BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG
---------o0o---------

TÌM HIỂU KIẾN TRÚC INTERNET MỞ RỘNG CHO MẠNG CẢM NHẬN

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY
NGÀNH CÔNG NGHỆ THÔNG TIN

Sinh viên thực hiên: Phạm Văn Nam
Giáo viên hướng dẫn: Ths. Nguyễn Trọng Thể
Mã số sinh viên: 110778

LỜI CẢM ƠN

Để có thể hoàn thành được đồ án tốt nghiệp này, em đã được học hỏi những kiến thức quí báu từ các thầy, cô giáo của Trường Đại Học Dân Lập Hải Phòng trong suốt bốn năm đại học. Em vô cùng biết ơn sự dạy dỗ, chỉ bảo tận tình của các thầy, các cô trong thời gian học tập này.

Em xin bày tỏ lòng biết ơn tới thầy Nguyễn Trọng Thể - Khoa công nghệ thông tin – Trường Đại Học Dân Lập Hải Phòng đã tận tình chỉ bảo và định hướng cho em nghiên cứu đề tài này. Thầy đã cho em những lời khuyên quan trọng trong suốt quá trình hoàn thành đồ án. Cuối cùng, em xin cảm ơn gia đình và bạn bè luôn tạo điều kiện thuận lợi, động viên và giúp đỡ em trong suốt thời gian học tập, cũng như quá trình nghiên cứu, hoàn thành đồ án này.

Do hạn chế về thời gian thực tập, tài liệu và trình độ bản thân, bài đồ án của em không thể tránh khỏi những thiếu sót, rất mong các thầy cô góp ý và sửa chữa để bài đồ án tốt nghiệp của em được hoàn thiện hơn. Em xin chân thành cảm ơn!

Sinh viên

Phạm Văn Nam

MỤC LỤC

DANH MỤC HÌNH VẼ

Từ viết tắt	Từ tiếng anh
WSN	Wireless Sensor Network
TDOA	Time difference of arrival
AOA	Angle of arrival
TOA	Time of arrival
ES	Evolution Strategies
RSSI	Received Signal Strength Indicator
TOF	Time of flight
AHLoS	Ad-Hoc Localization System
RF	Radio frequency
MAC	Media Access Control
LESS	Localization Using Evolution Strategies in Sensornets
ADC	Analog to Digital Converter
ID	Identification
GPS	Global Positioning System

GIỚI THIỆU

Ngày nay dưới sự phát triển rất mạnh mẽ của khoa học kĩ thuật nói chung và công nghệ thông tin nói riêng, mạng cảm nhận không dây ra đời là một trong những thành tựu cao của công nghệ chế tạo và công nghệ thông tin. Một trong các lĩnh vực của mạng cảm nhận không dây (Wireless Sensor Network – WSN) là sự kết hợp của việc cảm nhận, tính toán và truyền thông vào trong các thiết bị nhỏ gọn đáp ứng nhu cầu ngày càng cao của con người cũng như phục vụ ngày một tốt hơn cho lợi ích của con người, làm cho con người không mất quá nhiều sức lực, nhân công nhưng hiệu quả công việc vẫn cao. Sức mạnh của WSN nằm ở chỗ khả năng triển khai một số lượng lớn các thiết bị nhỏ có khả năng tự thiết lập cấu hình của hệ thống. Sử dụng những thiết bị này để theo dõi theo thời gian thực, cũng có thể để giám sát điều kiện môi trường, theo dõi cấu trúc hoặc tình trạng thiết bị.

Trong những nghiên cứu mới nhất hiện nay thì hầu hết các ứng dụng của WSN là giám sát môi trường từ xa hoặc có thể mang theo một thiết bị nhỏ gọn nhưng có sức mạnh có thể làm việc hiệu quả không kém một hệ thống thiết bị cồng kềnh. Ví dụ như có thể ứng dụng WSN vào trong công việc phòng cháy rừng bằng rất nhiều nút cảm biến tự động kết nối thành một hệ thống mạng không dây để có thể ngay lập tức phát hiện những vùng có khả năng cháy và gây cháy có thể đưa ra cảnh báo hoặc báo động cần thiết. Một trong những ưu điểm lớn của mạng không dây WSN là chi phí chiển khai và lắp đặt được giảm thiểu, dễ dàng lắp đặt vì kích thước nhỏ gọn, dễ sử dụng.Thay vì hàng ngàn km dây dẫn thông qua các ống dẫn bảo vệ, người lắp đặt chỉ làm công việc đơn giản là đặt thiết bị đã được lắp đặt nhỏ gọn vào vị trí cần thiết. Mạng có thể được mở rộng theo ý muốn và mục đích sử dụng của WSN, rất đơn giản ta chỉ việc thêm vào các thiết bị, linh kiện không cần thao tác phức tạp.

Trước xu thế phát triển nhanh chóng của mạng cảm nhận không dây, căn cứ vào tình hình thực tế của nước ta đang cần các hệ thống giám sát các thông số trong môi trường để phục vụ cho nhiều nghành, nhiều lĩnh vực đồ án đã chọn hướng nghiên cứu là Mô hình mạng cảm nhận không dây – WSN.

Đồ án gồm những phần sau:

Chương 1: Cho cái nhìn tổng quan về sensornet và những ưu nhược điểm trong việc ứng việc triển khai cũng như những ứng dụng của chúng.

Chương 2: Tổng quan về khung giao thức Ipv6 trên kiến trúc sensornet. Nêu một số đặc điểm cũng như cách đánh địa chỉ ứng dụng trên IEEE 802.15.4

Chương 3: Trình bày một số kiểu nén header và thuật toán nén header Ipv6

Chương 4: Tìm hiểu về định tuyến Ipv6 trên kiến trúc sensornet

CHƯƠNG 1: TỔNG QUAN VỀ MẠNG CẢM NHẬN KHÔNG DÂY

1.1 Giới thiệu

Trong những năm gần đây, rất nhiều mạng cảm biến không dây đã và đang được phát triển và triển khai cho nhiều các ứng dụng khác nhau như: theo dõi sự thay đổi của môi trường, khí hậu, giám sát các mặt trận quân sự, phát hiện và do thám việc tấn công bằng hạt nhân, sinh học và hoá học, chuẩn đoán sự hỏng hóc của máy móc, thiết bị, theo dấu và giám sát các bác sỹ, bệnh nhân cũng như quản lý thuốc trong các bệnh viên, theo dõi và điều khiển giao thông, các phương tiện xe cộ...

Hơn nữa với sự tiến bộ công nghệ gần đây và hội tụ của hệ thống các công nghệ như kỹ thuật vi điện tử, công nghệ nano, giao tiếp không dây, công nghệ mạch tích hợp, vi mạch phần cảm biến, xử lý và tính toán tín hiệu...đã tạo ra những con cảm biến có kích thước nhỏ, đa chức năng, giá thành thấp, công suất tiêu thụ thấp, làm tăng khả năng ứng dụng rộng rãi của mạng cảm biến không dây.

Một mạng cảm biến không dây là một mạng bao gồm nhiều nút cảm biến nhỏ có giá thành thấp, và tiêu thụ năng lượng ít, giao tiếp thông qua các kết nối không dây, có nhiệm vụ cảm nhận, đo đạc, tính toán nhằm mục đích thu thập, tập trung dữ liệu để đưa ra các quyết định toàn cục về môi trường tự nhiên.

- Mạng cảm biến có một số đặc điểm sau:

-Truyền thông không tin cậy, quảng bá trong phạm vi hẹp và định tuyến multihop.

- Cấu hình mạng dày đặc và khả năng kết hợp giữa các nút cảm biến thay đổi thường xuyên phụ thuộc vào fading và hư hỏng ở các nút..0

- Các giới hạn về mặt năng lượng, công suất phát, bộ nhớ và công suất tính toán Chính những đặc tính này đã đưa ra những chiến lược mới và những yêu cầu thay đổi trong thiết kế mạng cảm biến.

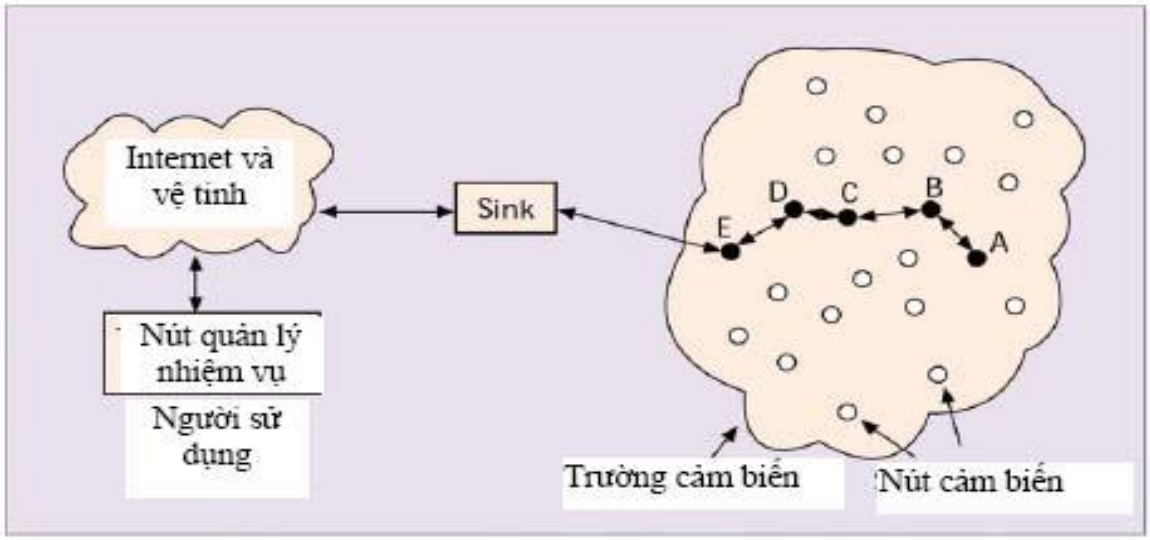
1.2 Cấu trúc của WSN

1.2.1 Các yếu tố ảnh hưởng đến cấu trúc mạng cảm biến

Các cấu trúc hiện nay cho mạng Internet và mạng adhoc không dây không dùng được cho mạng cảm biến không dây, do một số lý do sau: nút cảm biến trong mạng cảm biến có thể lớn gấp nhiều lần số lượng trong mạng adhoc. Các nút cảm biến chủ yếu sử dụng truyền thông kiểu quảng bá, trong khi hầu hết các mạng adhoc đều dựa trên việc truyền điểm-điểm.

Các nút cảm biến bị giới hạn về năng lượng, khả năng tính toán và bộ nhớ.Các nút cảm biến có thể không có số nhận dạng toàn cầu (global identification) (ID) vì chúng có một số lượng lớn mào đầu và một số lượng lớn các nút cảm biến.

Các nút cảm biến được phân bố trong một sensor field như hình 1.1. Mỗi một nút cảm biến có khả năng thu thập dữ liệu và định tuyến lại đến các sink.



Hình 1.1. Phân bố node cảm biến trong trường cảm biến

Dữ liệu được định tuyến lại đến các sink bởi một cấu trúc đa điểm như hình vẽ trên. Các sink có thể giao tiếp với các nút quản lý nhiệm vụ (task manager node) qua mạng Internet hoặc vệ tinh.

Sink là một thực thể, tại đó thông tin được yêu cầu . Sink có thể là thực thể bên trong mạng (là một nút cảm biến) hoặc ngoài mạng. Thực thể ngoài mạng có thể là một thiết bị thực sự ví dụ như máy tính xách tay mà tương tác với mạng cảm biến, hoặc cũng đơn thuần chỉ là một gateway mà nối với mạng khác lớn hơn như

Internet nơi mà các yêu cầu thực sựđối với các thông tin lấy từ một vài nút cảm biến trong mạng.

1.2.2 Cấu tạo Node cảm biến

Các đơn vị cảm biến (sensing units) bao gồm cảm biến và bộ chuyển đổi tương tự-số. Dựa trên những hiện tượng quan sát được, tín hiệu tương tự tạo ra bởi sensor được chuyển sang tín hiệu số bằng bộ ADC, sau đó được đưa vào bộ xử lý.

Đơn vị xử lý thường được kết hợp với bộ lưu trữ nhỏ (storage unit), quyết định các thủ tục làm cho các nút kết hợp với nhau để thực hiện các nhiệm vụ định sẵn. Phần thu phát vô tuyến kết nối các nút vào mạng.

Một trong số các phần quan trọng nhất của một nút mạng cảm biến là bộ nguồn. Các bộ nguồn thường được hỗ trợ bởi các bộ phận lọc như là tế bào năng lượng mặt trời. Ngoài ra cũng có những thành phần phụ khác phụ thuộc vào từng ứng dụng Ngoài kích cỡ ra các nút cảm biến còn một số ràng buộc nghiêm ngặt khác, như là phải tiêu thụ rất ít năng lượng, hoạt động ở mật độ cao, có giá thành thấp, có thể tự hoạt động, và thích biến với sự biến đổi của môi trường.

1.2.3 Đặc điểm của cấu trúc mạng cảm biến:

Khả năng chịu lỗi: Một số các node cảm biến có thể không hoạt động nữa do thiếu năng lượng, do những hư hỏng vật lý hoặc do ảnh hưởng của môi trường. Khả năng chịu lỗi thể hiện ở việc mạng vẫn hoạt động bình thường, duy trì những chức năng của nó ngay cả khi một số node mạng không hoạt động.

Khả năng mở rộng: Khi nghiên cứu một hiện tượng, số lượng các node cảm biến được triển khai có thể đến hàng trăm nghìn node, phụ thuộc vào từng ứng dụng mà con số này có thể vượt quá hàng trăm nghìn node. Do đó cấu trúc mạng phải có khả năng mở rộng để phù hợp với từng ứng dụng cụ thể.

Giá thành sản xuất: Vì mạng cảm nhận bao gồm một số lượng lớn các node cảm biến nên chí phí mỗi node là rất quan trọng trong việc điều chỉnh chi phí mạng. Do vậy chi phí cho mỗi node cảm biến phải giữ ở mức thấp.

Tích hợp phần cứng: Vì số lượng node cảm biến trong mạng là nhều nên node cảm biến cần phải có các ràng buộc phần cứng sau: kích thước nhỏ, tiêu thụ

năng lượng ít, chi phí sản xuất thấp, thích ứng với môi trường, có khả năng tự cấu hình và hoạt động không cần sự giám sát.

Môi trường hoạt động: Các node cảm biến thường là khá dày đặc và phân bố trực tiếp trong môi trường (kể cả môi trương ô nhiễm, độc hại hay dưới nước,...) => node cảm biến phải thích ứng với nhiều loại môi trường và sự thay đổi của môi trường.

Các phương tiện truyền dẫn: Ở mạng cảm nhận, các node được kết nối với nhau trong môi trường không dây, môi trường truyền dẫn có thể là sóng vô tuyến, hồng ngoại hoặc những phương tiện quang học. Để thết lập được sự hoạt động thống nhất chung cho các mạng này thì các phương tiện truyền dẫn phải được chọn phù hợp trên toàn thê giới.

Cấu hình mạng cảm nhận: Mạng cảm nhận bao gồm một số lượng lớn các node cảm biến, do đó phải thiết lập một cấu hình ổn định.

Sự tiêu thụ năng lượng: Mỗi node cảm biến được trang bị nguồn năng lượng giới hạn. Trong một số ứng dụng, việc bổ sung nguồn năng lượng là không thể thực hiện. Vì vậy thời gian sống của mạng phụ thuộc vào thời gian sống của node cảm biến, thời gian sống của node cảm biến lại phụ thuộc vào thời gian sống của phin. Do vậy, hiện nay các nhà khoa học đang nỗ lực tìm ra các giải thuật và giao thức thiết kế cho node mạng nhằm tiết kiệm nguồn năng lượng hạn chế này.

1.3 Kiến trúc giao thức mạng cảm nhận

Kiến trúc này bao gồm các lớp và các mặt phẳng quản lý. Các mặt phẳng quản lý này làm cho các node có thể làm việc cùng nhau theo cách có hiệu quả nhất, định tuyến dữ liệu trong mạng cảm nhận di động và chia sẻ tài nguyên giữa các node cảm biến.

Mặt phẳng quản lý công suất : Quản lý cách cảm biến sử dụng nguồn năng lượng của nó. Ví dụ : nút cảm biến có thể tắt bộ thu sau khi nhận được một bản tin. Khi mức công suất của con cảm biến thấp, nó sẽ broadcast sang nút cảm biến bên cạnh thông báo rằng mức năng lượng của nó thấp và nó không thể tham gia vào quá trình định tuyến .

Mặt phẳng quản lý di động : có nhiệm vụ phát hiện và đăng ký sự chuyển động của các nút. Các nút giữ việc theo dõi xem ai là nút hàng xóm của chúng.

Mặt phẳng quản lý nhiệm vụ : Cân bằng và sắp xếp nhiệm vụ cảm biến giữa các nút trong một vùng quan tâm. Không phải tất cả các nút cảm biến đều thực hiện nhiệm vụ cảm nhận ở cùng một thời điểm.

Lớp vật lý : có nhiệm vụ lựa chọn tần số, tạo ra tần số sóng mang, phát hiện tín hiệu, điều chế và mã hóa tín hiệu. Băng tần ISM 915 MHZ được sử dụng rộng rãi trong mạng cảm biến. Vấn đề hiệu quả năng lượng cũng cần phải được xem xét ở lớp vật lý, ví dụ : điều biến M hoặc điều biến nhị phân.

Lớp liên kết dữ liệu : lớp này có nhiệm vụ ghép các luồng dữ liệu, phát hiện các khung (frame) dữ liệu, cách truy nhập đường truyền và điều khiển lỗi. Vì môi trường có tạp âm và các nút cảm biến có thể di động, giao thức điều khiển truy nhập môi trường (MAC) phải xét đến vấn đề công suất và phải có khả năng tối thiểu hoá việc va chạm với thông tin quảng bá của các nút lân cận.

Lớp mạng : Lớp mạng của mạng cảm biến được thiết kế tuân theo nguyên tắc sau :

- Hiệu quả năng lượng luôn luôn được coi là vấn đề quan trọng.
- Mạng cảm biến chủ yếu là tập trung dữ liệu.
- Tích hợp dữ liệu chỉđược sử dụng khi nó không cản trở sự cộng tác có hiệu quả của các nút cảm biến.

Lớp truyền tải : chỉ cần thiết khi hệ thống có kế hoạch được truy cập thông qua mạng Internet hoặc các mạng bên ngoài khác.

Lớp ứng dụng : Tuỳ theo nhiệm vụ cảm biến, các loại phần mềm ứng dụng khác nhau có thể được xây dựng và sử dụng ở lớp ứng dụng.

1.4 Đặc điểm của WSN

Node mạng có tài nguyên hạn chế: Năng lực xử lí yếu, bộ nhớ hạn chế, truyền thông tốc độ thấp.

Dữ liệu hướng hoạt động: Node mạng phụ vụ như một công cụ để lấy dữ liệu từ thế giới bên trong. Một node có thể thay thế một cá nhân để lấy mẫu tại một vị trí nguy hiểm

Mô hình truyền thông mới: Có lưu lượng dữ liệu thông thường được chuyển từ nhiều nguồn tới đích, hoặc là dữ liệu dược thu thập hoặc chuyển tiếp qua các chặng để đáp ứng với các truy vấn, hoặc tổng hợp dữ liệu liên quan.

