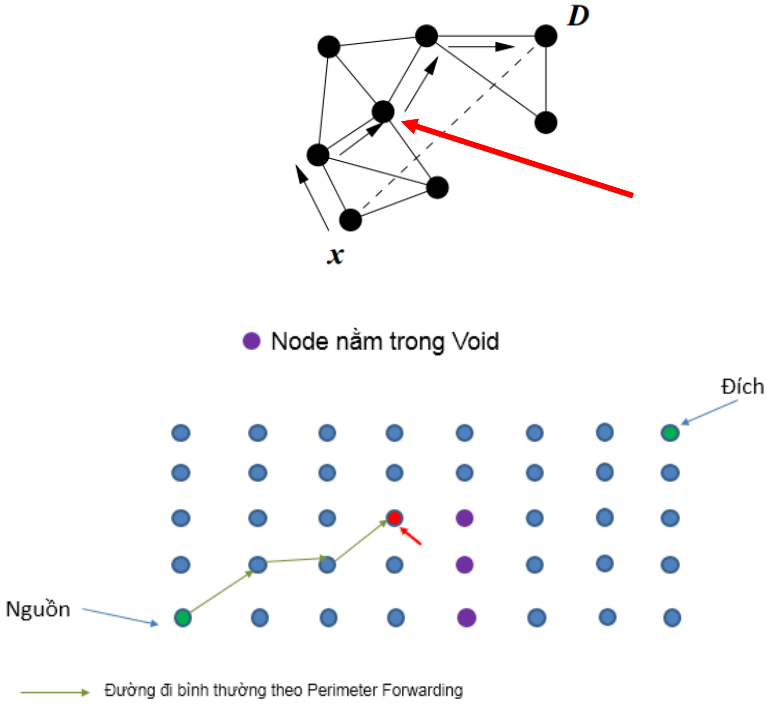
Trong nghiên cứu này, ngay từ đầu chúng tôi luôn mong muốn đưa ra được một giải pháp định tuyến an toàn hoàn chỉnh. Dựa trên bài báo của K.Liu [5] chúng

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 [5] 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

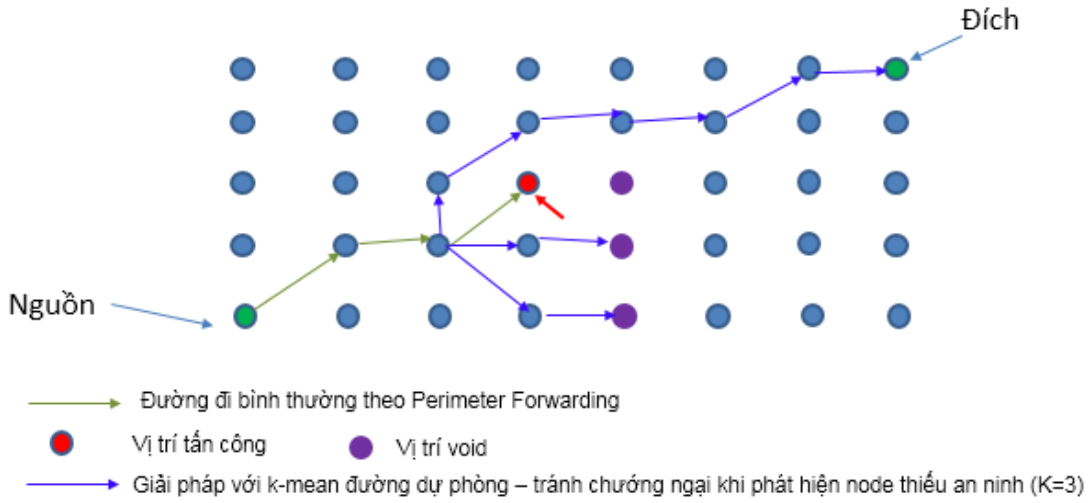
Việc xác định được thông tin vị trí đảm bảo an toàn là phần cốt lõi chính của bài toán chúng tôi đánh giá. Bài toán xác minh này chủ yếu được sử dụng để đảm bảo cho quá trình tiếp theo là định tuyến được thực hiện an toàn. Trong quá trình nghiên cứu chúng tôi phát hiện ra rằng, khi trong mạng xuất hiện 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.

