MỤC LỤC

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, đặc biệt trong thời gian làm đồ án 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!

MỞ ĐẦU

Trong nhiều thập kỷ qua, đã hình thành một cơ sở hạ tầng thông tin liên lạc ở khắp nơi - Internet. Sự thành công to lớn của cơ chế *end-to-end* và nguyên tắc thiết kế *kiến trúc IP* đã giúp cho Internet có được vị trí như ngày nay. Cơ chế *end-to-end* đơn giản, đồng thời khả năng nhân rộng tốt. Còn lớp *kiến trúc IP* sử dụng phân tầng với khả năng cung cấp bởi lớp dưới. Ưu điểm của kiến trúc mạng phân tầng: quản lý đơn giản, thúc đẩy sự đổi mới và tiến hóa nhanh chóng. Với sự phát triển mạnh mẽ của nhiều công nghệ mới, dần dần kiến trúc này đã có quy mô rộng khắp => minh chứng cho sự thành công của kiến trúc.

Và mới đây, mạng cảm nhận không dây (sensornet) nổi lên như một làn sóng nghiên cứu mạnh mẽ trong sự phát triển của thế giới vật lý và kỹ thuật số. Nhưng đặc điểm của nó rất khác với các thiết bị IP truyền thống, đã đẩy vấn đề kết nối mạng đến một nấc thang mới. Khi gắn sensornet vào không gian vật lý thì nó mang nhiều thách thức: bộ nhớ, khả năng tính toán và giao tiếp, nguồn năng lượng hạn chế.

Nhiều nghiên cứu trong lĩnh vực này lập luận rằng: "nhiều bài học kinh nghiệm từ Internet và thiết kế mạng di động sẽ được áp dụng cho các thiết kế ứng dụng sensornet... mạng lưới cảm nhận có đủ những thủ tục để xem xét lại cơ cấu tổng thể của các ứng dụng và dịch vụ". Kiến trúc Internet được tránh vì nhiều lý do như sau:

- Nguồn lực khó khăn làm ảnh hưởng đến việc cho ra kiến trúc nhiều lớp.
- Một số lượng lớn các thiết bị, đồng thời chúng không cần giám sát trong việc triển khai, sẽ ngăn cản sự phụ thuộc vào giao tiếp quảng bá hoặc cấu hình hiện thời cần thiết để triển khai và vận hành các thiết bị mạng.
- Thuật toán định vị và xử lý bên trong mạng yêu cầu phải linh hoạt và có tính mở rộng.
- Không giống như các mạng truyền thống, một node cảm biến có thể không cần một danh tính (ví dụ, một địa chỉ).
- Mạng lưới truyền thống được thiết kế để chứa một loạt các ứng dụng. Trong khi, sensornet sẽ được đặc dụng với nhiệm vụ cảm biến.

Hiện nay đã có những tiến bộ đáng kể trong nhiều lĩnh vực, bao gồm: giao thức liên kết với năng lượng thấp dựa trên lắng nghe hoặc truyền thông với thời gian đồng bộ, các giao thức mạng cung cấp truyền thông n-1, 1-n và n-n; kiểm soát tắc nghẽn Hop-by-Hop và kiểm soát dòng; giao thức vận chuyển liên quan đến chuyển giao đáng tin cậy cho cả dữ liệu nhỏ và lớn.

Trong đồ án này, sẽ triển khai IPv6 dựa trên kiến trúc mạng sensornet. Căn cứ vào những phân tích trong đồ án này, em tin rằng một kiến trúc truyền thông cho sensornet nên giữ "eo hẹp" tại lớp mạng. IPv6 cung cấp một kiến trúc: phân lớp, đánh địa chỉ, định dạng Header, cấu hình, quản lý, chuyển tiếp, và định tuyến cung cấp các cấu trúc cần thiết cho việc thiết kế và thực hiện ở tất cả các layer dạng ngăn xếp. Trong đồ án này, em sẽ cho thấy làm thế nào để triển khai IPv6 với kiến trúc mạng sensornet và sử dụng hiệu quả trong hiệu suất, năng lượng, và độ tin cậy cao với kiến trúc này.