Quy mô lớn: Có số lượng node cảm biến rất lớn và có quy mô thay đổi

Yêu cầu thời gian thực: Một số ứng dụng yêu cầu xử lí dữ liệu tức thì

1.5 Sự khác nhau giữa WSN và mạng truyền thống

Dựa vào sự trình bày ở trên, ta dễ dàng nhận thấy sự khác nhau giữa WSN và các mạng truyền thống:

- Số lượng node cảm biến trong một mạng cảm nhận lớn hơn nhiều lần so với những node trong các mạng truyền thống.
- Các node cảm biến thường được triển khai với mật độ dày hơn.
- Những node cảm biến dễ hỏng, ngừng hoạt động hơn.
- Cấu trúc mạng cảm nhận thay đổi khá thường xuyên.
- Mạng cảm nhận chủ yếu sử dụng truyền thông quảng bá, trong khi đó đa số các mạng truyền thống là điểm – điểm.
- Những node cảm biến có giới hạn về năng lượng, khả năng tính toán và bộ nhớ.
- Những node cảm biến có thể không có số định dạng toàn cầu (global identification) (ID).
- Truyền năng lượng hiệu quả qua các phương tiện không dây
- Chia sẻ nhiệm vụ giữa các node láng giềng

1.6 Những thách thức của WSN

Để WSN thực sự trở nên rộng khắp trong các ứng dụng, một số thách thức và trở ngại chính cần vượt qua:

- Vấn đề về năng lượng.
- Năng lực xử lý, tính toán.
- Bộ nhớ lưu trữ.
- Thích ứng tốt với môi trường.
- Ngoài ra, còn có một số thách thức và trở ngại thứ yếu như: vấn đề mở rộng mạng, giá thành các node, quyền sở hữu,…

1.7 Ứng dụng của WSN

Như trên ta đã đề cập đến các lĩnh vực ứng dụng mạng cảm biến không dây.Cụ thể ta sẽ xem xét kỹ một sốứng dụng như sau để hiểu rõ sự cần thiết của mạng cảm biến không dây.

Các mạng cảm biến có thể bao gồm nhiều loại cảm biến khác nhau như cảm biến động đất, cảm biến từ trường tốc độ lấy mẫu thấp, cảm biến thị giác, cảm biến hồng ngoại, cảm biến âm thanh, radar... mà có thể quan sát vùng rộng các điều kiện xung quanh đa dạng bao gồm:

- Nhiệt độ
- Độẩm
- Sự chuyển động của xe cộ
- Điều kiện ánh sáng
- Áp suất
- Sự hình thành đất
- Mức nhiễu
- Sự có mặt hay vắng mặt một đối tượng nào đó
- Mức ứng suất trên các đối tượng bị gắn
- Đặc tính hiện tại như tốc độ, chiều và kích thước của đối tượng

Các nút cảm biến có thểđược sử dụng để cảm biến liên tục hoặc là phát hiện sự kiện, số nhận dạng sự kiện, cảm biến vị trí và điều khiển cục bộ bộ phận phát động. Khái niệm vi cảm biến và kết nối không dây của những nút này hứa hẹn nhiều vùng ứng dụng mới. Chúng ta phân loại các ứng dụng này trong quân đội, môi trường, sức khỏe, gia đình và các lĩnh vực thương mại khác.

1.7.1 Ứng dụng trong quân đội

Mạng cảm biến không dây có thể tích là một phần tích hợp trong hệ thống điều khiển quân đội, giám sát, giao tiếp, tính toán thông minh, trinh sát, theo dõi mục tiêu. Đặc tính triển khai nhanh, tự tổ chức và có thể bị lỗi của mạng cảm biến làm cho chúng hứa hẹn kỹ thuật cảm biến cho hệ thống trong quân đội. Vì mạng cảm biến dựa trên sự triển khai dày đặc của các nút cảm biến có sẵn, chi phí thấp và sự phá hủy của một vài nút bởi quân địch không ảnh hưởng đến hoạt động của quân đội cũng như sự phá hủy các cảm biến truyền thống làm cho khái niệm mạng cảm biến là ứng dụng tốt đối với chiến trường. Một vài ứng dụng quân đội của mạng cảm biến là quan sát lực lượng, trang thiết bị, đạn dược, theo dõi chiến trường do thám địa hình và lực lượng quân địch, mục tiêu, việc đánh giá mức độ nguy hiểm của chiến trường, phát hiện và do thám việc tấn công bằng hóa học, sinh học, hạt nhân.

Giám sát chiến trường: địa hình hiểm trở, các tuyến đường , đường mòn và các chỗ eo hẹp có thể nhanh chóng được bao phủ bởi mạng cảm biến và gần như có thể theo dõi các hoạt động của quân địch. Khi các hoạt động này được mở rộng và

kế hoạch hoạt động mới được chuẩn bị một mạng mới có thểđược triển khai bất cứ thời gian nào khi theo dõi chiến trường.

Giám sát địa hình và lực lượng quân địch: mạng cảm biến có thể được triển khai ở những địa hình then chốt và một vài nơi quan trọng, các nút cảm biến cần nhanh chóng cảm nhận các dữ liệu và tập trung dữ liệu gửi về trong vài phút trước khi quân địch phát hiện và có thể chặn lại chúng. Đánh giá sự nguy hiểm của chiến trường: trước và sau khi tấn công mạng cảm biến có thểđược triển khai ở những vùng mục tiêu để nắm được mức độ nguy hiểm của chiến trường.

Phát hiện và thăm dò các vụ tấn công bằng hóa học, sinh học và hạt nhân. Trong các cuộc chiến tranh hóa học và sinh học đang gần kề, một điều rất quan trọng là sự phát hiện đúng lúc và chính xác các tác nhân đó. Mạng cảm biến triển khai ở những vùng mà được sử dụng như là hệ thống cảnh báo sinh học và hóa học có thể cung cấp các thông tin mang ý nghĩa quan trọng đúng lúc nhằm tránh thương vong nghiêm trọng.

1.7.2 Ứng dụng trong môi trường

Một vài ứng dụng môi trường của mạng cảm biến bao gồm theo dõi sự di cư của các loài chim, các động vật nhỏ, các loại côn trùng, theo dõi điều kiện môi trường mà ảnh hưởng đến mùa màng và vật nuôi; việc tưới tiêu, các thiết bịđo đạc lớn đối với việc quan sát diện tích lớn trên trái đất, sự thăm dò các hành tinh, phát hiện sinh-hóa, nông nghiệp chính xác, quan sát môi trường, trái đất, môi trường vùng biển và bầu khí quyển, phát hiện cháy rừng, nghiên cứu khí tượng học và địa lý, phát hiện lũ lụt, sắp đặt sự phức tạp về sinh học của môi trường và nghiên cứu sự ô nhiễm.

Phát hiện cháy rừng: vì các nút cảm biến có thểđược triển khai một cách ngẫu nhiên, có chiến lược với mật độ cao trong rừng, các nút cảm biến sẽ dò tìm nguồn gốc của lửa để thông báo cho người sử dụng biết trước khi lửa lan rộng không kiểm soát được. Hàng triệu các nút cảm biến có thểđược triển khai và tích hợp sử dụng hệ thống tần số không dây hoặc quang học. Cũng vậy, chúng có thểđược trang bị cách thức sử dụng công suất có hiểu quả như là pin mặt trời bởi vì các nút cảm biến bị bỏ lại không có chủ hàng tháng và hàng năm. Các nút cảm biến sẽ cộng tác với nhau để thực hiện cảm biến phân bố và khắc phục khó khăn, như các cây và đá mà ngăn trở tầm nhìn thẳng của cảm biến có dây.

1.7.3 Ứng dụng trong chăm sóc sức khỏe

Một vài ứng dụng về sức khỏe đối với mạng cảm biến là giám sát bệnh nhân, các triệu chứng, quản lý thuốc trong bệnh viện, giám sát sự chuyển động và xử lý bên trong của côn trùng hoặc các động vật nhỏ khác, theo dõi và kiểm tra bác sĩ và bệnh nhân trong bệnh viện.

Theo dõi bác sĩ và bệnh nhân trong bệnh viện : mỗi bệnh nhân được gắn một nút cảm biến nhỏ và nhẹ, mỗi một nút cảm biến này có nhiệm vụ riêng, ví dụ có nút cảm biến xác định nhịp tim trong khi con cảm biến khác phát hiện áp suất máu, bác sĩ cũng có thể mang nút cảm biến để cho các bác sĩ khác xác định được vị trí của họ trong bệnh viện.

1.7.4 Ứng dụng trong gia đình

Trong lĩnh vực tựđộng hóa gia đình, các nút cảm biến được đặt ở các phòng để đo nhiệt độ. Không những thế, chúng còn được dùng để phát hiện những sự dịch chuyển trong phòng và thông báo lại thông tin này đến thiết bị báo động trong trường hợp không có ai ở nhà.

1.8 Tại sao phải sử dụng Sensornets và IP

Giao thức Internet hay địa chỉ IP là một con số nhận biết từng người gửi hoặc người nhận thông tin gửi qua Internet. Ngành công nghiệp máy tính đã sử dụng Giao thức Internet IPv4 cho các địa chỉ này kể từ khi giao thức này được phát triển. Nay công nghệ này đã đạt đến các giới hạn kỹ thuật để hỗ trợ cho các địa chỉ Internet duy nhất. Với việc các địa chỉ IPv4 đang dần cạn kiệt vào năm nay, toàn bộ ngành công nghiệp Internet phải chấp nhận một giao thức mới - IPv6 - hỗ trợ nhiều địa chỉ hơn, hoặc rủi ro chi phí tăng và chức năng online bị hạn chế cho người dùng Internet ở khắp nơi. Trình trạng thiếu hụt địa chỉ IPv4 đang gia tăng và IPv6 là câu trả lời. IPv6 sẽ mang đến cho Internet một số lượng địa chỉ IP khả dụng lớn hơn rất nhiều - hơn 340 nghìn tỷ - cho phép nhiều thiết bị và người dùng hơn trên Internet cũng như sự linh động trong việc cấp phát địa chỉ và hiệu quả đối với lưu lượng định tuyến.

Những tiến bộ đáng kể trong việc nghiên cứu sensornet và ipv6 đã giúp chúng ta có hiểu biết tốt hơn về những thách thức cho các ứng dụng sensornet.

Sự phát triển của IEEE 802.15.4 tạo tiền đề cho sự phát triển mạng năng lượng ít, chi phí thấp, và yêu cầu số lượng các ứng dụng sensornet nhiều.

IPv6 cũng có những bước phát triển mạnh mẽ, thông qua kiến trúc địa chỉ IPv6, sensornet đã giải quyết các vấn đề về khả năng mở rộng một không gian địa chỉ lớn, khả năng tự động cấu hình, linh hoạt hơn trong mô hình giao tiếp và khả năng mở rộng thông qua các giao thức.

Nhờ những tiến bộ đáng kể đó, đây chính là cơ hội để hình thành cơ sở nghiên cứu sensornet. Đồ án này, trình bày việc áp dụng IPv6 dựa trên kiến trúc sensornet để khẳng định rằng IPv6 và sensornet có thể triển khai được trong thực tế. Hầu hết, các yêu cầu kết nối mạng của sensornet là được triển khai bởi kiến trúc IPv6. Cơ chế phát triển trong sensornet cung cấp giải pháp tốt cho các vấn đề chưa được giải quyết tối ưu bởi giải pháp thông thường của IETF. Các nhà nghiên cứu sensornet có xu hướng tập trung nhiều hơn vào các thuật toán giao thức mạng và các cơ chế, chứ không phải là mạng trong một ý nghĩa rộng hơn. Việc thiếu một kiến trúc mạng rõ ràng cho sensornet đã làm cho sensornet khó tạo ra bước đột phá, dẫn đến khó khăn trong việc xác định vấn đề nghiên cứu.

Có thể nói rằng việc triển khai IPv6 trong sensornet hiệu quả hơn khi so sánh với IPv4. IPv6 sử dụng một không gian địa chỉ lớn hơn nhiều và Header lớn hơn đáng kể. IPv6 bao gồm các chức năng bổ sung mà trước đó chưa được coi là một phần cốt lõi của IPv4 như Multicast, Phát hiện láng giềng, Tự động cấu hình và Giao thức. Chính điều này đã làm cho IPv6 thuyết phục hơn IPv4 trong việc triển khai cho sensernet. Không gian địa chỉ IPv6 đơn giản hơn IPv4 cho phép loại bỏ các yêu cầu về phân giải địa chỉ, sử dụng không cần giám sát, dễ dàng cấu hình và quản lý, những tính năng này rất phù hợp với nhu cầu ứng dụng của sensornet.

Nhưng ngay cả khi IPv6 có những lợi ích bổ sung thì vẫn còn nhiều vấn đề quan trọng vẫn cần được hỗ trợ IPv6 dựa trên kiến trúc mạng trong sensornet. Tầng mạng IPv6 đòi hỏi một lớp liên kết mạnh và hiệu quả cho nguồn năng lượng thấp. Liên kết phải cho phép lớp mạng đạt được nỗ lực cao nhất trong việc chuyển datagram mà vẫn tôn trọng nguồn năng lượng và bộ nhớ hạn chế. Giao thức định tuyến phải cung cấp khả năng tiếp cận trong khi tham gia vào liên kết năng động.

1.9 Kết luận:

Trong chương này đã trình bày tổng quan về mạng cảm nhận không dây, các thách thức trong thiết kế, triển khai cùng với những ứng dụng của nó trong đời sống. Mạng cảm nhận không dây đang phát triển một cách mạnh mẽ và trở thành một lĩnh vực nghiên cứu được nhiều nhà khoa học quan tâm, đặc biệt là việc thiết kế các giao thức định tuyến hiệu quả trong việc tiết kiệm năng lượng. Trong chương tiếp theo em xin trình bày một số giao thức định tuyến phổ biến đã được triển khai trong mạng cảm nhận không dây.

CHƯƠNG 2: GIAO THỨC IPV6

2.1 Sự ra đời của IPv6

Khi đưa ra chuẩn của IPv4 thì IETF cũng đã tiên đoán được về sự thay thế của nó nhưng họ nghĩ là cần 10 năm để giải quyết các vấn đề còn tồn tại của IPv4. Nhưng đến năm 1990 với sự phát triển nhanh của mạng Internet và WWW đã làm cho IPv4 không thể đáp ứng kịp thời cùng với sự phát triển đó.Không gian địa chỉ IPv4 hiện tại không thể đáp ứng thoả đáng cùng với sự tăng nhanh của người sử dụng Internet từ khắp thế giới mặc dù đã có rất nhiều kĩ thuật nhằm làm tăng tuổi thọ của IPv4 như NAT, CIDR hay DHCP. Nhưng điều này cũng chỉ là giải pháp mang tính tạm thời chứ không thể giải quyết một cách triệt để được hết hai tồn tại sâu xa của IPv4 đó chính là:

Sự giới hạn mạng tính nguyên tắc của không gian địa chỉ IPv4.

Tốc độ phát triển của mạng Internet quá nhanh làm cho dung lượng bảng định tuyến ở các bộ định tuyến tăng nhanh. Điều này làm cho các bộ định tuyến không đủ sức chứa hết các thông tin về định tuyến.

Trước tình hình trên, cộng sự phát triển như vũ bão của các thiết bị không dây, các thiết bị điều khiển, các thiết bị hổ trợ các máy cá nhân số,… đòi hỏi phải có một công nghệ mới ra đời nhằm khắc phục được những vấn đề mà IPv4 không giải quyết một cách triệt để được. Thách thức mà IETF phải đối mặt đó chính là việc lựa chọn một công nghệ Internet thế hệ mới IPng(Internet Protocol next generation) như thế nào để có thể đáp ứng được sự đòi hỏi của thị trường. Nhưng một vấn đề đặt ra là IPng phải tương thích ngược với IPv4. Và công nghệ mới đó chính là IPv6. IPv6 được thiết kế đáp ứng lại được yêu cầu của người sử dụng, các chương trình ứng dụng, sự đòi hỏi của chất lượng dịch vụ đồng thời nó cũng đảm bảo tính trong suốt của các ứng dụng đối với người sử dụng với các đặc tính nỗi bật như sau:

Phần mào đầu của IPv6 : được thiết kế với dạng khác hơn so với IPv4 nhằm làm cho kích thước phần mào đầu là nhỏ nhất.

IPv6 có 128 bits nên không gian địa chỉ của IPv6 lớn hơn rất nhiều so với IPv4. Chính điều này tạo điều kiện cho IPv6 có thể phân cấp được nhiều mức hơn mà không cần sử dụng cơ chế dịch địa chỉ NAT.

IPv6 hổ trợ cho cả hai cơ chế đánh địa chỉ stateful và stateless mà không cần dùng đến server DHCP. Với cơ chế đánh địa chỉ stateful, nó cho phép các host hoặc router tự động cấu hình địa chỉ IPv6 cho mình mà không cần đến sự trợ giúp của con người.

Một đặc điểm rất nỗi bật của IPv6 so với IPv4 chính là cơ chế bảo mật. IPv6 được sự hổ trợ một cách mặc định của giao thức IPSec điều này đã tạo ra một giải pháp bảo mật mạng rất hiệu quả.

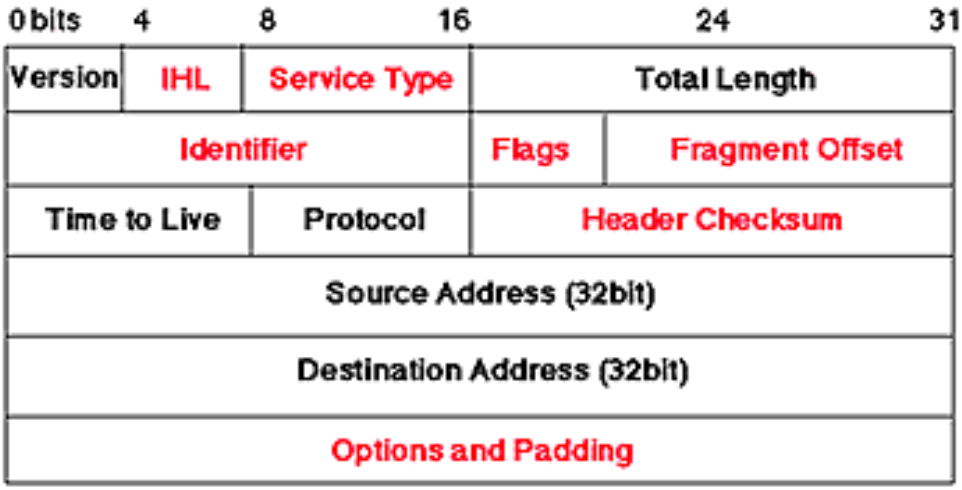
Trong phần mào đầu của IPv6 có sự xuất hiện của trường Flow label. Trường này cho phép router chuyển các gói một cách liên tục nhau từ nguồn đến đích nhằm đảm bảo chất lượng cho các dịch vụ được cung cấp ngay cả khi gói đó được mã hoá trong IPSec.

IPv6 còn cung cấp một đặc điểm ưu tiên nhằm hổ trợ cho các ứng dụng thời gian thực. Nên đây chính là sự lựa chọn của các ứng dụng thời gian thực.