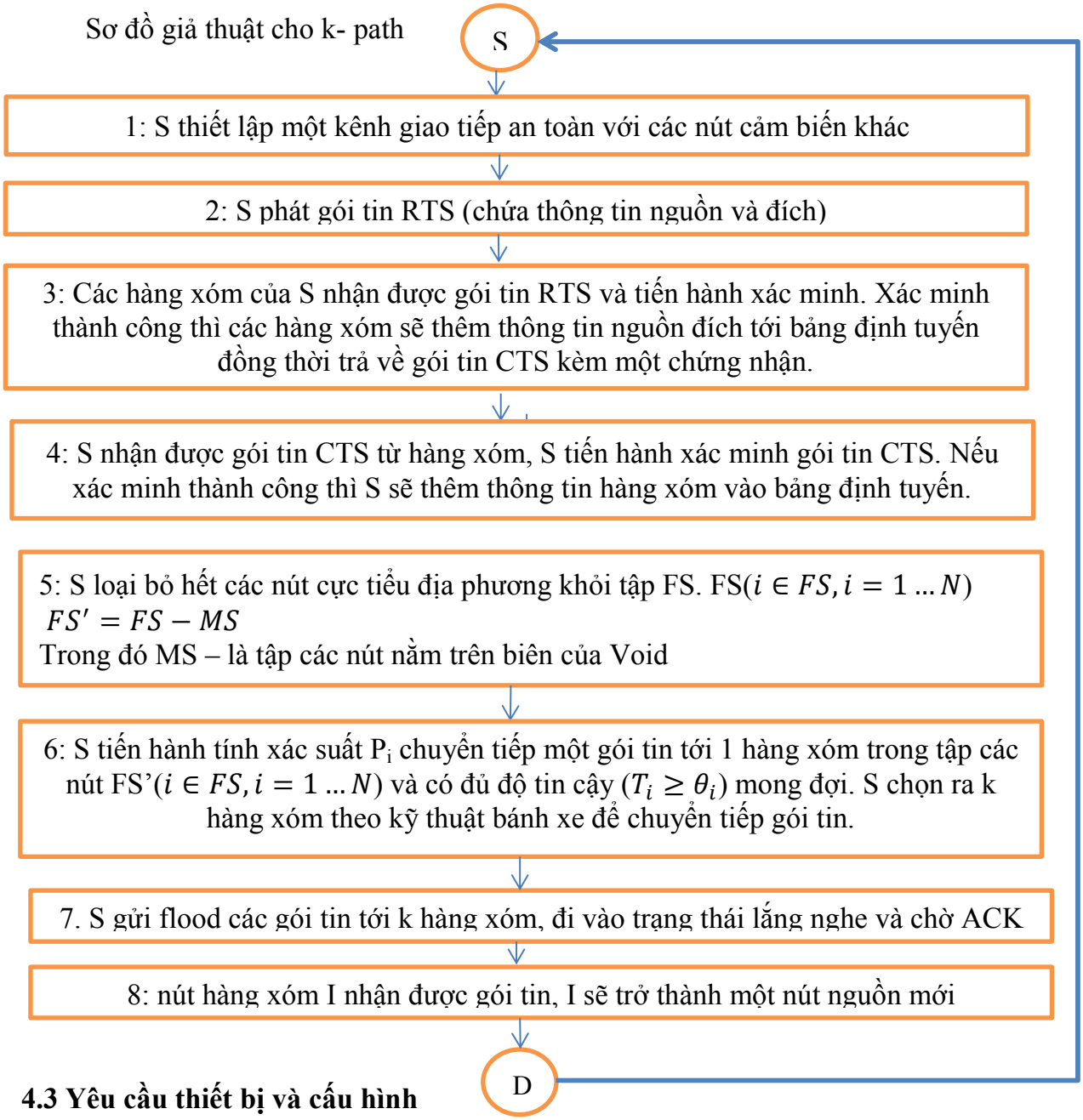
Hiện tại giải thuật RGR do Kliu đề xuất xác định FS – tập các nút hàng xóm có khả năng chuyển tiếp gói tin. Tuy nhiên một số nút vẫn có khả năng chuyển tiếp gói tin, nhưng nằm trên đường biên của Void thì không nên thuộc tuyến. Vì các lý do như sau:

- 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

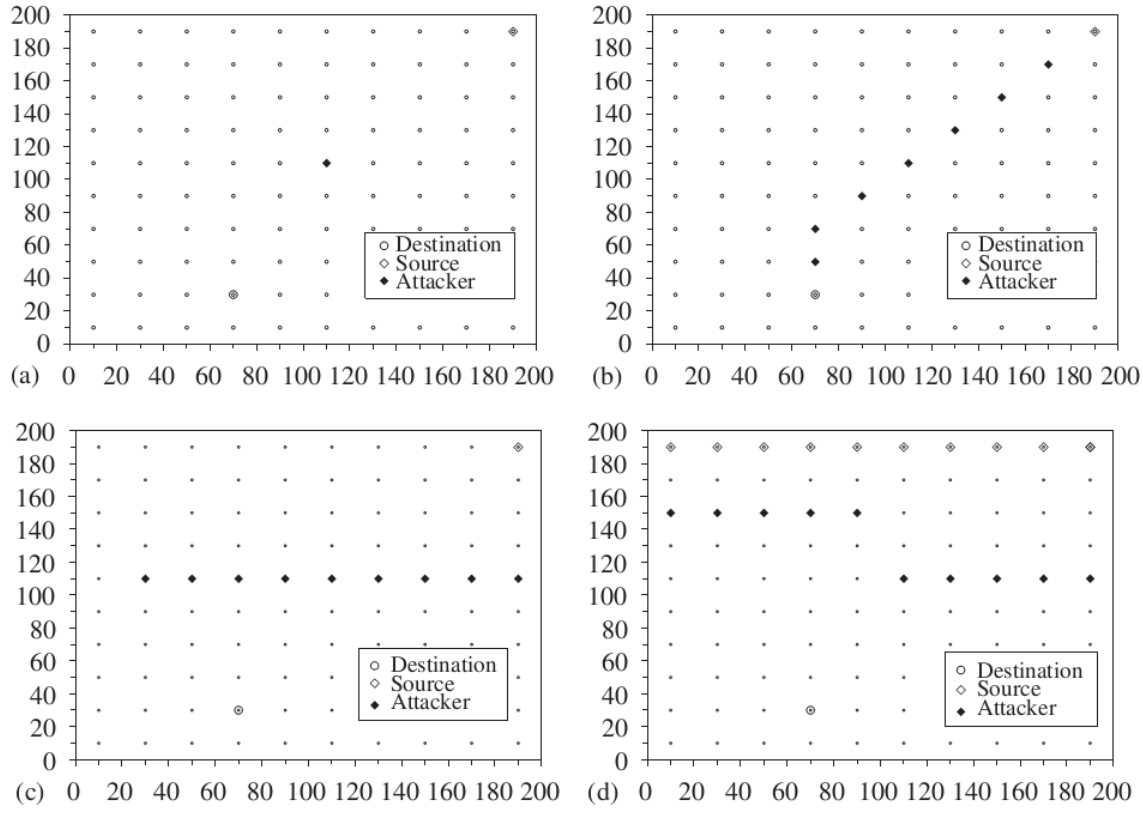
Chương trình mô phỏng được thực hiện trên NS2, là sự mở rộng của giao thức GPSR gọi là RGR (resilient geographic routing) cho mạng cảm biến không dây. Đồng thời thời cũng có một số thay đổi giao thức trong cài đặt IEEE 802.11 để phù hợp với thí nghiệm. Trong thí nghiệm này 100 cảm biến được triển khai 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