Đố án bao gồm các chương sau:

+ Chương I: Cho ta cái nhìn tổng quan về sensornet, cũng như những ưu, nhược điểm của nó. Đồng thời, giới thiệu các mô hình OSI, TCP/IP; và khung giao thức IPv4, IPv6. Từ đó cho ta biết lý do tại sao nên triển khai IPv6 dựa trên kiến trúc sensornet.

+ Chương II: Mô tả các thành phần vật lý của mạng, đó là các thiết bị biên và định tuyến, cũng như thiết bị định tuyến biên giới trong kết nối IP. Đồng thời, cũng trình bày tổng quan về IPv6 dựa trên kiến trúc sensornet, mà vẫn duy trì giao thức lớp và phân tách chức năng của kiến trúc Internet, nêu rõ lý do tại sao cạnh tranh LAN kém phù hợp với các khó khăn và thách thức của sensornet. Chương này, cũng mô tả đánh địa chỉ IPv6 và cấu trúc tiền tố, tận dụng không gian lớn của địa chỉ IPv6 để giảm lưu lượng thông tin và yêu cầu bộ nhớ trong việc gán địa chỉ.

+ Chương III: Phát triển lớp mạng IPv6 hoàn chỉnh cho sensornet bao gồm cấu hình và quản lý, chuyển tiếp và định tuyến. Sử dụng kiến trúc này và các cơ chế thực hiện, lớp mạng có thể cung cấp cách tiếp cận phân phát datagram với "nỗ lực cao nhất" giữa một node sensornet và bất kỳ thiết bị IP khác.

CHƯƠNG I: MẠNG CẢM NHẬN KHÔNG DÂY VÀ CÁC KHUNG GIAO THỨC

I. TỔNG QUAN VỀ MẠNG CẢM NHẬN KHÔNG DÂY (WSN)

1. Định nghĩa

WSN có thể hiểu đơn giản là mạng liên kết các node với nhau bằng sóng radio, trong đó các node mạng thường là các thiết bị đơn giản, nhỏ gọn, giá thành thấp... và có số lượng lớn, được phân bố một cách không có hệ thống trên một diện tích rộng (phạm vi hoạt động rộng), sử dụng nguồn năng lượng hạn chế và có thể hoạt động trong môi trường khắc nghiệt (chất độc, ô nhiễm, nhiệt độ cao...).

2. Cấu trúc của WSN

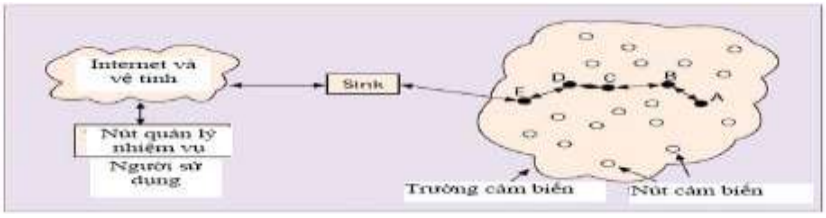
2.1. Node cảm biến: được cấu tạo bởi 3 thành phần: **vi điều khiển, sensor, bộ phát radio**. Ngoài ra, còn có các cổng kết nối với máy tính.

a. Vi điều khiển: bao gồm: CPU; bộ nhớ ROM, RAM; bộ phận chuyển đổi tín hiệu tương tự thành tín hiệu số và ngược lại.

b. Sensor: để cảm nhận thế giới bên ngoài, sau đó chuyển dữ liệu qua bộ phận chuyển đổi để xử lý.

c. Bộ phát radio: bởi vì node cảm biến là thành phần quan trọng nhất trong WSN, do vậy việc thiết kế các node cảm biến sao cho có thể tiết kiệm được tối đa nguồn năng lượng là vấn đề quan trọng hàng đầu.