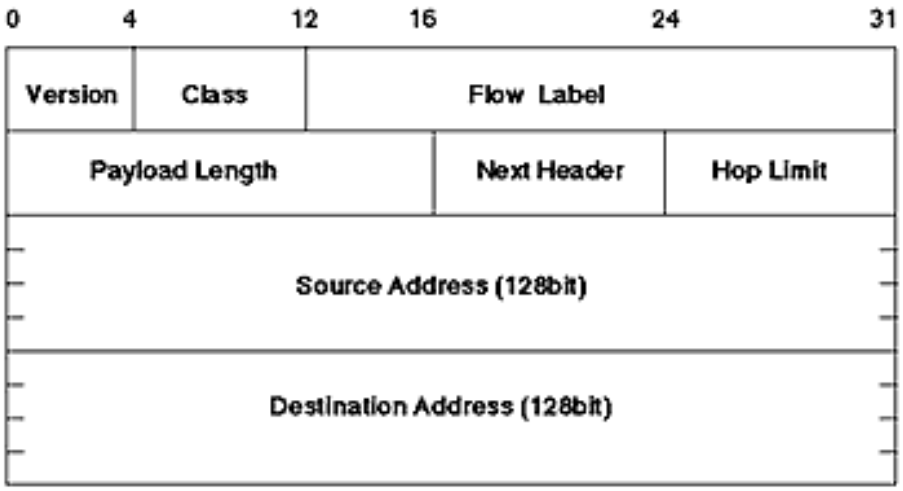
2.2 Khác biệt cơ bản giữa IPv4 header và IPv6 header

IPv6 là một cải tiến về version của thủ tục Internet hiện thời, IPv4. Tuy nhên, nó vẫn là một thủ tục Internet. Một thủ tục là một tập các quy trình để giao tiếp. Trong thủ tục Internet, thông tin như địa chỉ IP của nơi gửi và nơi nhận của gói tin dữ liệu được đặt phía trước dữ liệu. Phần thông tin đó được gọi là header. Cũng tương tự như khi xác định địa chỉ người nhận và người gửi khi bạn gửi một bưu phẩm qua đường thư tín.

Hãy so sánh về header giữa IPv4 và IPv6.



Hình 2.1: IPv4 Header.



Hình 2.2: IPv6 Header

Trường địa chỉ nguồn (Source Address) và địa chỉ đích (Destination Address) có chiều dài mở rộng đến 128 bít.

Mặc dù trường địa chỉ nguồn và địa chỉ đích có chiều dài mở rộng tới gấp 4 lần số bít, song chiều dài header của IPv6 không hề tăng nhiều so với header của IPv4. Đó là bởi vì dạng thức của header đã được đơn giản hoá đi trong IPv6.

Một trong những thay đổi quan trọng là không còn tồn tại trường options trong header của IPv6. Trường Options này được sử dụng để thêm các thông tin về các dịch vụ tuỳ chọn khác nhau. VD thông tin liên quan đến mã hoá có thể được thêm vào tại đây.

Vì vậy, chiều dài của IPv4 header thay đổi tuỳ theo tình trạng. Do sự thay đổi đó, các router điều khiển g`iao tiếp theo những thông tin trong IP header không thể đánh giá chiều dài header chỉ bằng cách xem xét phần đầu gói tin. Điều này làm cho khó khăn trong việc tăng tốc xử lý gói tin với hoạt động của phần cứng.

Trong địa chỉ IPv6 thì những thông tin liên quan đến dịch vụ kèm theo được chuyển hẳn tới một phân đoạn khác gọi là header mở rộng “extension header”. Trong hình vẽ trên là header cơ bản. Đối với những gói tin thuần tuý, chiều dài của header được cố định là 40 byte. Về xử lý gói tin bằng phần cứng, có thể thấy trong IPv6 có thể thuận tiện hơn IPv4.

Một trường khác cũng được bỏ đi là Header Checksum. Header checksum là 1 số sử dụng để kiểm tra lỗi trong thông tin header, được tính toán ra dựa trên

những con số của header. Tuy nhiên, có một vấn đề nảy sinh là header chứa trường TTL (Time to Live), giá trị trường này thay đổi mỗi khi gói tin được truyền qua 1 router. Do vậy, header checksum cần phải được tính toán lại mỗi khi gói tin đi qua 1 router. Nếu giải phóng router khỏi công việc này, chúng ta có thể giảm được trễ.

Thực ra, tầng TCP phía trên tầng IP có kiểm tra lỗi của các thông tin khác nhau bao gồm cả địa chỉ nhận và gửi. Vậy có thể thấy các phép tính tương tự tại tầng IP là dư thừa, nên Header Checksum được gỡ bỏ khỏi IPv6.

Trường có cùng chức năng với "Service Type" được đổi tên là Traffic Class. Trường này được sử dụng để biểu diễn mức ưu tiên của gói tin, ví dụ có nên được truyền với tốc độ nhanh hay thông thường, cho phép thiết bị thông tin có thể xử lý gói một cách tương ứng. Trường Service Type gồm TOS (Type of Service) và Precedence. TOS xác định loại dịch vụ và bao gồm: giá trị, độ tin cậy, thông lượng, độ trễ hoặc bảo mật. Precedence xác định mức ưu tiên sử dụng 8 mức từ 0-7.

Trường Flow Label có 20 bít chiều dài, là trường mới được thiết lập trong IPv6. Bằng cách sử dụng trường này, nơi gửi gói tin hoặc thiết bị hiện thời có thể xác định một chuỗi các gói tin, ví dụ Voice over IP, thành 1 dòng, và yêu cầu dịch vụ cụ thể cho dòng đó. Ngay cả trong IPv4, một số các thiết bị giao tiếp cũng được trang bị khả năng nhận dạng dòng lưu lượng và gắn mức ưu tiên nhất định cho mỗi dòng. Tuy nhiên, những thiết bị này không những kiểm tra thông tin tầng IP ví dụ địa chỉ nơi gửi và nơi nhận, mà còn phải kiểm tra cả số port là thông tin thuộc về tầng cao hơn. Trường Flow Label trong IPv6 cố gắng đặt tất cả những thông tin cần thiết vào cùng nhau và cung cấp chúng tại tầng IP.

IPv6 có mục tiêu cung cấp khung làm việc truyền tải thông minh, dễ dàng xử lý cho thiết bị bằng cách giữ cho header đơn giản và chiều dài cố định.

2.3 Chức năng của header mở rộng (extension header) trong IPv6.

Header mở rộng (extension header) là đặc tính mới trong thế hệ địa chỉ IPv6.

Trong IPv4, thông tin liên quan đến những dịch vụ thêm vào được cung cấp tại tầng IP được hợp nhất trong trường Options của header. Vì vậy, chiều dài header thay đổi tuỳ theo tình trạng.

Khác thế, địa chỉ IPv6 phân biệt rõ ràng giữa header mở rộng và header cơ bản, và đặt phần header mở rộng sau phần header cơ bản. Header cơ bản có chiều dài cố định 40 byte, mọi gói tin IPv6 đều có header này. Header mở rộng là tuỳ

chọn. Nó sẽ không được gắn thêm vào nếu các dịch vụ thêm vào không được sử dụng. Các thiết bị xử lý gói tin (ví dụ router), cần phải xử lý header cơ bản trước, song ngoại trừ một số trường hợp đặc biệt, chúng không phải xử lý header mở rộng. Router có thể xử lý gói tin hiệu quả hơn vì chúng biết chỉ cần nhìn vào phần header cơ bản với chiều dài như nhau.

Header mở rộng được chia thành nhiều loại tuỳ thuộc vào dạng và chức năng chúng phục vụ. Khi nhiều dịch vụ thêm vào được sử dụng, phần header mở rộng tương ứng với từng loại dịch vụ khác nhau được đặt tiếp nối theo nhau.

Trong cấu trúc header IPv6, có thể thấy 8 bít của trường Next Header. Trường này sẽ xác định xem extension header có tồn tại hay không, khi mà header mở rộng không được sử dụng, header cơ bản chứa mọi thông tin tầng IP. Nó sẽ được theo sau bởi header của tầng cao hơn, tức hoặc là header của TCP hay UDP, và trường Next Header chỉ ra loại header như hình 2.2

Mỗi header mở rộng (extension header) cũng chứa trường Next Header và xác định header mở rộng nào sẽ theo sau nó. Node đầu cuối khi nhận được gói tin chức extension header sẽ xử lý các extension header này theo thứ tự được sắp xếp của chúng.

Dạng của extension header

Có 6 loại của extension header: Hop-by-Hop Option, Destination Option, Routing, Fragment, Authentication, and ESP (Encapsulating Security Payload). Khi sử dụng cùng lúc nhiều extension header, thường có một khuyến nghị là đặt chúng theo thứ tự như thế này.

Hop-by-Hop Option

Phía trên có đề cập là thông thường, chỉ có những node đầu cuối xử lý các extension header. Chỉ có một ngoại lệ của quy tắc này là header Hop-by-Hop Option. Header này, như tên gọi của nó, xác định một chu trình mà cần được thực hiện mỗi lần gói tin đi qua một router.

Destination Option

Destination Option header được sử dụng để xác định chu trình cần thiết phải xử lý bởi node đích. Có thể xác định tại đây bất cứ chu trình nào. Chúng tôi đã đề cập là thông thường chỉ có những node đích xử lý header mở rộng của IPv6. Như vậy thì các header mở rộng khác ví dụ Fragment header có thể cũng được gọi là Destination Option header. Tuy nhiên, Destination Option header khác với các header khác ở chỗ nó có thể xác định nhiều dạng xử lý khác nhau.

Routing

Routing header được sử dụng để xác định đường dẫn định tuyến. Ví dụ, có thể xác định nhà cung cấp dịch vụ nào sẽ được sử dụng, và sự thi hành bảo mật cho những mục đích cụ thể. Node nguồn sử dụng Routing header để liệt kê địa chỉ của các router mà gói tin phải đi qua. Các địa chỉ trong liệt kê này được sử dụng như địa chỉ đích của gói tin IPv6 theo thứ tự được liệt kê và gói tin sẽ được gửi từ router này đến router khác tương ứng.

Fragment

Fragment header được sử dụng khi nguồn gửi gói tin IPv6 gửi đi gói tin lớn hơn Path MTU, để chỉ xem làm thế nào khôi phục lại được gói tin từ các phân mảnh của nó. MTU (Maximum Transmission Unit) là kích thước của gói tin lớn nhất có thể gửi qua một đường dẫn cụ thể nào đó. Trong môi trường mạng như Internet, băng thông hẹp giữa nguồn và đích gây ra vấn đề nghiêm trọng. Cố gắng gửi một gói tin lớn qua một đường dẫn hẹp sẽ làm quá tải. Trong địa chỉ IPv4, mối router trên đường dẫn có thể tiến hành phân mảnh (chia) gói tin theo giá trị của MTU đặt cho mỗi giao diện. Tuy nhiên, chu trình này áp đặt một gánh nặng lên router. Bởi vậy trong địa chỉ IPv6, router không thực hiện phân mảnh gói tin (các trường liên quan đến phân mảnh trong header IPv4 đều được bỏ đi).

Node nguồn IPv6 sẽ thực hiện thuật toán tìm kiếm Path MTU, để tìm băng thông hẹp nhất trên toàn bộ một đường dẫn nhất định, và điều chỉnh kích thước gói tin tuỳ theo đó trước khi gửi chúng. Nếu ứng dụng tại nguồn áp dụng phương thức này, nó sẽ gửi dữ liệu kích thước tối ưu, và sẽ không cần thiết xử lý tại tầng IP. Tuy nhiên, nếu ứng dụng không sử dụng phương thức này, nó phải chia nhỏ gói tin có kích thướng lớn hơn MTU tìm thấy bằng thuật toán Path MTU Discovery. Trong trường hợp đó, những gói tin này phải được chia tại tầng IP của node nguồn và Fragment header được sử dụng.

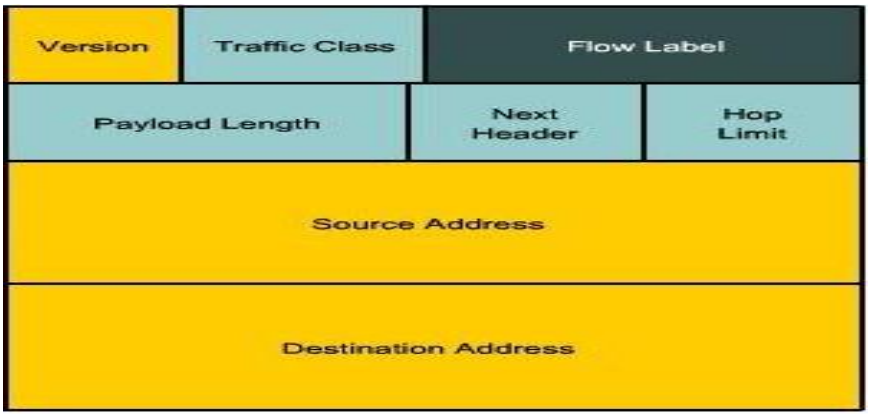
Authentication and ESP

Ipsec là phương thức bảo mật bắt buộc được sử dụng tại tầng IP. Mọi node IPv6 phải thực thi Ipsec. Tuy nhiên, thực thi và tận dụng lại là khác nhau, và Ipsec có thực sự được sử dụng trong giao tiếp hay không phụ thuộc vào thời gian và từng trường hợp. Khi Ipsec được sử dụng, Authentication header sẽ được sử dụng cho xác thực và bảo mật tính đồng nhất của dữ liệu, ESP header sử dụng để xác định những thông tin liên quan đến mã hoá dữ liệu, được tổ hợp

lại thành extension header. Trong IPv4, khi có sử dụng đến Ipsec, thông tin được đặt trong trường Options.

IPv6 ứng dụng một hệ thống tách biệt các dịch vụ gia tăng khỏi các dịch vụ cơ bản và đặt chúng trong header mở rộng (extension header), cao hơn nữa phân loại các header mở rộng theo chức năng của chúng. Làm như vậy, sẽ giảm tải nhiều cho router, và thiết lập nên được một hệ thống cho phép bổ sung một cách linh động các chức năng, kể cả các chức năng hiện nay chưa thấy rõ ràng.

2.4 Khung giao thức IPv6



Hình 2.3. Cấu trúc Header của Ipv6

Version (4 bit): chức năng của trường này giống như IPv4. Nó chứa giá trị 6 cho Ipv6 thay vì 4 cho Ipv4.

Traffic Class (8 bit): trường này thay thế cho trường Type of Service (ToS) trong Header IPv4. Nó được sử dụng để biểu diễn mức ưu tiên của gói tin. Giá trị mặc định của trường này là 0. Nếu một node hỗ trợ một chức năng cụ thể nào đó thì giá trị này sẽ thay đổi. Ngược lại, nếu không hỗ trợ thì nó sẽ giữ nguyên giá trị ban đầu là 0.

Flow Label – Nhãn dòng (20 bit): khi các Router nhận được gói tin đầu tiên của một dòng mới, Flow Label sẽ xử lý thông tin trên Header IPv6, *định tuyến Header* trong các *Header mở rộng*, và lưu trữ kết quả trong một bộ nhớ cache và sử dụng kết quả để định tuyến các gói dữ liệu khác thuộc cùng một dòng, bằng cách sử dụng các dữ liệu được lưu trữ trong bộ nhớ cache.

Payload Length (16 bit): trường này thay thế các trường *Total Length* của Header IPv4. Thay vì đo chiều dài của toàn bộ datagram, nó chỉ chứa số byte tải trọng của gói dữ liệu. Trường này được tính theo Byte, và kích thước tối đa là 64

KB. Trong trường hợp tải trọng gói cao hơn 64KB, một *Jumbo Payload* của *tùy chọn Hop-by-hop* trong *Header mở rộng*, cho phép chuyển các datagram vượt quả 64 KB.

Next Header (8 bit): chỉ rõ Header theo sau Ipv6 Header và nằm ở vị trí đầu của trường Data. Nó có thể là một *Header mở rộng* hoặc giao thức ở lớp cao hơn (TCP và UDP). Trường này tương tự như trường *Protocol* trong IPv4.

Hop Limit (8 bit): Chỉ rõ số Hop tối đa mà gói tin có thể đi qua tương tự trường *TTL* (*Time To Live*) của Ipv4. Node gửi sẽ gán 1 giá trị cho trường này để chỉ tối đa số Hop mà 1 datagram có thể đi qua để tới đích. Tại mỗi node chuyển tiếp giá trị này sẽ được giảm xuống 1. Nếu giá trị này bằng 0, datagram bị bỏ và 1 thông điệp ICMP được gửi lại cho nơi gửi. Chức năng chính của trường này là xác định và loại bỏ các gói tin đang bị mắc kẹt trong một vòng lặp vô hạn vì bất kỳ sai sót thông tin định tuyến nào.

Source Address (128 bit): chứa địa chỉ IP của thiết bị khởi tạo datagram. Như đã nói trong IPv4, trường này luôn luôn chứa địa chỉ của thiết bị ban đầu gửi datagram.

Destination Address (128 bit): chứa địa chỉ đích của node nhận gói tin IPv6. Như đã nói trong IPv4, trường này luôn chứa duy nhất một địa chỉ đến cuối cùng mà thôi.

2.5 Đánh địa chỉ IPv6

Giao diện được cấu hình với một hoặc nhiều địa chỉ, tiền tố IPv6. Bởi vì liên kết IP không cung cấp khả năng tiếp cận ngầm, không có tiền tố sử dụng để xác định có hoặc không có điểm đến trên liên kết, trừ tiền tố liên kết cục bộ. Hạn chế của không gian IP là cách đưa các địa chỉ và tiền tố IPv6 cho các giao diện trong mạng.

Đánh địa chỉ IPv6 phải tuân thủ:

- Một phạm vi đánh địa chỉ IPv6 mới được gọi là phạm vi sensornet, bao gồm cả địa chỉ liên kết cục bộ cho các node là duy nhất trong phạm vi sensornet.

- Yêu cầu của kiến trúc IPv6 phải thiết lập được mô hình giữa IID và địa chỉ liên kết. Điều này cho phép các node giải quyết địa chỉ lớp mạng và lớp liên kết mà không có bất kỳ thông tin hoặc cache phân giải địa chỉ.

- Kiến trúc IPv6 cũng giả định rằng các địa chỉ IPv6 được cấu hình sử dụng tiền tố toàn cầu cho sensornet, hỗ trợ cơ chế nén để làm giảm đáng kể tiêu đề overhead và các yêu cầu cache cho chuyển tiếp và định tuyến.

2.6 Đặc điểm của Ipv6

2.6.1 Tăng kích thước của tầm địa chỉ

IPv6 sử dụng 128 bit địa chỉ trong khi IPv4 chỉ sử dụng 32 bit; nghĩa là Ipv6 có tới 2128 địa chỉ khác nhau; 3 bit đầu luôn là 001 được dành cho các địa chỉ khả định tuyến toàn cầu (Globally Routable Unicast –GRU). Nghĩa là còn lại 2125 địa chỉ. Một con số khổng lồ. Điều đó có nghĩa là địa chỉ IPv6 sẽ chứa 1028 tầm địa chỉ IPv4.