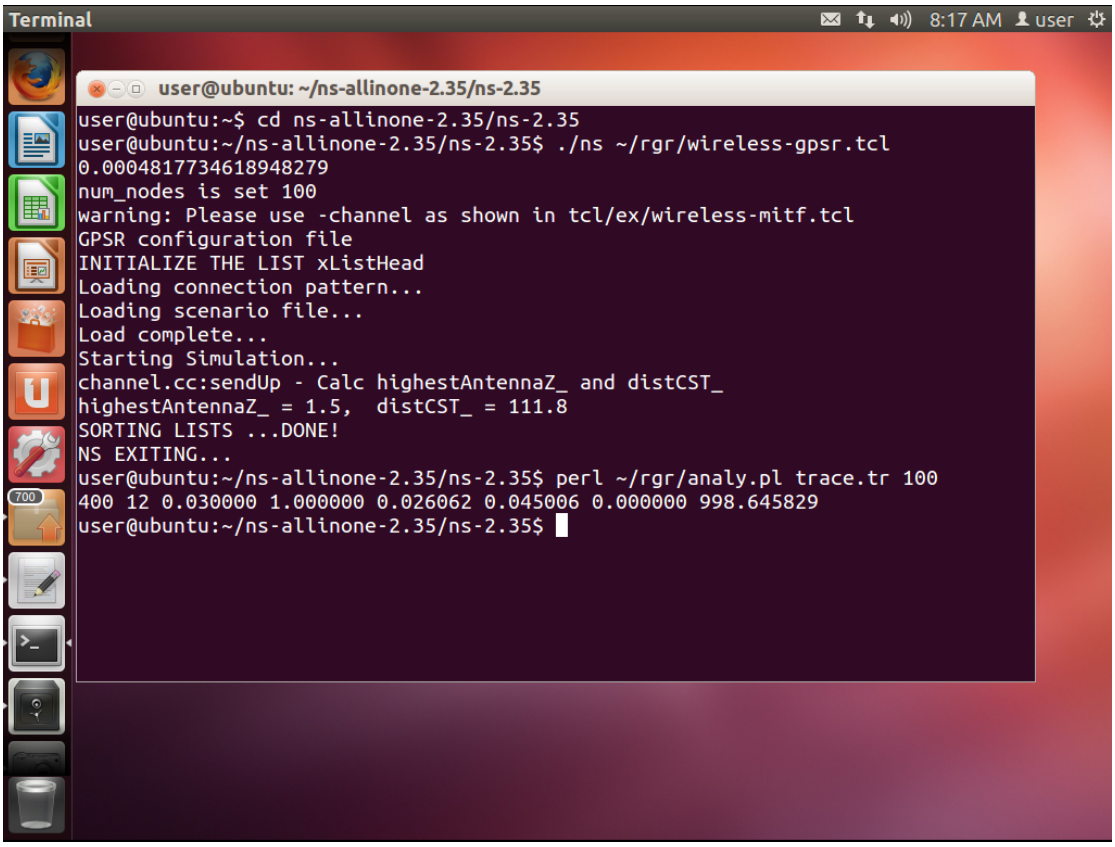
Tham số đo đạc

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:

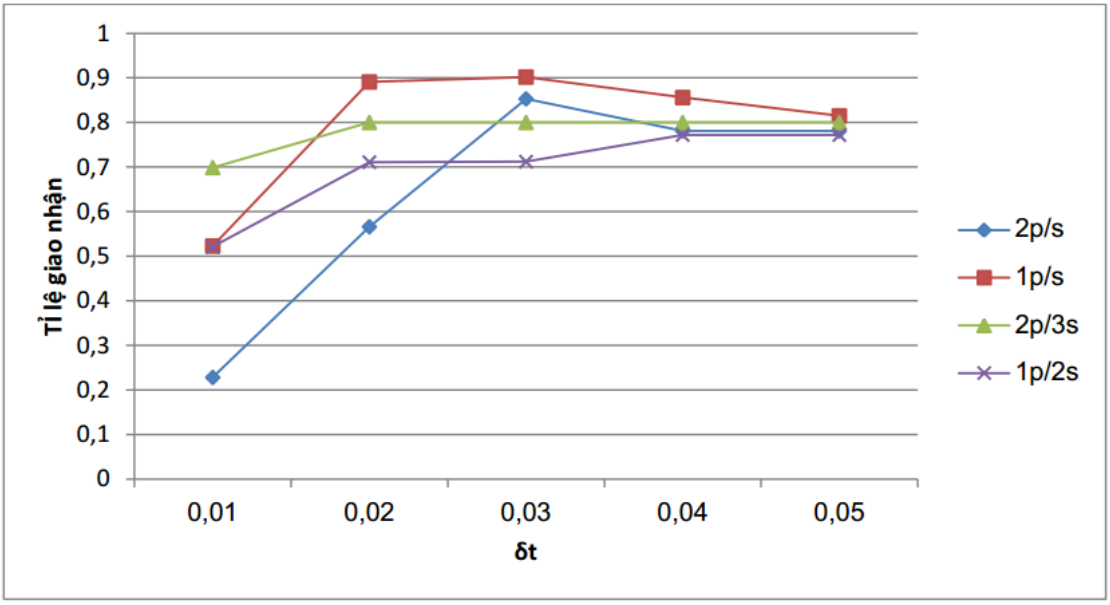
- ✓ Tỉ lệ chuyển tiếp các gói tin đến đích thành công trong các trường hợp có tấn công
- ✓ Tỉ lệ chuyển tiếp các gói tin đến đích thành công trong khi thay đổi chỉ số độ tin cậy.
- ✓ Tỉ lệ chuyển tiếp các gói tin đến đích thành công trong thay đổi chỉ số độ tin cậy và tăng số lượng nút nguồn