2.2. Sensornet



Hình 1.1.1. Phân bố node cảm biến trong trường cảm biến

Như hình 1.1.1, sensornet bao gồm rất nhiều các node cảm biến được phân bố trong một trường cảm biến. Các node này có khả năng thu thập dữ liệu thực tế, sau đó chọn đường (thường là theo phương pháp đa bước nhảy) để chuyển

những dữ liệu thu thập này về *node gốc*. Node gốc liên lạc với *node quản lý nhiệm vụ* thông qua Internet hoặc vệ tinh. Việc thiết kế sensornet như Hình 1.1.1 phụ thuộc vào nhiều yếu tố như:

Khả năng chịu lỗi	**Môi trường hoạt động**
Khả năng mở rộng	**Các phương tiện truyền dẫn**
Giá thành sản xuất	**Cấu hình sensornet**
Tích hợp phần cứng	**Sự tiêu thụ năng lượng**

3. 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
- Sự thích ứng 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,…

4. Ứng dụng WSN

- Trong lĩnh vực an ninh
- Trong lĩnh vực môi trường
- Trong lĩnh vực gia đình
- Trong lĩnh vực y tế

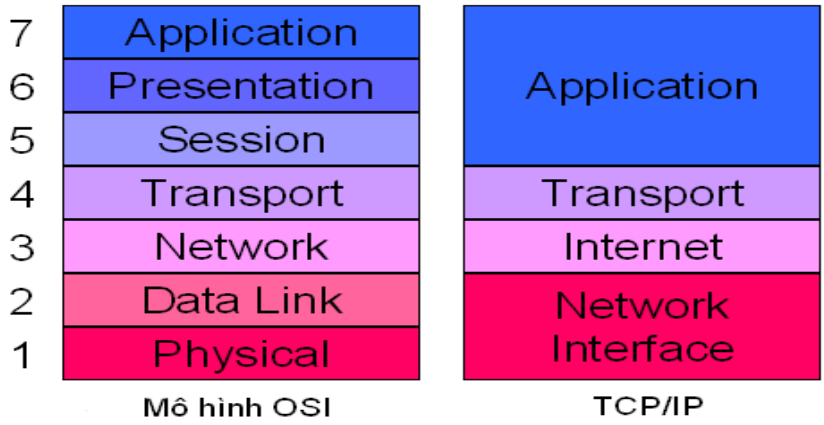
II. MÔ HÌNH OSI

Mô hình OSI gồm có 7 lớp: **Application, Presentation, Session, Transport, Network, Data Link và Physical**.

Hình 1.2.1. Mô hình OSI

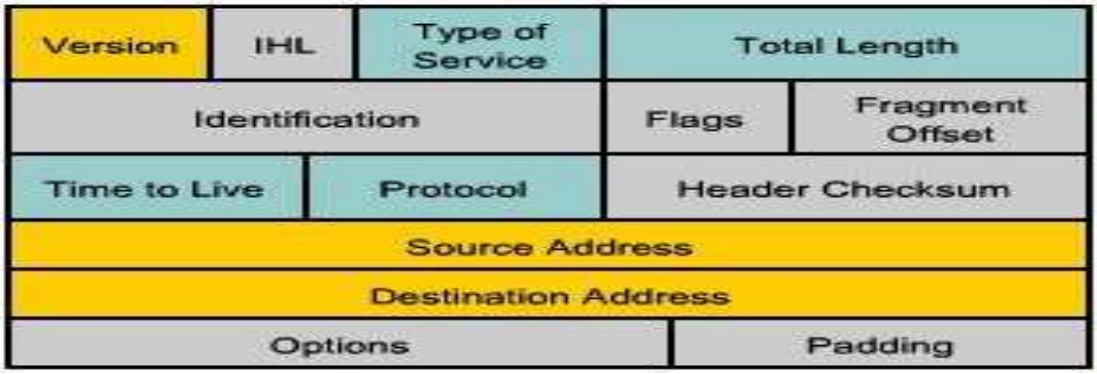
III. MÔ HÌNH TCP/IP

TCP/IP được xem là giản lược của mô hình OSI với bốn lớp sau: **Application**,**Transport, Internet**, **Network Interface.** Mô hình OSI là một mô hình trên lý thuyết, trong khi đó TCP/IP xem như là một mô hình biến thể của OSI và phù hợp với thực tế hơn.