2.6.2 Tăng sự phân cấp địa chỉ

IPv6 chia địa chỉ thành một tập hợp các tầm xác định hay boundary: 3 bit đầu cho phép biết được địa chỉ có thuộc địa chỉ khả định tuyến toàn cầu (GRU) hay không, giúp các thiết bị định tuyến có thể xử lý nhanh hơn. Top Level Aggregator (TLA) ID được sử dụng vì 2 mục đích: thứ nhất, nó được sử dụng để chỉ định một khối địa chỉ lớn mà từ đó các khối địa chỉ nhỏ hơn được tạo ra để cung cấp sự kết nối cho những địa chỉ nào muốn truy cập vào Internet; thứ hai, nó được sử dụng để phân biệt một đường (Route) đến từ đâu. Nếu các khối địa chỉ lớn được cấp phát cho các nhà cung cấp dịch vụ và sau đó được cấp phát cho khách hàng thì sẽ dễ dàng nhận ra các mạng chuyển tiếp mà đường đó đã đi qua cũng như mạng mà từ đó Route xuất phát. Với IPv6, việc tìm ra nguồn của 1 Route sẽ rất dễ dàng. Next Level Aggregator (NLA) là một khối địa chỉ được gán bên cạnh khối TLA, những địa chỉ này được tóm tắt lại thành những khối TLA lớn hơn, khi chúng được trao đổi giữa các nhà cung cấp dịch vụ trong lõi Internet, ích lợi của loại cấu trúc địa chỉ này là: Thứ nhất, sự ổn định về định tuyến, nếu chúng ta có 1 NLA và muốn cung cấp dịch vụ cho các khách hàng, ta sẽ cố cung cấp dịch vụ đầy đủ nhất, tốt nhất. Thứ hai, chúng ta cũng muốn cho phép các khách hàng nhận được đầy đủ bảng định tuyến nếu họ muốn, để tạo việc định tuyến theo chính sách, cân bằng tải... Để thực hiện việc này chúng ta phải mang tất cả các thông tin về đường đi trong Backbone để có thể chuyển cho họ.

2.6.3 Đơn giản hóa việc đặt địa chỉ Host

IPv6 sử dụng 64 bit sau cho địa chỉ Host, trong 64 bit đó có cả 48 bit là địa chỉ MAC của máy, do đó, phải đệm vào đó một số bit đã được định nghĩa trước mà các thiết bị định tuyến sẽ biết được những bit này trên subnet. Ngày nay, ta sử dụng chuỗi 0xFF và 0xFE (:FF:FE: trong IPv6) để đệm vào địa chỉ MAC. Bằng cách này, mọi Host sẽ có một Host ID duy nhất trong mạng. Sau này nếu đã sử dụng hết 48 bit MAC thì có thể sẽ sử dụng luôn 64 bit mà không cần đệm

2.6.4 Việc tự cấu hình địa chỉ đơn giản hơn

Một địa chỉ Multicast có thể được gán cho nhiều máy, địa chỉ Anycast là các gói Anycast sẽ gửi cho đích gần nhất (một trong những máy có cùng địa chỉ) trong khi Multicast packet được gửi cho tất cả máy có chung địa chỉ (trong một nhóm Multicast). Kết hợp Host ID với Multicast ta có thể sử dụng việc tự cấu hình như sau: khi một máy được bật lên, nó sẽ thấy rằng nó đang được kết nối và nó sẽ gửi một gói Multicast vào LAN; gói tin này sẽ có địa chỉ là một địa chỉ Multicast có tầm cục bộ (Solicited Node Multicast address). Khi một Router thấy gói tin này, nó sẽ trả lời một địa chỉ mạng mà máy nguồn có thể tự đặt địa chỉ, khi máy nguồn nhận được gói tin trả lời này, nó sẽ đọc địa chỉ mạng mà Router gửi; sau đó, nó sẽ tự gán cho nó một địa chỉ IPv6 bằng cách thêm Host ID (được lấy từ địa chỉ MAC của interface kết nối với subnet đó) với địa chỉ mạng, Do đó, tiết kiệm được công sức gán địa chỉ IP

2.6.5 Tính di động

IPv6 hỗ trợ tốt các máy di động như laptop. IPv6 giới thiệu 4 khái niệm giúp hỗ trợ tính toán di động gồm: Home address; Care-of address; Binding; Home agent.

Trong IPv6 thì các máy di động được xác định bởi một địa chỉ Home address mà không cần biết hiện tại nó được gắn vào đâu. Khi một máy di động thay đổi từ một subnet này sang subnet khác; nó phải có một Care-of address qua một quá trình tự cấu hình. Sự kết hợp giữa Home address và Care-of address được gọi là một Binding. Khi một máy di động nhận được một Care-of address, nó sẽ báo cho Home agent của nó bằng gói tin được gọi là Binding update để Home agent có thể cập nhật lại Binding cache của Home agent về Care-of address của máy di động vừa gửi. Home agent sẽ duy trì một ánh xạ giữa các Home address và Care-of address và bỏ nó vào Binding cache. Một máy di động có thể được truy cập bằng cách gửi một packet đến các Home address của nó. Nếu máy di động không được kết nối trên subnet của Home agent thì Home agent sẽ gửi packet đó cho máy di động qua Care-of address của máy đó trong Binding cache của Home agent (Lúc này, Home agent được xem như máy trung gian để máy nguồn có thể đến được máy di động). Máy di động sau đó sẽ gửi một gói tin Binding update cho máy nguồn của gói tin. Máy nguồn sau đó sẽ cập nhật Binding cache của nó, thì sau này máy nguồn muốn gửi đến máy di động, chỉ cần gửi trực tiếp đến cho máy di động qua Care-of address chứa trong Binding cache của nó mà không cần phải gửi qua Home address. Do đó, chỉ có gói tin đầu tiên là qua Home agent

2.6.6 Hiệu suất

IPv6 cung cấp các lợi ích sau:

Giảm được thời gian xử lý Header, giảm Overhead vì chuyển dịch địa chỉ: vì trong IPv4 có sử dụng private address để tránh hết địa chỉ, Do đó, xuất hiện kỹ thuật NAT để dịch địa chỉ, nên tăng Overhead cho gói tin. Trong IPv6 do không thiếu địa chỉ nên không cần private address, nên không cần dịch địa chỉ.

Giảm được thời gian xử lý định tuyến: nhiều khối địa chỉ IPv4 được phânphát cho các user nhưng lại không tóm tắt được, nên phải cần các entry trong bảng định tuyến làm tăng kích thước của bảng định tuyến và thêm Overhead cho quá trình định tuyến. Ngược lại, các địa chỉ IPv6 được phân phát qua các ISP theo một kiểu phân cấp địa chỉ giúp giảm được Overhead.

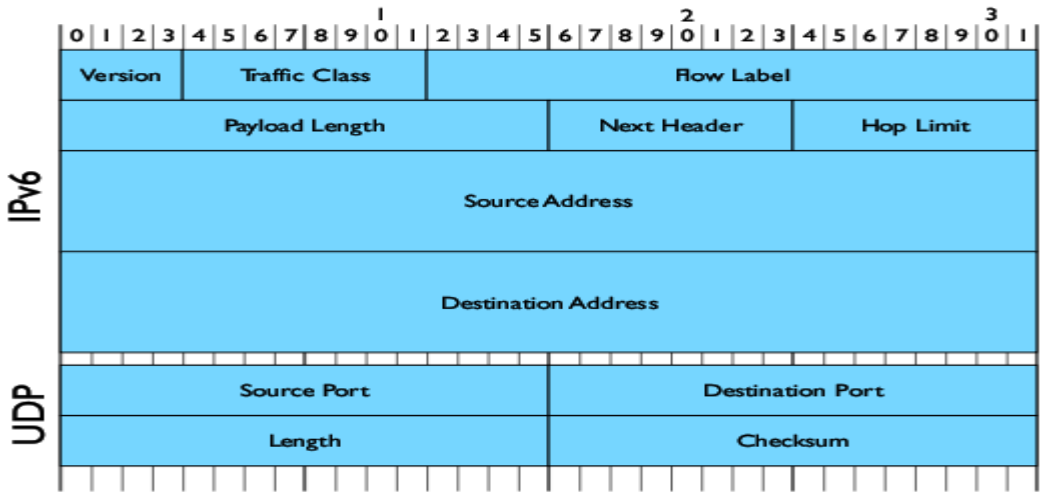
Tăng độ ổn định cho các đường: trong IPv4, hiện tượng route flapping thường xảy ra, trong IPv6, một ISP có thể tóm tắt các route của nhiều mạng thành một mạng đơn, chỉ quản lý mạng đơn đó và cho phép hiện tượng flapping chỉ ảnh hưởng đến nội bộ của mạng bị flapping.

Giảm Broadcast: trong IPv4 sử dụng nhiều Broadcast như ARP, trong khi IPv6 sử dụng Neighbor Discovery Protocol để thực hiện chức năng tương tự trong quá trình tự cấu hình mà không cần sử dụng Broadcast.

Multicast có giới hạn: trong IPv6, một địa chỉ Multicast có chứa một trường scope có thể hạn chế các gói tin Multicast trong các Node, trong các link, hay trong một tổ chức. Không có checksum.

2.7 Nén datagram IPv6

Trong khi lớp thích ứng cho phép giao tiếp với datagram IPv6 sử dụng khung IEEE 802.15.4, nén Header IPv6 là cần thiết để IPv6 truyền thông có tính khả thi trong sensornet. Một chuẩn Header UDP/IPv6 là 48 byte và được hiển thị trong hình 2.4. Mà Header lớp mạng và lớp giao vận là lớn => trong phần này, sẽ trình bày một phương pháp nén Header lớp mạng và lớp giao vận.



Hình 2.4: Header UDP/IPv6

Các Header IPv6 và UDP là tương đối lớn, tương ứng là 40 và 8 byte. Một mình địa chỉ IPv6 sử dụng 32 byte. Nén Header lớp mạng và lớp giao vận là cần thiết để hoạt động hiệu quả

2.8 Vận chuyển datagram IPv6 trên IEEE 802.15.4

Lớp thích ứng nằm hợp lý giữa lớp liên kết và mạng, có trách nhiệm phân mảnh, vận chuyển, và ghép mảnh datagram IPv6. Lớp thích ứng có thể hỗ trợ cơ chế nén Header để giảm chi phí Overhead và tần số phân mảnh datagram IPv6. Lớp thích ứng này hỗ trợ các cơ chế sau:

Phân mảnh: Chia datagram IPv6 thành nhiều khung IEEE 802.15.4 và hỗ trợ IPv6 tối thiểu 1280 byte MTU.

Lớp 2 - Chuyển tiếp: Hỗ trợ các cơ chế giống như MPLS (chuyển tiếp đa giao thức), nghĩa là định tuyến sẽ xảy ra ở lớp 3 và chuyển tiếp sẽ xảy ra ở lớp 2.

Nén Header: Giảm chi phí overhead của Header và nhu cầu phân mảnh bằng cách áp dụng tối ưu hóa và nén các giá trị cross-layer (liên tầng). Hỗ trợ nén Header bằng hai cơ chế flow-independent và flow-based. Flow-independent thu nhỏ trạng của mạng và cho phép lớp mạng linh hoạt để tự động thay đổi tuyến đường trên Hop tiếp theo. Tuy nhiên, flow-based lợi dụng điểm mạnh trong dư thừa của dòng.

CHƯƠNG 3: NÉN HEADER CỦA IPv6 ÁP DỤNG CHO WSN

3.1 Giới thiệu

Việc nén Header ngày càng phổ biến, điều này thông báo sự đa dạng của ứng dụng, trong đó mạng cảm nhận không dây năng lượng thấp (WSN) đang được triển khai. Với quy mô hiện tại và sự tăng trưởng nhanh chóng các triển khai là dấu hiệu cho thấy khả năng WSN có thể được kết nối với một hay nhiều mạng lưới toàn cầu. Nếu điều này xảy ra, thì việc hưởng lợi từ nền IP có sẵn là rất nhiều, nơi tất cả sự can thiệp các node phải có liên quan đến các địa chỉ IP. Khi IPv4 ra khỏi không gian địa chỉ toàn cầu của mình ngay và các ứng dụng của nó, thì địa chỉ IP này không thể coi là hữu hiệu đối với mạng cảm biến. Hơn nữa, nhờ có những khả năng tính toán của các node WSN, nó không thể đem lại lợi ích để có một loại ngăn xếp kép hỗ trợ (IPv6 và IPv4) được cung cấp. Trong bối cảnh đó, IPv6 Low Power Wireless Personal Area Network (Mạng cá nhân không dây năng lượng thấp - 6LoWPAN) là có ý nghĩa.

Phần ứng dụng này đưa ra một cơ chế nén header làm cho overhead là tối thiểu nhất bằng các giả định phù hợp để tiết kiệm tính toán và năng lượng, cung cấp nhiều hơn các byte cho dữ liệu.

Tổng quát một số loại nén

3.1.1 Nén Flow-based

Kỹ thuật nén Header IP truyền thống là flow-based, dựa trên nén dư thừa trong một flow. Kỹ thuật nén flow-based tối ưu hóa "thời gian sống lâu" của flow và cho rằng việc nén và giải nén là trong giao tiếp trực tiếp và độc quyền trên một liên kết là rất hạn chế (ví dụ như modem qua đường điện thoại). Nén flow-based hoạt động liên lớp, nén cả Header lớp mạng và lớp giao vận. Bằng cách dựa trên dư thừa trong một flow, tỉ lệ nén tăng lên theo thời gian và có thể đạt được 1 byte duy nhất cho cả hai Header trong trường hợp tốt nhất.

Nén flow-based đã thành công và được sử dụng rộng rãi. Nén Flow-based yêu cầu việc nén và giải nén thiết lập và duy trì trạng thái cho mỗi dòng. Trong triển khai đa Hop, nén và giải nén phải xảy ra Hop-by-hop, có nghĩa là việc chuyển tiếp phải duy trì trạng thái cho mỗi dòng tại các Hop. Trạng thái yêu cầu tại các node chuyển tiếp có thể ngăn cản việc chuyển tiếp trong các mạng lớn, ngay cả khi mỗi node là một điểm kết thúc trong một dòng duy nhất. Trạng thái nén cho mỗi dòng phải phù hợp giữa việc nén và giải nén, đòi hỏi hoạt động phải hiệu quả giữa một

liên kết với nỗ lực cao trong việc phân gói tin. Tỷ lệ mất mát lớn có thể làm giảm lợi ích nén, như: cố gắng bổ sung để tái đồng bộ hóa trạng thái nén giữa các điểm kết thúc. Các node cũng phải thiết lập lại trạng thái mỗi dòng khi thay các tuyến đường, như: giới hạn nén trong mạng di động và ép tần số mà tại đó các tuyến đường có thể thay đổi.

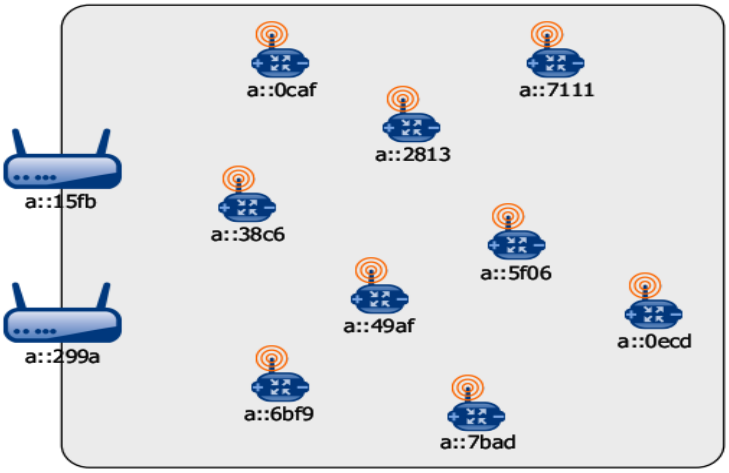
Ban đầu flow-based tối ưu hóa "thời gian sống dài" và tương đối các dòng tốc độ cao, cơ chế flow-based hiện tại không thích hợp cho các dòng tốc độ thấp trong sensornet. Nhiều ứng dụng sensornet chỉ khai báo dữ liệu theo một hướng duy nhất, dựa vào phân gói tin với "nỗ lực cao nhất" chứ không phải là cơ chế tin cậy end-to-end. Thứ hai, flow-based thường gánh chịu đáng kể overhead. Do tốc độ dữ liệu thấp theo hướng chuyển tiếp, mỗi thông điệp yêu cầu một sự chấp nhận rõ ràng. Các kỹ thuật nén flow-based, nén giá trị bằng cách quan sát những điểm chung trong một dòng theo thời gian. Dữ liệu tốc độ thấp nghĩa là nén flow-based có thể mất đáng kể thời gian để tập trung nén tốc độ cao.

3.1.2 Nén Stateless

Nén Header Staless không duy trì trạng thái mỗi flow và do đó flow độc lập. RFC 4944 nén datagram bằng cách khai thác dư thừa liên lớp, bao gồm cả lớp liên kết, mạng, và giao vận. Trường Length luôn bị lược đi, giả định rằng chúng có thể được xác định từ các Header lớp dưới, định danh giao diện IPv6 có thể được lược đi khi chúng được xác định từ các địa chỉ có trong lớp liên kết. Các trường khác được nén bằng cách giả sử giá trị chung và nén các trường hợp thông thường. Ví dụ, phiên bản IPv6 được giả định là 6, Traffic Class và Flow Label được giả định là 0, Next Header được giả định là UDP, TCP hoặc ICMPv6, và tiền tố cho Source Address và Destination Address được giả định là tiền tố liên kết cục bộ. Trong trường hợp tốt nhất, RFC 4944 có thể nén một tiêu đề UDP/IPv6 xuống 6 byte.

3.1.3 Nén shared-context

Nén shared-context đòi hỏi tất cả các node thiết lập một số shared-context. Điều này trái với nén flow-based, nơi mà chỉ có nén / giải nén trạng thái hình thành và duy trì flow. Ví dụ, tất cả các giao diện trong một mạng được gắn với các địa chỉ IP cùng chia sẻ một tiền tố định tuyến toàn cầu phổ biến. Kết quả là, các node trong sensornet có thể khai thác shared-context này để nén tiền tố phổ biến thường xuất hiện trong Header. Đối với các mạng sơ khai, tất cả các thông tin vào và ra của mạng sẽ thực hiện ít nhất một tiền tố phổ biến. Đối với truyền thông trong mạng, cả địa chỉ nguồn và đích sẽ mang theo tiền tố phổ biến.



Hình 3.1: Nén shared-context

Header lớp mạng truyền datagram trong cùng một mạng có mối tương quan cao, chẳng hạn như tiền tố định tuyến toàn cầu trong các địa chỉ IPv6 như thể hiện trong hình 3.1. Nén shared-context là flow độc lập và tận dụng các mối tương quan để nén các Header mà không yêu cầu trạng thái cho mỗi flow.