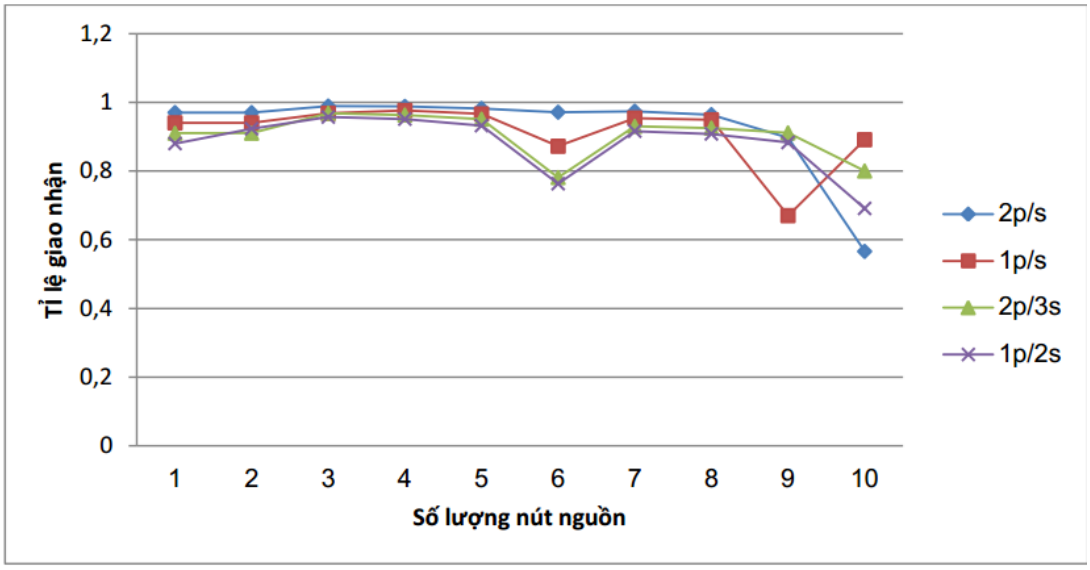
Hình 27. Kết quả chạy thuật toán định tuyến phục hồi