Hình 1.3.1. Mối quan hệ giữa mô hình OSI và tiêu chuẩn TCP/IP

IV. KHUNG GIAO THỨC IPv4



Hình 1.4.1. Header của IPv4

V. KHUNG GIAO THỨC IPv6

Hình 1.5.1. 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.

+ **Flow Label (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 và lưu trữ kết quả trong một bộ nhớ cache.

+ **Payload Length (16 bit)**: trường này thay thế trường *Total Length* của Header IPv4. Nó chỉ chứa số byte tải trọng của gói dữ liệu.

+ **Next Header (8 bit):** chỉ rõ Header theo sau Ipv6 Header và nằm ở vị trí đầu của trường Data. 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, nó tương tự trường *TTL* (*Time To Live*) của Ipv4.

+ **Source Address (128 bit**): chứa địa chỉ IP của thiết bị khởi tạo datagram.

+ **Destination Address (128 bit):** chứa địa chỉ đích của node nhận gói tin IPv6.

VI. TẠI SAO PHẢI KẾT HỢP SENSORNET VÀ IPv6

+ Sensornet đã có những thay đổi đáng kể trong thập kỷ qua.

+ Sự ra đời của IEEE 802.15.4 thiết kế đặc biệt cho mạng năng lượng thấp.

+ IPv6 cũng có nhiều chức năng hỗ trợ mạng năng lượng thấp.

Do những tiến bộ đáng kể trong ba lĩnh vực, đây chính là thời điểm để áp dụng IPv6 dựa trên kiến trúc sensornet.

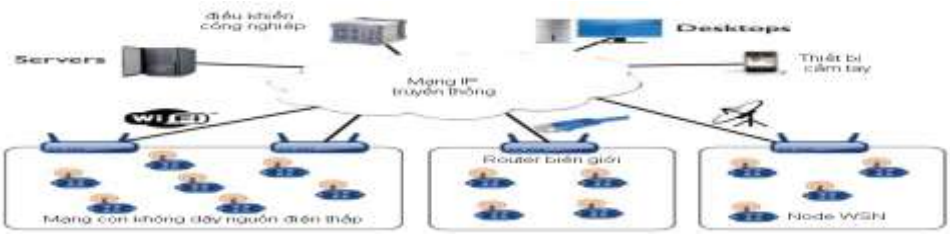
Có thể nói rằng việc triển khai IPv6 trong sensornet hiệu quả hơn khi so sánh với IPv4

Mặc dù, IPv6 những nhiều chức năng bổ sung nhưng vẫn còn nhiều vấn đề quan trọng vẫn cần được hỗ trợ IPv6 trong sensornet.

CHƯƠNG II: IPv6 TRÊN KIẾN TRÚC WSN

I. KIẾN TRÚC INTERNET MỞ RỘNG

Trong hình 2.1.1, mạng Internet mở rộng kết nối với Sensornet giống như bất kỳ một mạng IP nào khác, bằng cách sử dụng Router.



Hình 2.1.1. Kiến trúc Internet mở rộng

1. Các thành phần mạng

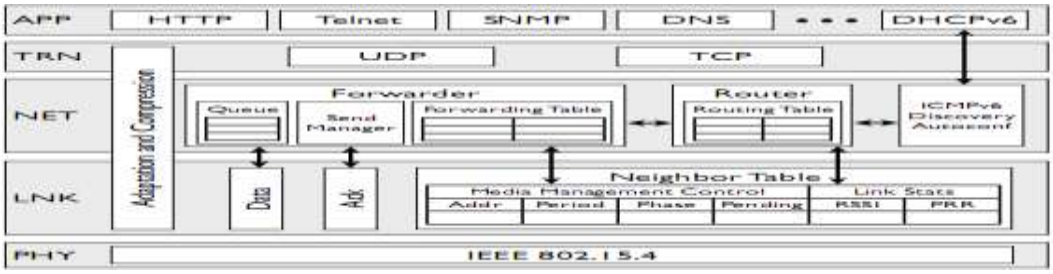
Một mạng IEEE 802.15.4 (thường được gọi là một PAN - Personal Area Network), bao gồm: *các giao diện* giống như một PAN ID; sau đó sử dụng các *cơ chế truy cập môi trường* như CSMA; tiếp đến, là *duy trì cơ chế liên kết một cách linh hoạt* ở lớp liên kết.