3.1.4 Nén kết hợp

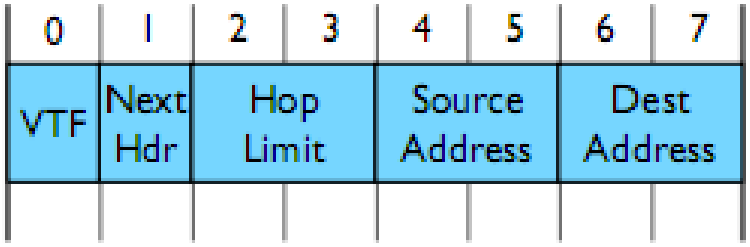
Nén Stateless và Shared-context hoạt động tốt tại lớp mạng khi các Header lớp mạng có điểm chung trên tất cả các flow thông tin trong mạng. Tuy nhiên, Header lớp giao vận có điểm chung trên một flow cụ thể nhiều hơn là trên các flow => hỗ trợ nén kết hợp giữa nén stateful cho Header lớp giao vận kết hợp với nén stateless và shared-context tại lớp mạng. Một ưu điểm của nén stateful tại lớp giao vận là bất kỳ trạng thái nén nào cũng chỉ duy trì tại các điểm kết thúc. Hơn nữa, lớp giao vận yêu cầu giao tiếp hai hướng, có thể dựa vào đó để thiết lập và duy trì trạng thái nén.

3.1.5 Nén Header IPv6

Mục này sẽ trình bày một chương trình nén Header LOWPAN HC, cho một mạng IPv6 trên sóng radio IEEE 802.15.4. LOWPAN HC xây dựng dựa trên RFC 4944 và nó hỗ trợ cả 2 loại giao tiếp toàn cầu và multicast, đồng thời nó cũng hỗ trợ giao tiếp liên kết cục bộ. LOWPAN HC sử dụng nén kết hợp, nhưng mở rộng để hỗ trợ cả 2 cơ chế stateless (không trạng thái) và stateful (trạng thái) tại lớp mạng và lớp giao vận.

Đối với IPv6, trường Version luôn luôn là 6 và trong LOWPAN HC thì trường này bị lược đi. LOWPAN HC giả định trường Traffic Class và Flow Label mang giá trị 0; đồng thời LOWPAN HC giả định tiền tố định tuyến toàn cầu cho Source Address và Destination Address kết hợp với tiền tố được giao cho sensornet này. Cuối cùng, LOWPAN HC hỗ trợ nén tùy ý trường Next Header, (như UDP hoặc Header mở rộng IPv6). Khi trường Next Header được nén, trường Next Header được lược đi và sử dụng mã hóa để nén.

Kết quả nén IPv6 sử dụng mã hóa được hiển thị trong hình 3.2



Hình 3.2: Nén Header Ipv6

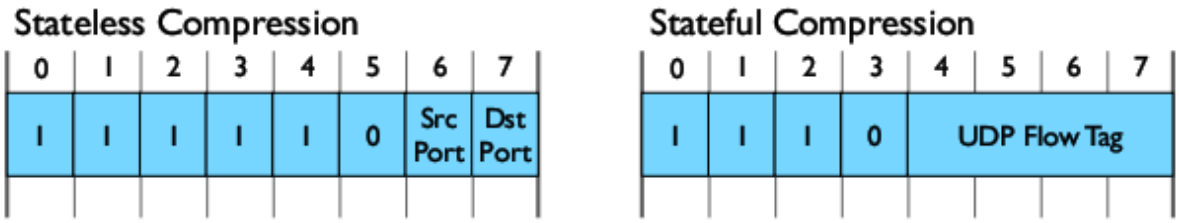
Nén IPv6 bằng phương pháp mã hóa sử dụng một byte duy nhất để nén các trường Version, Traffic Class, Flow Label, Next Header, Hop Limit, Source Address và Destination Address. Còn trường Payload Length được lược đi. Như vậy, một Header IPv6 dài 40 byte, nhưng có thể được nén xuống chỉ còn 1 byte duy nhất.

3.1.6 Nén Next Header

LOWPAN HC cho phép nén Next Header, trong khi RFC 4944 chỉ cho phép nén UDP, TCP, và ICMPv6. LOWPAN HC cho phép nén trường Next Header bằng cách tận dụng 1 bit trong mã hóa IPv6 để xác định Next Header được nén. Và những bit kế tiếp sẽ tạo ra định danh Next Header. Định danh này quy định cụ thể Next Header đang được nén và phương pháp nén của nó. Định danh cho phép LOWPAN HC tối ưu hóa số bit cần thiết để nén.

Nén Header rất phù hợp cho các ứng dụng sensornet. Cũng giống như lớp mạng, nén UDP có thể dùng cơ chế stateless hoặc stateful. Header UDP có 8 byte bao gồm các trường: Source Port, Destination Port, Length, và Checksum. Cả 2 cơ chế nén stateless và stateful luôn lược đi trường Length và được xác định từ Header

lớp thấp hơn. Tuy nhiên, Checksum luôn thực hiện nội tuyến, điều này rất cần thiết cho IPv6 và để chống lại lỗi giải nén của LOWPAN HC.



Hình 3.3:Nén Header UDP

Nén UDP theo cơ chế Stateless giả định một giá trị chung cho 8 bit đầu của Source Port hoặc Destination Port trong phạm vi tạm thời. Khi cả 2 cổng thực hiện trong phạm vi chung, LOWPAN HC sử dụng 3 byte để nén Header UDP.

Nén UDP theo cơ chế Stateful cho phép LOWPAN HC để nén Header UDP xuống 2 byte với bất kỳ cổng nào được sử dụng. Bởi vì cả Source Port hoặc Destination Port là các cổng tĩnh trong một dòng, LOWPAN HC nén cả hai 2 cổng thành 1 tag duy nhất. Các node ban đầu giao tiếp bằng cơ chế stateless, các node có thể thương lượng tag này bằng cách gửi tin nhắn ICMPv6. Khi giao tiếp với các thiết bị IP bên ngoài sensornet, LOWPAN HC dựa trên Router biên giới để nén theo cơ chế Stateful.

=> Tóm lại: Sử dụng mã hóa để nén Header Next phải có một định danh (xác định ở các bit đầu tiên). Cơ chế stateless và stateful đều dùng để nén cho Header UDP. Cơ chế Stateless nén các cổng vào tập hợp phạm vi cổng của một subnet. Cơ chế Stateful nén tất cả các cổng xuống một nhãn duy nhất. Cả hai phiên bản đều nén độ dài UDP, nhưng không nén UDP Checksum.

3.2 Bối cảnh

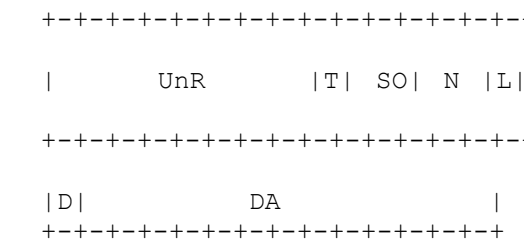
Giao thức IEEE 802.15.4 quy định kích thước một gói tin tối đa là 127 byte. Lớp Physical áp đặt overhead tối đa là 25 byte, còn lại 102 byte cho lớp kiểm soát truy cập phương tiện truyền thông (media). Bảo mật lớp link trong trường hợp tối đa là 21 byte, chỉ còn lại 81 byte. Hơn nữa, Header IPv6 là 40 byte, như vậy còn lại 41 byte cho các giao thức lớp trên, như UDP. Tiếp sau, sử dụng 8 byte trong Header, chỉ còn 33 byte cho dữ liệu ứng dụng. Tình hình này, rõ ràng cần nhấn

mạnh nhu cầu về nén Header và phân mảnh.

Việc sử dụng chuyên sâu sự phân mảnh và sự kết hợp sẽ dẫn đến lãng phí không cần thiết về năng lực tính toán và năng lượng. Vấn đề lớn phải đối mặt trong sự phân mảnh và nén Header bao gồm các vấn đề: xác định một cơ chế định tuyến các mảnh, tính phức tạp của việc xác định mất mát và phục hồi mảnh, và đảm bảo rằng mảnh bù đắp không bị ảnh hưởng bởi nén Header, bằng cách sử dụng tín hiệu Thừa nhận / không Thừa nhận (ACK/ no ACK) để giải quyết và điều này cũng đảm bảo độ tin cậy. Tuy nhiên, sẽ tốn nhiều pin do overhead của chuyển gói tin ACK/ no ACK.

Vì vậy, để tránh việc sử dụng sự phân mảnh và sự kết hợp, nén Header cần phải được xem xét để lược bỏ hoặc giảm thiểu một số tính năng nhất định của IPv6.

3.3 Nén header IPv6



Trong đó:

* UnR: UnReserved : 7 bit

Hiện tại, không sử dụng các bit này mà để sử dụng trong tương lai và có thể được chỉ định cho giá trị ngẫu nhiên nào đó.

* T: Traffic Class: 1 bit

T=0: Không ưu tiên

T=1: Độ ưu tiên cao

Các Header IPv6 ban đầu (chưa được nén) được thừa nhận bởi gateway chứa 8-bit Traffic Class và 20-bit flow label. Trong trường hợp này, 28-bit này được trừu tượng thành hai class: thời gian nhạy cảm và thời gian không nhạy cảm. Do đó, kỹ thuật nén Hedaer chỉ cần sử dụng 1 bit, có thể được thiết lập hoặc không thiết lập biểu thị thời gian nhạy cảm của gói tin.

* SO: Security Option: 2 bit

SO=00: Không bảo mật

SO=01: Chứng thực

SO=10: Mật mã

SO=11: Để dành

Trong hầu hết trường hợp, WSN không bảo mật dữ liệu nhạy cảm, nhưng SO lại thực hiện đầy đủ chính sách bảo mật bao gồm cả bảo mật dữ liệu nhạy cảm, chính điều này dẫn đến lãng phí không cần thiết trong tính toán và thất thoát năng lượng. Cơ bản, bảo mật có thể được cung cấp bởi các lớp thấp hơn. Tuy nhiên, trong trường hợp các biện pháp bảo mật bổ sung tại tầng IP được yêu cầu, sự cần thiết phải chứng thực hoặc mã hóa, giải mã, có thể được xác định nhờ Security Option.

* N: Next Header: 2 bit

N=00: Không có Header tiếp theo

N=01: Header UDP

N=10: Header Định tuyến

N=11: Sử dụng trong tương lai

Rất ít các tùy chọn Next Header được lấy ở dạng ban đầu của nó, thường nó bị thay đổi hoặc lược bỏ:

- Hop-by-Hop Header Options

Vấn đề với Hop-by-hop là nó phải được nhìn thấy, hiểu và thực thi bởi mỗi node, điều này gây ra sự lãng phí năng lượng không cần thiết. Các dữ liệu được thu thập và truyền tải trong phần lớn các ứng dụng thực tế của WSN, không yêu cầu bất kỳ xử lý đặc biệt nào tại các node trung gian, mà các node trung gian có thể lợi dụng sự cung cấp từ Header mở rộng Hop-by-hop. Vì vậy chúng ta không nên thực hiện các tùy chọn Hop-by-hop.

- Routing Header

Routing Header được thể hiện rõ ràng chỉ như là Loose Source Routing (Nguồn định tuyến không chính xác) được mô tả dưới đây:

Loose Source Routing dùng để xác minh một số node có thể truy cập từ một nguồn xác định. Trong nhiều trường hợp, tải trọng dữ liệu chỉ có địa chỉ; nội dung của gói tin là nhạy cảm, thì Loose Source Routing như là một biện pháp an ninh bổ sung, dữ liệu có thể có mặt đồng thời với địa chỉ. Điều này đảm bảo rằng gói tin đến đích thông qua một con đường an toàn. Với mục đích này, một số bit có thể được

dùng từ việc thiết lập các bit UnReserver để chỉ định số lượng địa chỉ hiện tại, một số byte từ tải trọng dữ liệu cũng có thể được đưa lên như một sự thay thế => KHÔNG NÊN làm điều này vì dữ liệu có thể bị phân mảnh.

- Authentication Header (Header xác thực)

Authentication Header được lược đi ở dạng Header ban đầu. ESP (Encapsulating Security Payload – Gói gọn bảo mật Tải trọng) bao gồm tất cả các chức năng mà sẽ được thực hiện bởi một Authentication Header. Trong trường hợp chỉ xác thực là cần thiết, nó được thiết lập trong bit SO được mô tả như ở trên.

- Encapsulating Security Payload Header (Đóng gói dữ liệu bảo mật)

Mã hóa và giải mã tiêu thụ tài nguyên nhiều trong khi WSN giới hạn nguồn điện và năng lực xử lý. Vì vậy, sử dụng Encapsulating Security Payload Header là không nên. Chỉ sử dụng nó trong trường hợp bảo mật cao.

- Destination Options Header (Header tùy chọn điểm nguồn)

Sử dụng Destination Options không được được giới thiệu vì nếu sử dụng Header mở rộng này sẽ dẫn đến sự mở rộng của kích thước gói tin vượt quá MTU.

- Fragment Header (Header phân mảnh)

Việc sử dụng Header này được lược bỏ hoàn toàn.

- No Next Header (Không có Header tiếp theo)

No Next Header được đặt là 00 trong Header nén và trong Header IPv6 ban đầu nó được ký hiệu là 59.

- Upper Layer Header (Header lớp trên)

Giá trị 01 để biểu thị Header lớp trên, có nghĩa là giao thức vận chuyển được sử dụng là UDP (ký hiệu là giá trị 17 trong Header IPv6 ban đầu) (mặc dù, TCP là đáng tin cậy, nhưng không được sử dụng như là một giao thức vận chuyển bắt tay), kết quả là trong việc gửi nhiều gói tin sẽ thất thoát nhiều năng lượng.

* L: Loose Source Routing: 1 bit

Nó được thiết lập để xác định gói tin được gửi bởi Header mở rộng Định tuyến.

Loose Source Routing dùng để xác minh một số node có thể truy cập từ một nguồn xác định. Trong nhiều trường hợp, tải trọng dữ liệu chỉ có địa chỉ; nội dung của gói tin là nhạy cảm, thì Loose Source Routing như là một biện pháp an ninh bổ sung, dữ liệu có thể có mặt đồng thời với địa chỉ. Điều này đảm bảo rằng gói tin đến đích thông qua một con đường an toàn. Với mục đích này, một số bit có thể được

dùng từ việc thiết lập các bit UnReserver để chỉ định số lượng địa chỉ hiện tại, một số byte từ tải trọng dữ liệu cũng có thể được đưa lên như một sự thay thế => KHÔNG NÊN làm điều này vì dữ liệu có thể bị phân mảnh.

* HL: Hop Limit: 8 bit

Hop Limit không được sửa đổi, vẫn có độ dài độ dài 8 bit. Vì vậy, có tối đa 255 Hop được thực hiện. Nếu con số này không đủ trong tương lai, các bit UnReserved có thể được sử dụng.

* SA: Source Address: 13 bit

- Địa chỉ được cấu hình như sau:

Truyền thông giữa thế giới bên ngoài và bên trong WSN: Xem xét một máy Ma bên ngoài mạng WSN, có nhu cầu giao tiếp với một node WSN là Wb, trong đó 1 <= Ma <= 255; 1 <= Mb <= 2 ^ 13. Ma gửi một yêu cầu tới Gateway để có được địa chỉ IPv6 của node Wb. Gateway sẽ gửi lại thông tin cho Ma.

Ma gửi một gói tin đến Wb với Destination Address đầy đủ là 128 bit. Gói tin này được ngăn chặn bởi Gateway - đây là con đường duy nhất để tiếp cận với WSN. Khi gói tin được thừa nhận bởi Gateway, Gateway dịch thông điệp trong một gói tin WSN, nghĩa là: Header được nén, Destination Address được thay thế bởi địa chỉ tương đương 13-bit và địa chỉ 128-bit của Ma được đăng ký trong bảng tra cứu của Gateway. Gateway giao một địa chỉ 13-bit mới cho Ma để nó đăng ký trong bảng tra cứu và địa chỉ này tương ứng với địa chỉ 128-bit của Ma. Địa chỉ 13-bit này được thiết lập tại trường Sourse Address. Địa chỉ này có tiền tố 11111 để chỉ ra rằng nó tương ứng với một máy bên ngoài. Thông điệp dịch sau đó được chuyển tiếp đến Wb.

Nếu sau đó Wb có nhu cầu giao tiếp với Ma, nó sẽ gửi một gói tin được dự định trước tới Ma. Gói tin này cũng được ngăn chặn bởi Gateway, Gateway dịch gói tin đó: Header được mở rộng, các Source Address được thay thế bằng một địa chỉ 128-bit (như thuật toán mô tả ở trên) và Destination Address vẫn được sử dụng bởi nhận được địa chỉ 128-bit tương ứng với địa chỉ 13-bit trong bảng tra cứu. Sau đó, gói tin được chuyển tiếp ra mạng bên ngoài. (Nén 128 bit địa chỉ thành 13 bit địa chỉ như phần V)

* D: Destination Address Type: 1 bit

D=0: Unicast

D=1: Multicast

Destination Address Type là một trường 1 bit. Nó xác định xem địa chỉ đích

là Anycast hay Multicast.

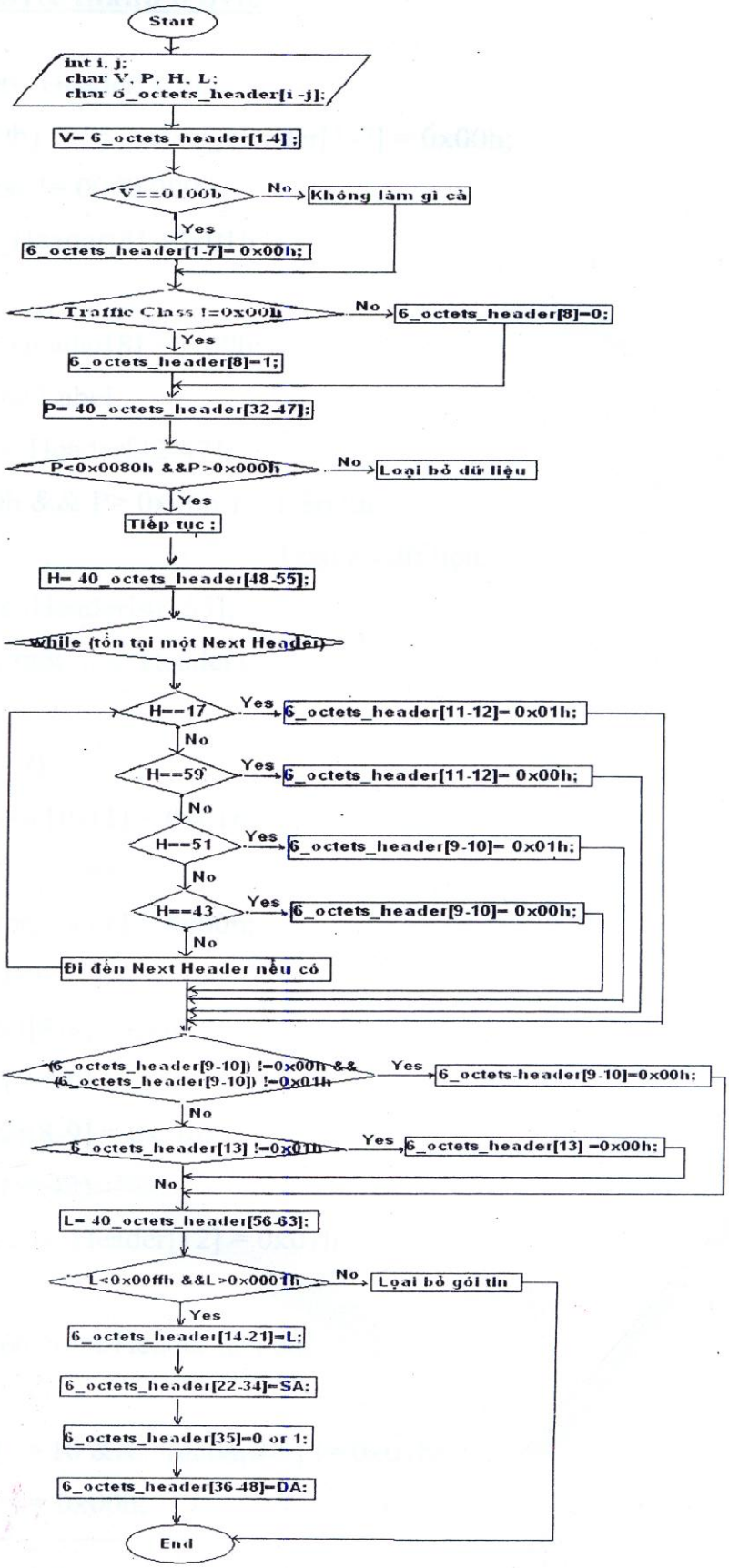
* DA: Destination Address: 13 bit

Địa chỉ được cấu hình như Source Address. Nén 128-bit địa chỉ thành 13 bit địa chỉ như đã trình bày trong phần Source Address.