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

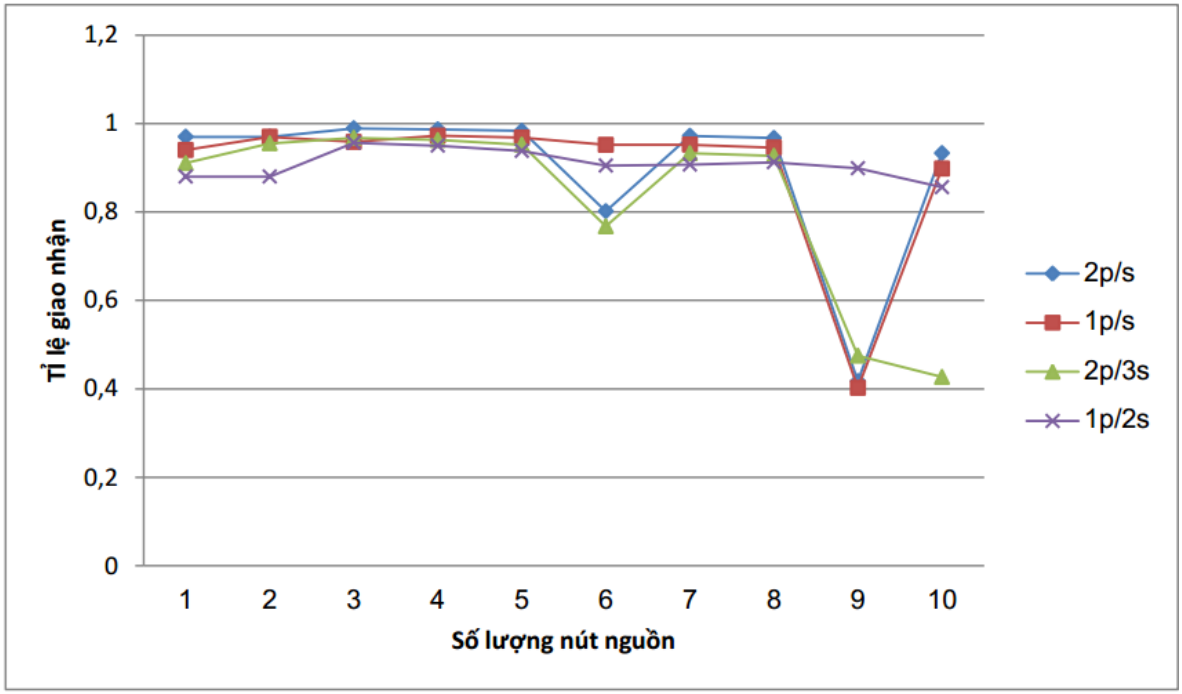
cài đặt giao thức của tác giả (RGR) (các đường khác nhau biểu thị kết quả cho mỗi tốc độ gửi gói tin).



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.

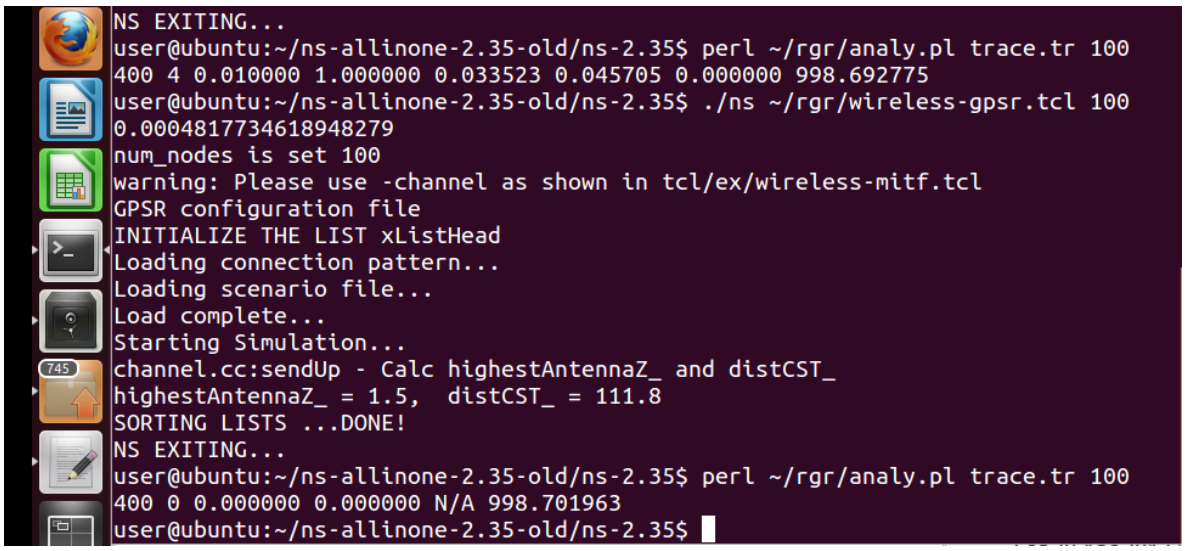
Trong trường hợp cấu hình thêm tấn công lỗ sâu chúng tôi thấy rõ ràng khả năng vượt qua của nó, đó là tín hiệu tốt khi sử dụng đa đường xác suất. Với giao thức mở rộng vừa mới xây dựng và thử nghiệm, nó đã cho thấy một số ưu điểm khi tỉ lệ thưởng là thích đáng và tốc độ truyền tin là phù hợp. Với tỉ lệ thưởng thấp giao thức mới vẫn chưa cho thấy ưu điểm hơn hẳn, khi tăng δt thì ở tốc độ càng cao thì điểm vượt lên của giao thức bổ sung càng sớm và đến cuối khi δt tương đối cao, kết quả đánh giá của các nút riêng biệt cũng sẽ tiến triển nhanh và lợi thế của trao đổi sẽ bị giảm vì cùng tỉ lệ thành công nhưng mất thêm năng lượng.