Một subnet IEEE 802.15.4 gồm *các thiết bị cuối, các thiết bị chuyển tiếp* (có thể có hoặc không).

Giao tiếp với các thiết bị IP bên ngoài sensornet thông qua một hoặc nhiều Router biên giới.

2. Kiến trúc nhiều lớp

Mô hình giao thức lớp IP có nghĩa là giao tiếp ngang nhau trong cơ chế được cung cấp bởi các lớp dưới. Hướng đi "hẹp" của kiến trúc này là lớp mạng IPv6. Lớp mạng gồm có ba thành phần: (i) Cấu hình và phát hiện, (ii) Chuyển tiếp, và (iii) Định tuyến.



Hình 2.1.2: Kiến trúc phần mềm IPv6 cho Sensornet.

Các kiến trúc cho sensornet bảo tồn giao thức lớp và cấu trúc phân lớp của kiến trúc IPv6 truyền thống. Lớp mạng đại diện cho các "eo hẹp" của kiến trúc này.

3. Sự kết hợp liên mạng

Để đáp ứng các hạn chế và thách thức của sensornet, các thành phần trong kiến trúc phải làm việc cùng nhau, sử dụng các cơ chế được cung cấp bởi các thành phần khác.

4. Triển khai IPv6 trong Sensornet

Đây là sự nỗ lực đầu tiên trong việc áp dụng IPv6 trong kiến trúc mạng sensornet. IPv6 cung cấp nhiều cơ chế cho sensornet nguồn điện thấp: sử dụng phản hồi Hop-by-Hop để tăng độ tin cậy và cơ chế nén với mục tiêu làm giảm đáng kể Header overhead và bộ nhớ cho việc chuyển tiếp và định tuyến…

II. TRÁNH LIÊN KẾT CẠNH TRANH

1. Các giả định truyền thống

IP đã thành công trong điều chỉnh một số công nghệ như kiến trúc mạng, IP và giao thức, các liên kết IP thường giả định rằng lớp liên kết cung cấp 3 đặc tính cơ bản sau: + Luôn luôn thức

+ Nỗ lực đáng tin cậy nhất

+ Miền phát sóng đơn

2. Những thách thức cạnh tranh LAN trong Sensornet

Các tính chất của Sensornet:

+ sensornet thường là mạng đa Hop.

+ sensornet không nhất thiết phải giao tiếp dựa trên kết nối với các node sensornet khác.

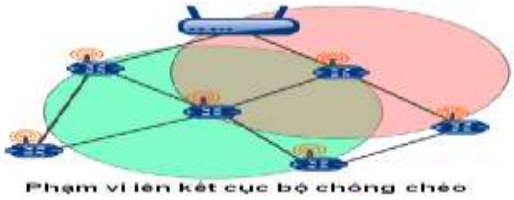
+ môi trường truyền thông là không dây.

=> Các tính chất này làm cho ta nhầm tưởng rằng: cạnh tranh LAN có thể được giải quyết một cách có hiệu quả trong sensornet.

Tuy nhiên, sensornet khác liên kết IP truyền thống một cách rõ rệt. Ethernet và WiFi cung cấp mạng lưới phát sóng rộng với nguồn tài nguyên lớn. Tuy nhiên, sensornet hoạt động với những nguồn tài nguyên hạn chế. Điều này làm giảm độ tin cậy của các gói tin khi truyền.

3. Liên kết IP <=> Phạm vi sóng radio

Mô hình liên kết IP tương đương với *phạm vi liên kết cục bộ* trong các miền phát sóng, kết quả là trong một mạng không dây đa Hop được kết nối bởi nhiều phạm vi liên kết cục bộ chồng chéo như trong hình 2.2.1.