3.4 Nén header và thuật toán mở rộng

Phần này sẽ trình bày làm thế nào để nén Header IPv6 có kích thước 40 byte thành định dạng 6 byte nén và làm thế nào để định dạng 6 byte nén thành Header 40 byte đầy đủ. Thuật toán sẽ lược bỏ một số trường, đó là giả định vẫn còn phổ biến cho truyền thông 6LoWPAN: Version là 6; Flow Label là 0; Payload Length có thể được suy ra từ các lớp thấp hơn từ Header IEEE 802.15.4; Hop Limit sẽ được đặt một giá trị tốt bởi node nguồn; 128 bit địa chỉ IPv6 được giảm xuống 13-bit địa chỉ. Mô hình đánh địa chỉ được giải quyết trong

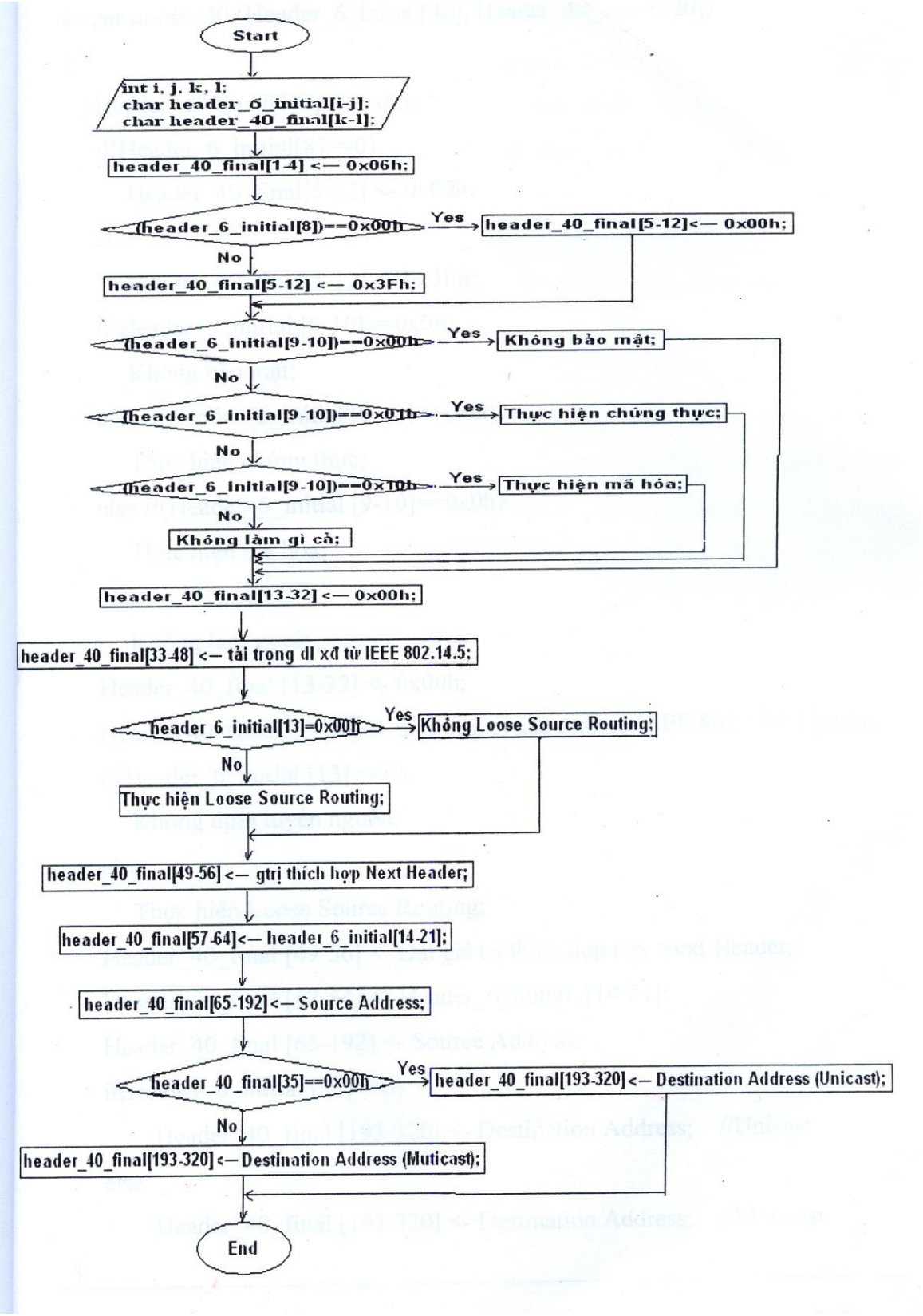
Sơ đồ nén 40 byte thành 6 byte


Start
int i, j;
char V, P, H, L;
char 6_octets_header[i-j];
V= 6_octets_header[1-4] ;
V==0100b
No
Không làm gì cả
Yes
6_octets_header[1-7]= 0x00h;
Traffic Class !=0x00h
No
6_octets_header[8]=0;
Yes
6_octets_header[8]=1;
P= 40_octets_header[32-47];
P<0x0080h &&P>0x000h
No
Loại bỏ dữ liệu
Yes
Tiếp tục :
H= 40_octets_header[48-55];
while (tồn tại một Next Header)
H==17
Yes
6_octets_header[11-12]= 0x01h;
No
H==59
Yes
6_octets_header[11-12]= 0x00h;
No
H==51
Yes
6_octets_header[9-10]= 0x01h;
No
H==43
Yes
6_octets_header[9-10]= 0x00h;
No
Đi đến Next Header nếu có
(6_octets_header[9-10]) !=0x00h &&
(6_octets_header[9-10]) !=0x01h
Yes
6_octets-header[9-10]=0x00h;
No
6_octets_header[13] !=0x01h
Yes
6_octets_header[13] =0x00h;
No
L= 40_octets_header[56-63];
L<0x00ffh &&L>0x0001h
No
Loại bỏ gói tin
Yes
6_octets_header[14-21]=L;
6_octets_header[22-34]=SA;
6_octets_header[35]=0 or 1;
6_octets_header[36-48]=DA;
End

Chương trình nén 40 byte thành 6 byte

```
{
V = 40_octets_Header[1-4];
if(V == 0100b)       6_octets_Header[1-7] = 0x00h;
if (traffic class != 0000 0000)
     6_octets_Header[8] =0x01h;
else
     6_octets_Header[8] =0x00h;
// Bỏ qua Flow Label
P = 40_octets_Header[32-47];
if(P< 0x0080h && P> 0x00h )    Tiếp tục;
else                                    Loại bỏ dữ liệu;
H = 40_octets_Header[48-55];
while (tồn tại một next Header)
{
       if(H == 17)
            6octet[10-11] = 0x01h;
       else if (H == 59)
            6octet[10-11] = 0x00h;
       else if (H== 51)
            6octet[8-9] = 0x0h;
       else if (H==50)
            6octet[8-9] = 0x10h;
       else if (H==43)
            6_octets_Header[12] = 0x01h;
       Else
            Đi đến Next Header nếu có;
}
if (6octet[8-9] != 10 &&  6octet[8-9] != 0x01h)
      6octet[8-9] = 0x00h;
if (6octet[12] != 0x01h)
      6octet[12] = 0;
L = 40_octets_Header[56-63];
if( L < 0x00ffh && L > 0x0001h)
     6_octets_Header[13-20] = L;
Else     Loại bỏ gói tin;
6_octets_Header[21-32] = SA ;
6_octets_Header[33] = 0 or 1;
6_octet_Header[34-46] = DA;
 }
```

Sơ đồ giải nén 6 byte thành 40 byte



```
Giải nén 6 byte thành 40 byte
Expansion6to40 (Header_6_initial[48], Header_40_final[320])
{
    Header_40_final[1-4] <- 0x6h;
    if(Header_6_initial[8]==0)
        Header_40_final[5-12] <- 0x00h;
    else
        Header_40_final[5-12] <- 0x3Fh;
    if Header_6_initial [9-10]==0x0h)
        Không bảo mật;
    else if(Header_6_initial [9-10]==0x0h)
        Thực hiện chứng thực;
    else if(Header_6_initial [9-10]==0x0h)
        Thực hiện mã hóa;
    else
        Không làm gì cả;
    Header_40_final [13-32] <- 0x00h;
    Header_40_final [33-48] <- tải trọng dl xác định từ IEEE 802.15.4
Header;
    if(Header_6_initial [13] ==0)
        Không định tuyến nguồn;
    else
        Thực hiện Loose Source Routing;
    Header_40_final [49-56] <- Đặt giá trị thích hợp của Next Header;
    Header_40_final [57-64] <- Header_6_initial  [14-21];
    Header_40_final [65-192] <- Source Address;
    if(Header_6_initial [35]==0)
          Header_40_final [193-320] <- Destination Address;    //Unicast
    else
          Header_40_final [193-320] <- Destination Address;    //Muticast
}
```

CHƯƠNG 4: ĐỊNH TUYẾN IPV6 CHO WSN

Trong chương này trình bầy các thành phần của IPv6 thực hiện trên lớp mạng, cơ sở thiết kế giao thức định tuyến cho sensornet thường bị hạn chế bởi tài nguyên của node mạng, được tập trung tại các bộ định tuyến, giao thức định tuyến đặt trên node và chi phí toàn mạng . Nhìn chung, lượng thông tin thực tế bị giảm tiếp vì vấn đề an ninh. Các router an ninh định tuyến thông tin phụ thuộc quảng bá và môi trường xung quanh để tạo ra liên kết, phát hiện vòng lặp và tuyến tối ưu, và cung cấp thông tin mặc định cho bộ định tuyến

4.1 Đồ thị kết nối

Mạng có khả năng chuyển tới đích,nó phải được cấu hình để duy trì hệ thống và đảm bảo liên kết bền vững (ví dụ như khoảng cách, độ trễ, sử dụng, hoặc kết hợp một số). Có phương pháp cấu hình định tuyến tĩnh cấu hình bằng mục bảng,nhưng không phù hợp với mạng có quy mô lớn đặc biệt là cấu trúc liên kết động. Thực tế hiện nay các mạng sử dụng giao thức định tuyến động phát hiện cấu trúc liên kết mạng và truyền thông tin định tuyến trong một nỗ lực để hình thành đường dẫn phù hợp và hiệu quả cho điểm khác nhau.

Các giao thức định tuyến động cho mạng ad-hoc gặp khó khăn vì đồ thị liên kết không đúng quy định. Các mạng có dây truyền thống có liên kết tương đối bền vững topolo-Gies với liên kết được lên hoặc xuống, cung cấp tỉ lệ thành công là rất cao (ví dụ như cao hơn 99,9%) tuy nhiên trong các mạng không dây liên kết đến các nút lân cận được xác định bằng yếu tố môi trường và thường có một loạt các tỷ lệ thấp hơn và bị rớt theo thời gian. Ngay cả các liên kết có tỷ lệ mất tương đối cao thường cung cấp một số liên kết hạn chế, và các giao thức định tuyến phải xem xét hoặc không sử dụng các liên kết này.

Hơn nữa, do thời gian thay đổi lượng liên kết vật lí cũng thay đổi và yếu tố điện từ, các giao thức định tuyến liên tục phải đánh giá các liên kết, xem xét tác động của chúng trong tổng thể và chi phí đường, thích ứng nếu cần thiết.

Nguồn tài nguyên hạn chế của mạng làm cho bài toán định tuyến gặp nhiều khó kkhăn hơn. hạn chế bộ nhớ tác động đến nút mạng có thể duy trì trạng thái về tập các nút hơn là các nút trong mạng đôi khi ít hơn láng riềng mà nó bao phủ. Thông luợng hạn chế và năng lượng hạn chế của các nút thuờng có thể giao tiếp với

các láng riềng, những hạn chế làm giới hạn khả năng phát hiện và khả năng tính toán của các nút lân cận. chúng cũng giới hạn khối luọng thông tin định tuyến của giao thức định thuyến mà có thể giao tiếp và duy trì đừơng liên kết một cách rõ ràng.

Nguồn tài nguyên giới hạn ảnh hửơng của các nút phải thực hiện định tuyến với một phần thông tin trong khung IP. Điều này có nghĩa các nút thuờng có thông tin của trạm kế tiếp của một tập các giới hạn đích và tuyến ngầm định cho tất cả các nút khác.

Những yêu cầu cơ bản của Ip không nhất thiết phải có thông tin vị trí thuờng thì chúng đươc tối ưu. Khung Ip được phân bố trên mạng cản nhận và dữ liệu. Chính giao thức ngầm định với router biên. mỗi nút cung cấp router biên cho các tuyến ngầm định cho phép router biên duy trì cây liên thông với nút chủ hoặc nút chủ tới từng nút. Khi dùng cây liên thông thì các router biên đẩy gói tin bao gồm cả router định tuyến.

Bài toán định tuyến tập trung tại sác router biên giao thức định tuyến cũng phải đáp ứng yêu cầu về hạn chế tài nguyên. Các nút duy trì trạng thái cấu hình của một tuyến đơn gọi là tuyến ngầm định. Trong khi nhu cầu xử lí bài toán ở định tuyến biên là tuyến tính với số nút và số router thuờng hạn chế hơn thông thuờng. Khi truyền vuợt khung trong nút mạng thuờng rất hữu hạn. Các yêu cầu truyền có liên quan đến phát quảng bá từ các router và phải truyền đơn từ các nút tới các router. Số luợng các sóng vừa truyền là trạng thái thấp và mở rộng mật độ mạng cũng khá tốt. Việc truyền vuợt khung trong tực tế được giảm nhiều vì dữ liệu được bảo mật tồn tại trên đường truyền. Trạng thái định truyến an ninh trên router thường phát quảng bá và tối ưu luồng dữ liệu để tạo ra đường link ước lượng cho phép lặp và xác định đường truyền tối ưu con hoặc cung cấp thông tin đường truyền tới các nút biên.

Với yêu cầu tài nguyên hạn chế giao thức định tuyến cung cấp đươờng truyền tối ưu khi trao đổi thông qua 1 router biên, mẫu dữ liệu được truyền lớp ứng dụng của mạng cảm nhận. Việc căt bỏ thao tác vì thông tin hạn chế thì phải hi sinh tối ưu tuyến đường trong trường hợp tổng quát. một nút mà Ip truyền đi bằng 0 về tối ưu thì mạng phải cung cấp một cách tương đối. Tuy nhiên việc đẩy các gói tin sẽ được thảo luận khi cần thiết.

4.2 Nền tảng

Giao thức định tuyến đáp ứng việc phát hiện các đường đi tới đích mong muốn. Phương pháp truyền thống router cung cấp thông tin đường truyền và chuyển tiếp nó tới bảng chuyển tiếp, nhưng đối với router hiện nay nó chỉ cung cấp thông tin của đường truyền trong gói dữ liệu. Ví dụ router gồm một danh sách các nút mà truyền tới đích để phát hiện 1 tuyến. Các giao thức định tuyến động phải sử dụng các danh sách trên và thiết lập đường liên kết và thuộc tính cần thiết của đường liên kết tới láng riềng. Các nút được lan rộng tới toàn bộ hình trạng mạng do đó các nút có thể chọn các đường trong khi tối ưu một số phép đo. Giao thức định tuyến động hoạt động trên miền phân bố cung cấp các tinh chất mở rộng tốt hơn nhưng nó cũng gây khó khăn cho việc duy tì độ bền của định tuyến qua các mạng và ra quyết định định tuyến 1 cách rõ ràng.

` Giao thức định tuyến chia làm 2 lớp: khoảng cách vector và trạng thái liên kết. Khoảng cách vector thực hiện bài toán người bán hàng. Mỗi kết nối nút của bảng định tuyến cho phép láng riềng tính toán giá của định tuyến thông qua nút quảng cáo tới đích. Các nút này lựa chọn các láng riềng với giá cực tiểu. Bài toán người bán hàng là một hình thức đơn giản nhưng có thể kéo dài thời gian và trạng thái định tuyến, có thể gây cho việc lặp truyền và vấn đề khởi tạo điểm. Cơ chế đơn giản này được phát triển để phát hiện những tuyến bất ổn giữa 2 nút. Cơ chế phức tạp hơn phát triển để đảm bảo duy trì trạng thái định tuyến nhưng độ tin cây định tuyến không theo trật tự.

Trạng thái liên kết của giao thức đựoc phát triển để giải quyết bài toán về phủ thời gian đựoc hiểu là giao thức vector khoảng cách. Các trạng thái kiên kết có các nut tạo thành bản đồ về toàn bộ mạng độ trong suốt về tuyến đường đi ngắn nhất. Mỗi nút phát hiện đường liên kết tới nút láng riềng và tràn thông tin tới các nút khác vì vậy chúng có thể tạo thành topo. Các giải thuậtvề thông tin liên kết thường được sử dụng phổ biến ở mạng có dây vì độ liên kết là chặt chẽ và không có vấn đề về đếm lặp, chỉ bị mất trạng thái khi thông tin phát thông qua mạng. cắt bỏ một số thuộc tính có ý nghĩa là về trạng thái và yêu cầu truyền mà nó có thể mở rộng đường liên kết trong mạng đối với đường truyền mạnh với bộ nhớ và băng thông lớn thì điều này là có ý nghĩa.

Cả 2 giao thức định tuyên vector và định tuyến trạng thái đều được đề xuất cho mạng Manet không giống việc thiết kế giao diện cho mạng có dây. Giao thức

manet được thiết kế cụ thể cho việc phát quảng bá một cách đặc biệt cho mạng không dây và mạng với khả năng di động cao. Kết quả là các giao thức manet đặt trên các thông tin định tuyến làm tràn và các tuyến đã được phát hiện. Sử dụng số tuần tự thì đảm bảo sự tràn kết thúc. Các giao thức vector định tuyến dựa trên số tuần tự của các trạng thái lặp dựa trên trên những liên kết ngược trong đó các tuyến đường được tính toán đẻ cung cấp các đường dẫn cho việc phát hiện các giao thức manet. Dựa trên phép tràn để phân bố thông tin topo phân tán tới tất cả các nút tương tự như trong mạng dây.