Tuy nhiên các kết quả trên đây vẫn còn nằm trong một số trường hợp hữu hạn và đa phần dựa vào tỉ lệ gói tin đến đích để đánh giá, một số hiệu ứng phụ xảy ra nhiều hơn mong muốn và nên làm rõ thêm trong các trường hợp riêng biệt.

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.

TÀI LIỆU THAM KHẢO

[1] U. S. a. D. W. N. Sastry, "Secure Verification of Location Claims," in *ACM Workshop Wireless Security (WiSe)*, 2003.

[2] A. P. a. D. J. Y. Hu, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," in *INFOCOM*, 2003.

[3] M. C. a. M. S. S. Capkun, "Secure Localization with Hidden and Mobile Base Stations," in *IEEE INFOCOM*, 2006.

[4] S. C. a. J. Hubaux, "Secure Positioning of Wireless Devices with Application to Sensor Networks," in *IEEE INFOCOM*, 2005.

[5] N. A.-G. K.-D. K. Ke Liu, "Location verification and trust management for resilient geographic routing," in *Proceedings of the First IEEE/ACM Workshop on QoS and Security in Wireless Networks (Q2SWinet 2005)*, 2006.

[6] Y. L. X.-Y. L. Zheng Yang, "Beyond Trilateration: On the Localizability of Wireless Ad-hoc Networks," in *IEEE INFOCOM*, 2009.

[7] S. M. I. a. Y. G. M. I. Yawen Wei, "Lightweight Location Verification Algorithms for Wireless Sensor Networks," *IEEE transactions on parallel and distributed systems,* pp. Vol.24, no.5, May 2013.

[8] Z. Y. a. Y. G. Y. Wei, "Location verification algorithms for wireless sensor networks," in *Proceedings of ICDCS*, June 2007.

[9] J. H. a. D. E. N. Bulusu, "GPS-less low cost outdoor localization for very small devices," *IEEE Personal Communications Magazine,* pp. 28-34, 2000.

[10] A. V. a. M. Nesterenko, "Secure location verification using radio broadcast," pp. vol. 3, no. 4, pp. 377–385, 2006.

[11] S. V. J. M. a. D. A.-A. E. Ekici, "Secure prob-abilistic location verification in randomly deployed wireless sensor networks," in *Ad Hoc Networks*, 2008.

[12] E. S. a. F. K. T. Leinmuller, "Position verification approaches for vehicular ad hoc networks," *IEEE Wireless Communications,* pp. vol. 13, no. 5, pp. 16–21, 2006.

[13] H. T. K. Brad Karp, "GPSR: Greedy Perimeter Stateless Routing for Wireless," in *MobiCom*, Harvard University, 2000.

[14] Y. Z. a. F. Z. J. Liu, "Robust distributed node localization with error management," in *Proceedings of MobiHoc*, 2006.

[15] S. B. a. D. Chaum, "Distance-Bounding Protocols," in *Workshop the Theory and Application of Cryptographic Techniques on Advances in Cryptology EUROCRYPT '93)*, 1994.

[16] C.-C. H. a. M. S. A. Savvides, "Dynamic fine-grained localization in ad-hoc networks of sensors," in *Pro-ceedings of MobiCom*, Rome, Italy, 2001.

[17] L. F. a. P. N. W. Du, "LAD: Localization Anomaly Detection for Wireless Sensor Networks," in *IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS '05)*, 2005.

[18] K. R. M. C. a. M. S. S. Capkun, "Secure location verification with hidden and mobile base stations," *IEEE Transactions on Mobile Computing,* pp. vol. 7, no. 4, pp. 470–483, 2008.

[19] R. P. a. S. C. L. Lazos, "ROPE: Robust Position Estimation in Wireless Sensor Networks," in *Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN '05)*, 2006.