Hình 2.2.1. Phạm vi sóng radio <=> Phạm vi liên kết cục bộ

III. ĐÁNH ĐỊA CHỈ IPv6 VÀ MÔ HÌNH TIỀN TỐ

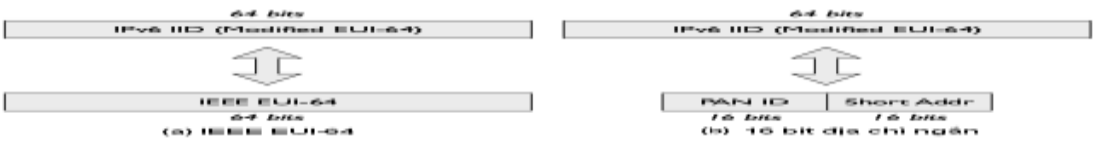
Giao diện được cấu hình với một hoặc nhiều địa chỉ, tiền tố IPv6. Đánh địa chỉ IPv6 phải tuân thủ:

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

+ Kiến trúc IPv6 phải thiết lập được mô hình giữa định danh giao diện và địa chỉ liên kết để địa chỉ lớp mạng và lớp liên kết không cần cache phân giải địa chỉ.

+ 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.

1. Định danh giao diện (IID).



Hình 2.3.1. Mô hình tổng quan giữa Giao diện định danh và Địa chỉ liên kết

Các kiến trúc IPv6 yêu cầu các IID đưa vào định dạng Modified EUI-64, khác với IEEE EUI-64 là sự trái ngược bit *toàn nhóm/cục bộ*. Kết quả là:

+ Một IID xác định từ một địa chỉ ngắn 16-bit liên, thiết lập 16-bit dưới là địa chỉ ngắn, 16-bit trên là của PAN ID hoặc bất kỳ định danh nào xác định duy nhất các PAN.

+ Một IID được xác định địa chỉ liên kết IEEE EUI-64 yêu cầu trái ngược bit *toàn nhóm/cục bộ* với Modified EUI-6.

2. Tiền tố định tuyến toàn cầu

Trong kiến trúc IPv6 của sensornet, tiền tố định tuyến toàn cầu để xác định phạm vi một sensornet. Các node có thể tự do di chuyển trong mạng hoặc thay đổi topo định tuyến mà không bận tâm sự thay đổi địa chỉ IPv6.

IV. TỔNG KẾT

Chương này, mô tả các thành phần vật lý của mạng. Đồng thời, cũng trình bày tổng quan về IPv6 dựa trên kiến trúc mạng, mà vẫn duy trì giao thức lớp và phân tách chức năng của kiến trúc Internet. Sau đó, cũng trình bày về các cơ sở của IPv6 dựa trên kiến trúc mạng, bắt đầu với mô hình liên kết IP tương đương liên kết IP trong phạm vi phát sóng, nêu rõ lý do tại sao cạnh tranh LAN kém phù hợp với các khó khăn và thách thức của sensornet. Chương này, cũng mô tả đánh địa chỉ IPv6 và cấu trúc tiền tố, tận dụng không gian lớn của địa chỉ IPv6 để giảm lưu lượng thông tin và yêu cầu bộ nhớ trong việc gán địa chỉ.

CHƯƠNG III: NÉN HEADER VÀ PHÁT TRIỂN LỚP MẠNG IPv6 ÁP DỤNG CHO SENSORNET

I. ĐIỀU CHỈNH

1. Đối phó với datagram IPv6 lớn

MTU-gói truyền lớn nhất theo IEEE 802.15.4 là 127 byte. Trong khi đó, lớp physical áp đặt overhead tối đa là 25 byte, bảo mật lớp link trong trường hợp tối đa là 21 byte, Header IPv6 dài 40 byte, cả hai giao thức UDP và TCP trên lớp vận chuyển có kích thước Header tương ứng là 8 và 20 byte => chỉ còn 13 byte cho dữ liệu ứng dụng (quá ít).