Tuy nhiên các giao thức manet thì giảm các trạng thái và yêu cầu truyền bằng lựa chọ động với lớp con của nút để hoạt động như một nút chuyển tiếp, Những nút chuyển tiếp này duy trì thông tin topo và thông điệp chuyển tiếp có khả năng cung cấp mật độ mạng tốt hơn. Các giao thức manet đều không phù hợp cho nhu cầu của mạng cảm nhận. Giao thức manet tối ưu chuyển tiếp đường đi ngắn nhất giữa các nút và không mang tính chất truyền được các nút di động.

Những giả thiết khiến các giao thức manet đều dựa trên phép tràn để phát hiện và duy trì các tuyến để đạt đường đi ngắn nhất. Khi kích thước tăng thì giao thức manet không khả thi với mạng cảm nhận. Thay vào đó mạng cảm nhận phải có cấu trúc và khả năng mở rộng tính chất này có ý nghĩa giảm đi những yêu cầu về tài nguyên cho giao thức định tuyến động. Giao thức định tuyến động cho mạng cảm nhận thường tập trung vào việc tối ưu trạng thái định tuyến, giao thức định tuyến lựa chọn để đạt đươc những yêu cầu về trạng thái chỉ có thể tối ưu chuyển tiếp truyền tới đích đơn. Việc tối ưu này cho phép các giao thức định tuyến đánh giá tập con của các liên kết khi cơ hội lớn nhất, cung cấp một tuyến đường tới đích. Các giao thức định tuyến phân cấp thường duy trì trạng thái về láng riềng bằng việc định tuyến theo topo hình cây.

Phương pháp tiếp cận phân cấp trong các nút IP sử dụng biến độ dài cố định để hỗ trợ tổ chức mạng phân cấp. Tuy nhiên việc dựa trên phát đơn phân cấp có thể dẫn tới căng thẳng của tuyến ở trạnh thái tồi khi mở rộng bán kính của mạng. Các giao thức định tuyến dựa trên nút điều phối cố gắng tối ưu các tuyến giữa của các cặo nút với nhau. Giao thức định tuyến đồ thị dựa trên thông tin về vị trí vì vậy các nút phải duy trì trạng thái thông tin láng riềng. Các giao thức định tuyến điều phối ảo sinh các điều phối dựa trên liên kết nhưng yêu cầu tài nguyên hơn cho việc xây dựng cấu trúc. Thách thức của điều phối là chúng được giấu tên nút cho topo định tuyến. Việc này cực khó điều khiển trong việc thay đổi nút di động. Việc tối ưu hoá

chất lượng đường truyền, giá đường truyền là một phần quan trọng trọng mạng cảm nhận.

Một số giao thức đơn giản dựa trên các phép ở tầng vật lý như trong chỉ số của tín hiệu RSSI hoặc giá trị phối hợp chip. Phương pháp đo liên kết ở tầng vật lí được thực hiện vì chúng tính toán thông qua các khung radio nhận được nhưng nó có thể có nhiều tỉ lệ lỗi bit đôi lớn. Các giao thức khác tinh toán lỗi gói tin trực tiếp và duy trì trạng thái trao đổi thất bại. Mỗi phương pháp đều dựa trên thông điệp quảng bá với số thứ tự cho phép nút láng riềng tính toán tỉ lệ lỗi gói tin trong hướng đơn gần đấy thì người ta ước lượng đường liên kết sử dụng tấng xác nhận và liên kết dữ liệu để tính toán tỉ lệ lỗi gói tin.

Tỉ lệ lỗi gói tin nghĩa là cung cấp dữ liệu liên quan nhất nhưng yêu cầu nhiều thời gian năng lượng để tính toán trạng thái khi bộ ước lượng phép đo trực tiếp lớp vật lí, kết quả là đo tỉ lệ lỗi. hạn chế tài nguyên ở mạng cảm nhận tác động tới các giao thức định tuyến như hạn chế bộ nhớ, khả năng định tuyến,thực hiện một phần chức năng. Trong đó một phần trạng thái định tuyến vào các router có thể tối ưu tới một số các đích và chấp nhận các tuyến đường giữa tập các nút. Trong khi các giao thức định tuyến tìm kiếm và duy trì cấu trúc toàn cục một cách nhanh chóng hơn là việc cố gắng duy trì trạng thái định tuyến qua các nút trong mạng. Các nút nên tối ưu các quyết định và giải quyết những bất ổn khi nó xuất hiện. Tóm lại việc lựa chọn bỏ những điều cần thiết trong quá trình phân tán để phù hợp với tài nguyên hạn chế là cần thiết

4.3 Tuyến đường mặc định

Trong phần này, chúng tôi mô tả làm thế nào để các giao thức định tuyến lựa chọn và duy trì các tuyến đường mặc định. Các cấu hình giao thức định tuyến và duy trì các tuyến đường mặc định đối với thiết bị định tuyến biên giới, sử dụng quảng cáo ICMPv6 để khám phá bộ định tuyến lân cận và truyền đạt thông tin định tuyến. Các bộ định tuyến duy trì một bảng định tuyến để quản lý tuyến đường mặc định và sắp xếp chúng dựa trên chi phí tuyến đường và ước lượng liên kết tin cậy.

Bộ định tuyến thường lựa chọn các mục trên để sử dụng như là tuyến đường mặc định, nhưng có thể chọn một mục khác để hỗ trợ tái định tuyến hoặc tìm kiếm các tuyến đường tốt hơn. Trong khi các tuyến đường có thể được lựa chọn dựa trên các số liệu khác,phát hiện trạng thái bằng cách sử dụng bộ đếm hot. Bộ đếm hop

cung cấp một chỉ số ổn định hơn giảm thiểu sự phụ thuộc vào đường liên kết cá nhân. Bởi khi vận chuyển lượng dữ liệu môi trường xung quanh, router đòi hỏi chi phí truyền thông ít và không yêu cầu kiểm soát bất cứ thông điệp nào. Trạng thái yêu cầu không đổi.

4.4 Khám phá tuyến đường tiềm năng

Router sử dụng thông điệp thông báo sự hiện diện của bộ định tuyến và cho phép các nút phát hiện bộ định tuyến lân cận. IPv6 sử dụng các giao thức định tuyến truyền thống để định tuyến dữ liệu, bộ định tuyến thông tin hiện vẫn đang sử dụng giao thức này. Các thông tin có yêu cầu phát hiện láng riềng và các giao thức định tuyến, cả hai cần phải tìm ra các nút lân cận và truyền thông tin qua nhiều bước nhảy. Truyền tải theo giai đoạn cách sử dụng thuật toán gián tiếp. Bộ định tuyến cho phép thiết lập lại khoảng thời gian truyền dẫn.

Để nhanh chóng phát hiện ra các nút, các bộ định tuyến có thể truyền tải thông điệp ICMPv6 để tìm hiểu yêu cầu từ các nút lân cận. Các bộ định tuyến có thể tìm các nút khi một biến cố xảy ra bên ngoài và tham gia vào mạng khi số lượng các mục trong bảng định tuyến thấp hơn một số ngưỡng.

Các giao thức định tuyến của mang bất kỳ là các giao thức định tuyến để quảng cáo. Các giao thức định tuyến bao gồm số hop với các bộ định tuyến biên giới gần nhất và đường dẫn số liệu để lựa chọn tuyến đường. Các bộ đếm được sử dụng để phát hiện sự mâu thuẫn và làm cho cơ chế để phát hiện sự mâu thuẫn độc lập với con đường truyền số liệu.

Trong chương này, chúng ta tìm hiểu một con đường đơn giản: số lượng dự kiến sẽ được truyền đi (ETX) để đến bộ định tuyến biên giới. Các số liệu ETX là hữu ích vì nó nắm bắt được những liên kết dọc theo đường hướng tới các điểm đến cũng như số lượng hop. Trong giao thức truyền thống quan tâm chủ yếu về tính liên kết, nút nguồn (ví dụ như bộ nhớ và năng lượng) có thể khác nhau trong sensornets và giao thức định tuyến cần tận dụng nguồn lực bổ sung bất cứ khi nào có thể. Hỗ trợ cho cấu trúc liên kết với nhiều số liệu khác nhau bằng cách thêm nhiều tùy chọn trong bộ định tuyến quảng cáo.

Bộ định tuyến không giới hạn cấu hình các tuyến đường mặc định và có thể bổ sung thông tin cho tuyến đường đến điểm khác.Tập trung phát triển một đường cơ sở để giải quyết những cơ chế phức tạp hơn.

4.5 Quản lý bảng định tuyến

Các bộ định tuyến lưu trữ trạng thái về các tuyến đường tiềm năng mà nó phát hiện ra trong bảng định tuyến. Trong số các tuyến đường tiềm năng chọn một một tuyến đường mặc định trong bảng chuyển tiếp. Sự khác biệt giữa định tuyến và các bảng là đặc biệt quan trọng trong các mạng không dây - các bộ định tuyến phải dành thời gian để đánh giá một liên kết và so sánh nó với khả năng khác trước khi sử dụng nó để định tuyến gói tin. Khi thêm tuyến đường tiềm năng vào bảng định tuyến nó sẽ liên kết với láng riềng trong bảng. Như vậy các lớp liên kết sẽ duy trì chất lượng liên kết để kkét nối, đó là điều cần thiết để đưa ra chi phí khi lựa chọn tuyến đường đường mặc định.

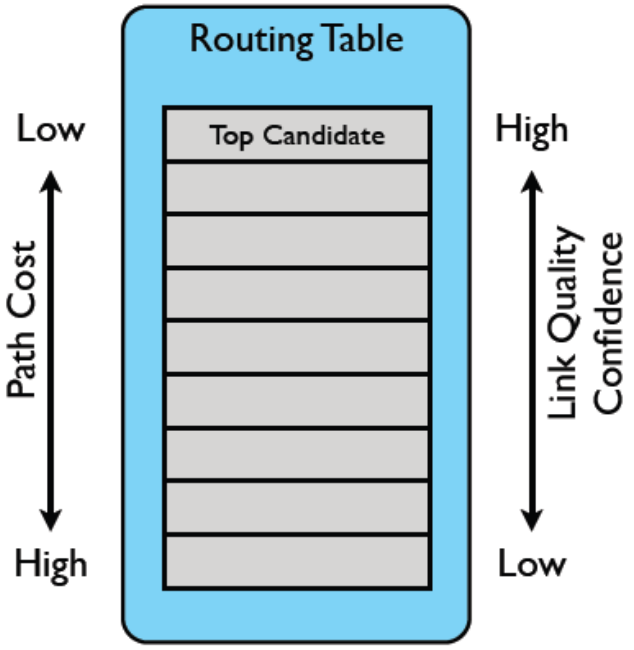
Đối với những người hàng xóm mới được phát hiện, liên kết chỉ cung cấp ít thông tin liên kết: một mẫu duy nhất của RSSI và tương quan chip cho các quảng cáo nhận được. Cả hai đều có phương sai cao và không phải là chỉ số thực sự của gói tin lỗi.

Với mỗi lần truyền trên một liên kết, các lớp liên kết có thể tính toán lượng liên kết mới chính xác cao hơn. Bộ định tuyến đưa ra liên kết chính xác hơn, định tuyến chấp nhận liên kết mới trong trường hợp tìm được một định tuyến chi phí thấp hơn. Giới hạn bộ nhớ có nghĩa là các bộ định tuyến có thể ra khỏi mục bảng và tạo ra định tuyến liên kết mất nhiều thời gian và năng lượng.

Quản lý bảng định tuyến bao gồm ba hoạt động cơ bản: (i) chèn vào bảng định tuyến, xúc tiến trong bảng định tuyến, và loại bỏ từ bảng định tuyến. Mục mới luôn được đưa vào cuối danh sách và chỉ khi các thông tin lớp vật lý (RSSI và tương quan chip) ở trên một ngưỡng mà sẽ có khả năng cung cấp một liên kết chấp nhận được. Ngưỡng này có thể được thích nghi dựa trên thông tin thu thập được về môi trường. Nếu bảng định tuyến đầy, các bộ định tuyến lựa chọn có hay không trục xuất mục cuối.

Hình 4.1: Quản lý bảng định tuyến. Trong khi các bộ định tuyến nên thích ghi với lượng liên kết, định tuyếnr cũng nên được chấp nhận liên kết mới có thể cung cấp một con đường chi phí thấp hơn. Các bảng định tuyến bằng cách tin tưởng vào lượng liên kết và chi phí đường dẫn quảng cáo. Các router chỉ chèn các mục ở dưới cùng của danh sách và các tuyến đường liên kết tốt với chất lượng cao sẽ đưa lên

danh sách. Bảng định tuyến phục vụ như một bộ lọc để chấp nhận các tuyến đường mới



Hình 4.1: Quản lý bảng định tuyến

- Chi phí quảng cáo cho các tuyến đường mới là ít hơn đáng kể so với chi phí quảng cáo của con đường mục cuối.

- Chi phí con đường quảng cáo cho các tuyến đường mới, nhập dưới là tương tự và liên kết mới tốt hơn đáng so với mục cuối.

Các mục trong bảng định tuyến bằng cách di chuyển chúng lên một vị trí trong danh sách, nhưng chỉ khi mục đã có tỷ lệ liên kết thành công và đường dẫn với chi phí thấp hơn. Lưu ý rằng chi phí đường dẫn kết hợp các chi phí quảng cáo liên kết thành số liệu duy nhất. Phương pháp thống kê kết hợp độ lệch chuẩn để tính toán khoảng tin cậy cũng có thể được sử dụng với chi phí cao hơn các yêu cầu tính toán. Router đánh giá việc thúc đẩy một mục mỗi lần xảy ra một cố gắng truyền tải trên liên kết, khiến cho lớp liên kết để cập nhật các liên kết thành công tỷ lệ ước tính. Định tuyến được thực hiện nếu:

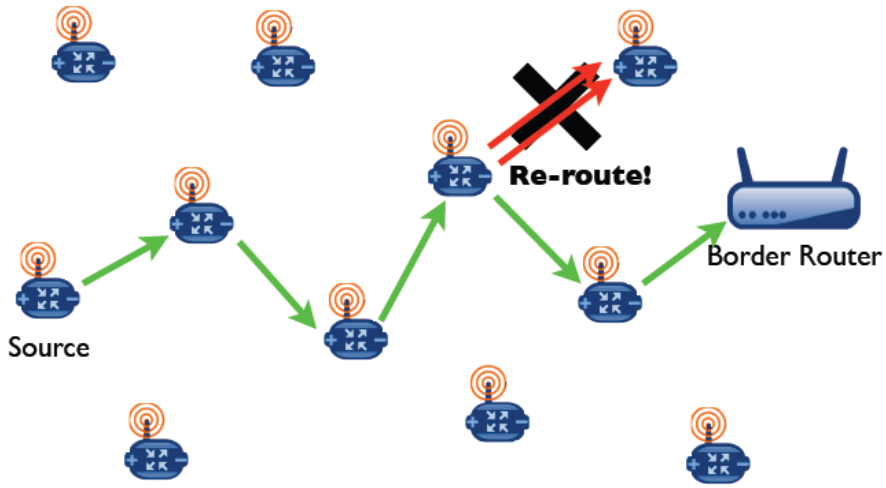
-Có một con đường chi phí thấp hơn và thành công trong liên kết hơn so với mục ở trên.

- Có một con đường tương tự như chi phí hơn so với mục trên tỷ lệ thành công trên một ngưỡng chấp nhận được.

4.6 Lựa chọn tuyến Mặc định

Router thường chọn mục đầu tại bảng định tuyến để sử dụng như là tuyến đường mặc định trong bảng chuyển tiếp. Đôi khi các bộ định tuyến có thể chọn các mục khác vì hai lý do: (i) để hỗ trợ tái định tuyến khi truyền tải liên tiếp và (ii) để thăm dò các ứng cử viên khác, tăng tỷ lệ thành công liên kết.

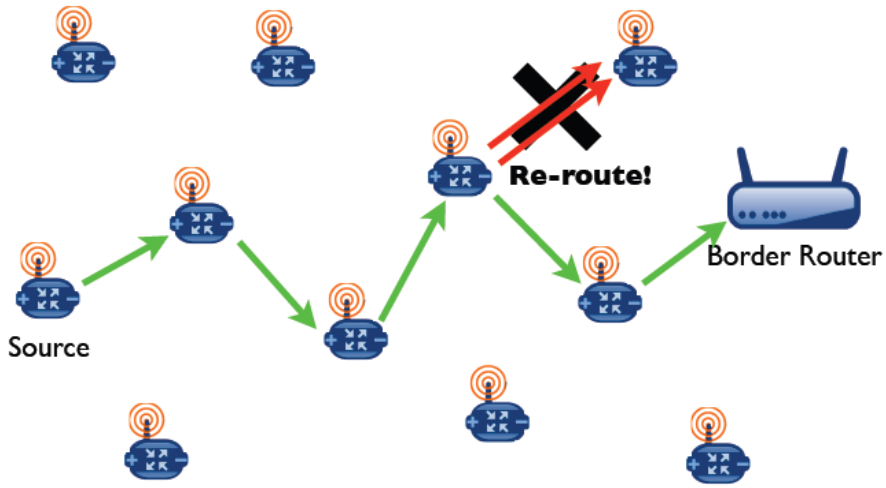
Các bộ định tuyến phát hiện sự cố lặp đi lặp lại bằng cách theo dõi tỷ lệ thành công liên kết của các tuyến đường mà nó đã cấu hình. Nếu tỷ lệ thành công đi xuống sau vài lần liên tiếp, router sẽ chuyển hướng bằng cách chọn mục thay thế trong bảng định tuyến để phục vụ như các tuyến đường mặc định, như trong hình 4.2.



Cơ chế tái định tuyến thể hiện một ví dụ về nơi mà các bộ định tuyến được phép đưa ra quyết định trước khi quyết định tối ưu toàn bộ. Vòng lặp định tuyến sẽ không xảy ra khi lựa chọn mục với hop nhỏ hơn hoặc bằng với mục đầu. Định tuyến các vòng có thể xảy ra khi thông tin định tuyến không phù hợp. Lựa chọn các mục trong khi tái định tuyến sẽ giúp giảm thiểu sự xuất hiện của các vòng lặp định tuyến.

Các tìm kiếm các tuyến đường chi phí thấp hơn và giữ liên kết up-to-date cho các mục trong bảng định tuyến. Rõ ràng việc gửi một tin nhắn và nhận được thừa nhận tỷ lệ thành công liên kết. Thăm dò sẽ cung cấp thêm thông tin về liên kết, nhưng cũng tốn kém hơn. Tỷ lệ liên kết thành công cũng phụ thuộc thời gian và nếu liên kết không được sử dụng trong tương lai.

Hình 4.2: Tái định tuyến. Nếu router phát hiện sự cố trên các tuyến đường mặc định hiện tại, router bắt đầu chọn mục khác trong nỗ lực để tiếp nhận chuyển tiếp các gói tin.

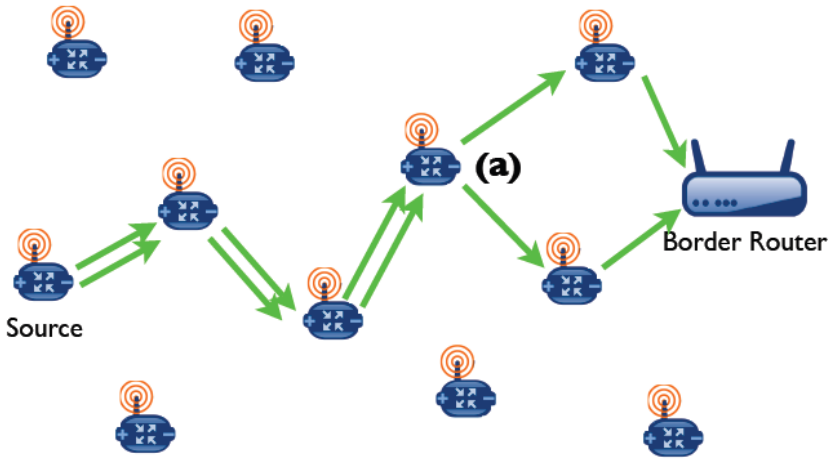


Hình 4.2: Tái định tuyến

Thay vì dựa vào thông điệp điều khiển rõ ràng, các bộ định tuyến cũng tạo ra lượng ước tính liên kết động thay đổi tuyến đường mặc định trong bảng chuyển tiếp. Cấu hình các tuyến đường mặc định với các mục khác để tiếp tục tìm kiếm các tuyến với chi phí tương tự hoặc thấp hơn, ngay cả khi các ứng cử viên hàng đầu là thực hiện tốt. Nếu ứng viên nhiều lần tồn tại, các bộ định tuyến xoay chuyển giữa

chúng. Tuy nhiên, router vẫn tiếp tục sử dụng cho đến khi truyền thất bại đến nút đó, cho phép một con đường với chi phí thấp hơn được quảng cáo để nhanh chóng lên danh sách nếu liên kết là tốt. Chỉ có mục thử nghiệm với số hop bằng hoặc thấp hơn thì các vòng lặp định tuyến không xảy ra.

Hình 4.3: Cập nhật lượng liên kết. Nếu một hoặc nhiều mục định tuyến có số hop nhỏ hơn hoặc bằng với mục hàng đầu, bộ định tuyến sẽ lựa chọn những các tuyến đường mặc định để chuyển tiếp các gói tin. Bằng cách đó, các bộ định tuyến có thể cập nhật tính liên kết và liên tục tìm kiếm các tuyến đường tốt hơn mà không cần thông báo thăm dò rõ ràng.



Hình 4.3: Cập nhật lượng liên kết

Các bộ định tuyến không tạo ra bất kỳ thông báo thêm để duy trì lượng liên kết và tìm kiếm các tuyến đường chi phí thấp hơn. Có thể cho các bộ định tuyến ngừng việc đánh giá các liên kết khi có lưu lượng truy cập bằng không, nhưng hy vọng rằng ứng dụng sensornet sẽ tạo ra một số lưu lượng truy cập cơ bản tối thiểu cho các mục đích quản lý. Giao thức kiểm soát khác cũng yêu cầu lưu lượng truy cập định kỳ để duy trì trạng thái mềm.

4.7 Duy trì ổn định tuyến

Thông tin định tuyến có thể trở nên không phù hợp khi thay đổi chưa các nút khác trong mạng. định tuyến thông tin không phù hợp có thể phải sử dụng các tuyến đường chi phí cao hơn. Trong trường hợp xấu nhất, định tuyến thông tin không phù hợp dẫn đến các vòng lặp. Một số giao thức định tuyến hiện có một cách tiếp cận

tích cực chủ động trong giao tiếp là thay đổi thông tin định tuyến, nhưng như vậy thì liên quan đến tốc độ dữ liệu thấp và hạn chế của sensornets

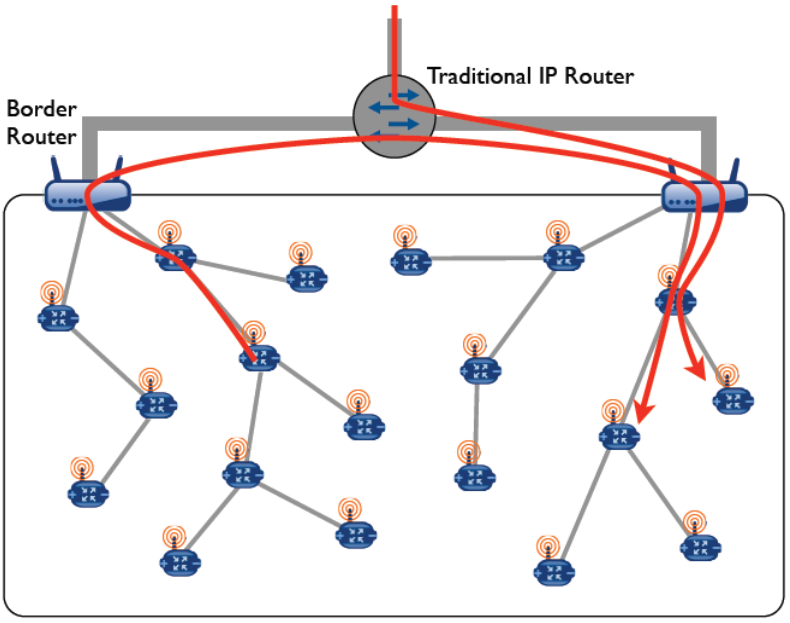
.

Thay vào đó, giao thức định tuyến có một cách tiếp cận thụ động, nơi các nút giao tiếp cập nhật thông tin định tuyến phát hiện khi không thống nhất. Nguyên tắc thiết kế sau này cho phép các nút quyết định khả quan sát tại địa phương và giải quyết mâu thuẫn khi chúng xảy ra

Các bộ định tuyến phát hiện đường có thể không hiệu quả và chọn tuyến đường bằng cách quan sát sự khác biệt đáng kể trong chi phí đường đi. Các đường đi có thể làm tăng chi phí liên kết trên các tuyến đường bị mất tỷ lệ so với trước đây. Tương tự như vậy, chi phí đường đi có thể giảm nếu tìm tuyến đường dọc theo con đường (ví dụ, bằng cách loại bỏ các chướng ngại vật). Tiếp nhận tin nhắn với một chi phí khác nhau cho thấy rằng việc lựa chọn tuyến đường mặc định có thể được tối ưu, kể từ khi người gửi sử dụng thông tin định tuyến cũ, như trong hình.

Sử dụng thông tin tuyến đường mặc định được cung cấp bởi mỗi nút sensornet, thiết bị định tuyến biên giới có thể tạo ra một cây bao trùm của toàn bộ mạng và sử dụng nó để tạo ra các tuyến đường chủ quay trở lại mỗi nút. Khi một bộ định tuyến biên nhận được một gói tin đi đến một nút trong sensornet, nó thực hiện một tra cứu trong cây bao trùm để xác định một tuyến đường đến đích. Nếu đích đến là bộ định tuyến biên giới trong phạm vi vô tuyến, các bộ định tuyến biên giới chuyển tiếp gói tin như bình thường bằng cách thiết lập địa chỉ đích của các tiêu đề liên kết đến đích. Nếu điểm đến được nhiều bước nhảy xa, biên định tuyến giới chèn có chứa một danh sách địa chỉ gói tin để đạt đến đích cuối cùng. Các nút chuyển tiếp gói tin bằng cách xử lý tiêu đề định tuyến để xác định điểm đến tiếp theo cho các gói tin

Hình 4.4: Bộ định tuyến tuyến biên giới . Nhiều thiết bị định tuyến biên giới có thể hỗ trợ một mạng lưới các tuyến đường bằng cách chia sẻ máy chủ IP giữa chúng. Bởi vì các nút sensornet chọn tuyến đường đến các bộ định tuyến biên giới gần nhất, chuyển datagrams đến các bộ định tuyến biên giới gần nhất đích, dựa mạng lưới có khả năng kết nối nhiều thiết bị định tuyến biên giới



Hình 4.4: Bộ định tuyến tuyến biên giới

Danh sách địa chỉ bao gồm một trong những tiêu đề IPv6 khi giao nhận tại tầng mạng hoặc trong 6LoWPAN khi giao nhận tại các lớp liên kết. Trong cả hai trường hợp, mỗi mục địa chỉ tương đương với 16-bit địa chỉ liên kết lớp ngắn. Các kỹ thuật sử dụng để nén tiêu đề IPv6 có thể được sử dụng trong tiêu đề định tuyến. Trong khi sử dụng địa chỉ ngắn làm cho danh sách địa chỉ nhỏ gọn hơn, nó yêu cầu các nút sensornet gán địa chỉ ngắn với giao diện không dây. Các tiền tố định tuyến toàn cầu được giả định là giống nhau cho tất cả các địa chỉ trong danh sách. Các tiêu đề định tuyến đã bị loại bỏ vì lý do an ninh và thừa nhận những quan ngại an ninh bằng cách tạo ra một loại định tuyến mới và chỉ cho phép sử dụng các tiêu đề định tuyến trong sensornet .Thiết bị định tuyến biên giới không nên chuyển bất kỳ định tuyến datagrams nào.

Hỗ trợ định tuyến IP giữa các bộ định tuyến biên giới dùng nhiều tiêu chuẩn IP-based . Thiết bị định tuyến biên giới đơn giản chỉ cần trao đổi các tuyến đường giữa các máy chủ. Các bộ định tuyến biên giới có thể kết nối trực tiếp trên một liên kết có khả năng cao (ví dụ Ethernet), trong trường hợp chúng chỉ đơn giản là quảng cáo trên các tuyến đường chủ. Phát hiện láng riềng dựa trên cơ chế Proxy cũng có thể được sử dụng có hiệu quả các tuyến đường giữa các hình trên thiết bị định tuyến biên giới đáp ứng với các truy vấn,router sẽ chuyển tiếp gói tin đến router biên giới thích hợp. Khi bộ định tuyến biên giới không kết nối với các liên kết đó, hoặc là mạng lưới vận chuyển để cấu hình các tuyến đường chủ cho sensornet hoặc bộ định

tuyến biên giới phải được kết nối trực tiếp dùng các đường hầm để hình thành một mạng lưới che phủ mà giả lập một liên kết IP duy nhất. Tất cả các cấu hình cho phép mạng xung quanh để chuyển tiếp các gói tin đến router biên giới thích hợp trước khi đưa nó vào sensornet này.

4.8 Tuyến đường chủ

Các tuyến đường mặc định cung cấp khả năng đến các nút sensornet để các bộ định tuyến biên giới và các thiết bị IP khác có kết nối với các mạng IP khác. Giao thức định tuyến hình thành các tuyến đường chủ cho mỗi nút sensornet cá nhân. Để có hiệu quả và duy trì các tuyến đường chủ, giao thức định tuyến tập trung tại các bộ định tuyến biên giới. Liên kết ngược là có thể bởi vì các tuyến đường mặc định chỉ được lựa chọn dựa trên kết nối hai chiều.Các bộ định tuyến biên giới chuyển tiếp một datagram trong nút sensornet bằng cách chèn một tiêu đề có chứa các tuyến đường. Sử dụng nguồn dựa trên định tuyến tại các bộ định tuyến biên giới, các nút sensornet không cần phải duy trì bất kỳ trạng thái cho các tuyến đường chủ.
Sự kết hợp của các tuyến đường mặc định và các tuyến đường lưu trữ tại các bộ định tuyến biên giới cho phép lớp mạng kết hợp một nút sensornet và thiết bị IP bất kỳ, bao gồm cả các nút sensornet trong cùng một sensornet, sensornet trong sensornets khác, và thiết bị IP bất kỳ khác có kết nốivới các mạng IP khác.Lưu ý rằng các tuyến đường đến và đi từ các thiết bị IP bên ngoài là tối ưu, như tuyến đường mặc định lựa chọn số liệu để giảm thiểu chi phí chuyển tiếp các gói tin. Giao tiếp với các thiết bị bên ngoài là điển hình cho nhiều ứng dụng sensornet.Ứng dụng thu thập dữ liệu thường chuyển tiếp dữ liệu đến một máy chủ trung tâm.Ứng dụng điều khiển thường được hướng dẫn kiểm soát từ một máy chủ trung tâm. Trong các phần sau, chúng tôi mô tả cấu hình giao thức định tuyến của chúng tôi như thế nào và duy trì các tuyến đường chủ.

4.8.1 Nghiên cứu tuyến đường chủ

Sensornet cung cấp thông tin của các tuyến đường mặc định bằng cách định thời gian gửi tin nhắn đến tuyến đường của bộ định tuyến biên giới bằng cách sử dụng các tuyến đường mặc định. Các bộ định tuyến cập nhật lượng liên kết và tinh chỉnh các quyết định định tuyến cho các tuyến đường mặc định.

Lựa chọn IPv6 khi chuyển tiếp tại tầng mạng hoặc một tiêu đề 6LoWPAN để chuyển tiếp.Khi có lưu lượng truy cập dữ liệu môi trường xung quanh, giao nhận piggybacks gửi một tin nhắn để tuyến đường trong datagrams đáp ứng thời gian đăng ký quảng cáo.Nếu tỷ lệ hiện tại thấp hơn so với thời gian đăng ký quảng cáo, các nút phải tạo ra datagrams riêng của mình đơn giản chỉ để giao tiếp thông tin tuyến đường.

4.8.2 Định tuyến biên giới

Tuyến đường mặc định sử dụng thông tin được cung cấp bởi mỗi nút sensornet, thiết bị định tuyến biên giới có thể tạo ra một cây bao trùm toàn bộ mạng và sử dụng nó để tạo ra các tuyến đường chủ. Khi một bộ định tuyến biên giới nhận được một gói tin đến một nút trong sensornet, nó thực hiện một tra cứu trong một cây bao trùm để xác định một tuyến đường đích.Nếu không có tuyến đường hợp lệ có sẵn cho nút đó, các bộ định tuyến biên giới tạo ra một lỗi ICMP Host Unreachable.Các bộ định tuyến biên giới chuyển tiếp các gói tin như bình thường bằng cách thiết lập các tiêu đề liên kết của địa chỉ đích. Nếu điểm đến là nhiều bước nhảy, các bộ định tuyến biên giới chèn một tiêu đề định tuyến có chứa một danh sách các địa chỉ trong gói tin để đạt đến đích cuối cùng. Các nút chuyển tiếp các gói tin bằng cách xử lý định tuyến tiêu đề để xác định điểm đến tiếp theo cho gói tin

Hình 4.4: Nhiều thiết bị định tuyến biên giới có thể hỗ trợ mạng lưới bằng cách chia sẻ các tuyến đường Host IP giữa chúng.Bởi vì sensornet chọn các tuyến đường đến các bộ định tuyến biên giới bộ gần nhất, lợi dụng mạng có khả năng kết nối các bộ định tuyến biên giới

Danh sách địa chỉ bao gồm tiêu đề định tuyến IPv6 khi chuyển tiếp tại tầng mạng hoặc trong một tiêu đề 6LoWPAN khi chuyển tiếp tại các lớp liên kết.Trong cả hai trường hợp, mỗi mục địa chỉ tương đương 16-bit địa chỉ lớp liên kết ngắn.Các kỹ thuật được sử dụng để nén các tiêu đề IPv6 có thể được sử dụng trong tiêu đề định tuyến. Trong khi sử dụng địa chỉ ngắn làm cho danh sách địa chỉ nhỏ gọn hơn, nó đòi hỏi các nút gán các địa chỉ ngắn với giao diện không dây. Tiền tố định tuyến toàn cầu được giả định là giống nhau cho tất cả các địa chỉ trong danh sách.Ttiêu đề định tuyến đã bị phản đối vì lý do an ninh và tạo ra một loại định tuyến mới chỉ cho phép sử dụng tiêu đề định tuyến trong sensornet. Các bộ định

tuyến biên giới không nên chuyển tiếp bất kỳ datagrams đã bao gồm một tiêu đề định tuyến.

Trong nhiều trường hợp một sensornet sử dụng nhiều thiết bị định tuyến biên giới, như thể hiện trong hình 4.4.Bằng cách thêm vào các bộ định tuyến biên giới, quản trị mạng có thể tăng hiệu quả năng lượng, giảm sử dụng kênh, và giảm độ trễ thông tin liên lạc bằng cách sử dụng các bộ định tuyến biên giới để giảm số lượng bước nhảy giữa các nút sensornet và các bộ định tuyến biên giới gần nhất. Nếu một bộ định tuyến biên giới bằng không, các nút định tuyến thông bộ định tuyến biên giới sẽ cấu hình lại các tuyến đường mặc định của họ và đăng ký chính nó vào một bộ định tuyến biên giới khác.

IP trivially hỗ trợ định tuyến giữa các bộ định tuyến biên giới nhiều bằng cách sử dụng cơ chế dựa trên tiêu chuẩn IP. Thiết bị định tuyến biên giới phải trao đổi các tuyến chủ với nhau. Các bộ định tuyến biên giới có thể được kết nối trực tiếp trên một liên kết (ví dụ Ethernet), trong trường hợp cần phải quảng cáo trên các tuyến đường chủ liên kết.Phát hiện láng riềng theo cơ chế Proxy cũng có thể được sử dụng có hiệu quả để hình thành các tuyến đường giữa các bộ định tuyến biên giới. Thiết bị định tuyến biên giới sử dụng Proxy để đáp ứng với các truy vấn cho rằng tất cả các nút sensornet được liên kết.Kết quả là, router sẽ chuyển tiếp các gói tin để thích hợp với các bộ định tuyến biên giới. Khi bộ định tuyến biên giới không kết nối với liên kết đó, hoặc là mạng quá cảnh cần phải cấu hình các tuyến đường chủ cho các nút sensornet hoặc các thiết bị định tuyến biên giới phải được kết nối trực tiếp bằng cách sử dụng các đường hầm để hình thành một mạng lưới che phủ mà giả lập một liên kết IP duy nhất. Tất cả các cấu hình cho phép mạng xung quanh chuyển tiếp các gói tin để các bộ định tuyến biên giới thích hợp trước khi đưa nó vào sensornet

4.9 Kết luận

Trong chương này trình bày một cơ sở giao thức định tuyến được thiết kế cho sensornet điển hình. Sơ sở giao thức định tuyến tập trung định tuyến trạng thái tại các bộ định tuyến biên giới để giảm thiểu các yêu cầu tài nguyên giữa các nút sensornet. Chỉ duy trì trạng thái cho một tập cố định của các tuyến đường mặc định tiềm năng cho các bộ định tuyến biên giới gần nhất, cơ sở giao thức định tuyến không bao giờ khởi sự tràn, đòi hỏi trạng thái nhỏ và liên tục, và hỗ trợ phục hồi địa

phương.Giao thức chỉ đòi hỏi mỗi trạng thái nút định tuyến và chi phí truyền thông mạng.

Sự phát triển một lớp mạng IPv6 cho sensornets bao gồm cấu hình và quản lý, giao nhận, và định tuyến.Sử dụng kiến trúc và cơ chế thực hiện nó, lớp mạng có thể cung cấp khả năng tạo lập với datagram tốt nhất giữa một nút sensornet và thiết bị IP bất kỳ khác (ví dụ, các nút trong sensornet và các thiết bị truyền thống IP bên ngoài).

Các tài liệu tham khảo

[1] Wireless Sensoe Network design and implement

[2] The IPv6 architecture for WSN

[3] http://www.wsn.com

[4] Networking Wireless Sensors, Bhaskar Krishnamachari, Cambridge University Press 2005

[5] Wireless communications,Andrea Goldsmith, 2005.