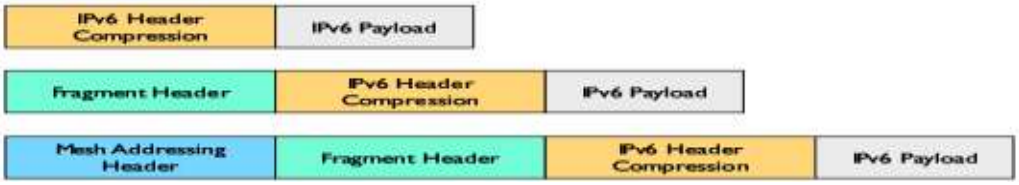
Trong phần này, sẽ đề cập tới một lớp có thể hỗ trợ cơ chế nén Header để giảm chi phí Overhead và tần số phân mảnh datagram IPv6. Lớp thích ứng này hỗ trợ các cơ chế sau: Phân mảnh, Lớp 2 - Chuyển tiếp, Nén Header.

2. Chuyển phát datagram IPv6

Để chuyển phát datagram IPv6 có hiệu quả, đặc biệt là trong sensornet thì định dạng Header phải đơn giản.

2.1. Header dạng ngăn xếp

Định dạng Header 6LoWPAN sử dụng một Header dạng ngăn xếp bắt nguồn từ IPv6, chúng thể hiện các cơ chế hỗ trợ cho lớp tương ứng. Header dạng ngăn xếp 6LoWPAN có từ 2 trường trở lên. Khi đủ tất cả các trường, các trường này phải xuất hiện theo trình tự sau: Mesh Addressing, Fragment và IPv6 Header Compression.



Hình 3.1.1.Các Header dạng ngăn xếp 6LoWAN

a. Fragment: được sử dụng khi dữ liệu quá lớn không phù hợp với một khung đơn IEEE 802.15.4. Nó bao gồm ba trường nhỏ Datagram Size, Datagram Tag, và Datagram Offset.

b. Mesh Addressing: được sử dụng khi khung 6LoWPAN được phân phát qua nhiều Hop phát sóng radio, nó bao gồm ba trường nhỏ: Hop Limit, Source Address, và Destination Address.

c. IPv6 Header Compression: được sử dụng để nén một Header IPv6. Định dạng nén Header sẽ được trình bày trong phần 3.

2.2. Chuyển tiếp tại lớp 2 và lớp 3

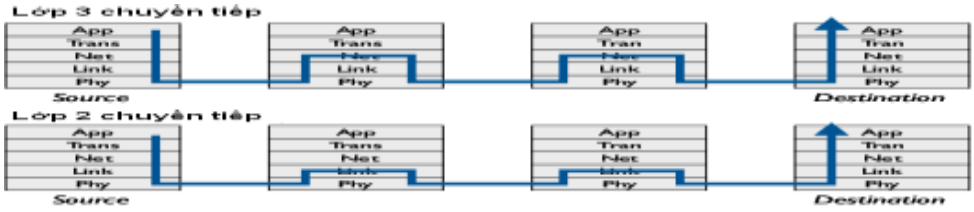
Lớp thích ứng 6LoWPAN cung cấp cơ chế Chuyển tiếp tại lớp 2. Các tổ chức sensornet và IETF, chưa xác định được Chuyển tiếp tại lớp nào hiệu quả hơn.

* Nếu chuyển tiếp ở lớp 2, mạng lưới hoạt động giống như chuyển tiếp đa giao thức. Các lợi ích khi lớp 2 chuyển tiếp là:

+ Các mảnh có thể được gửi qua đa Hop mà không cần phân mảnh hoặc ghép mảnh tại mỗi Hop.

+ Các mảnh trong một datagram có thể đi theo nhiều đường.

+ Cho phép các lớp dịch vụ và điều tiết lưu lượng hoạt động giống như chuyển tiếp đa giao thức.



Hình 3.1.2. Chuyển tiếp tại lớp 3 và lớp 2

* Chuyển tiếp lớp 3 hoạt động với một Hop phát sóng duy nhất.

- Hạn chế duy nhất của Chuyển tiếp tại lớp 3 là nó đòi hỏi phân mảnh và xác nhận lại 6LoWPAN tại mỗi Hop phát sóng.

- Chuyển tiếp tại lớp 3 **"ép"** phân phát mảnh trên một đường duy nhất, lợi ích trong việc sử dụng đường đi duy nhất:

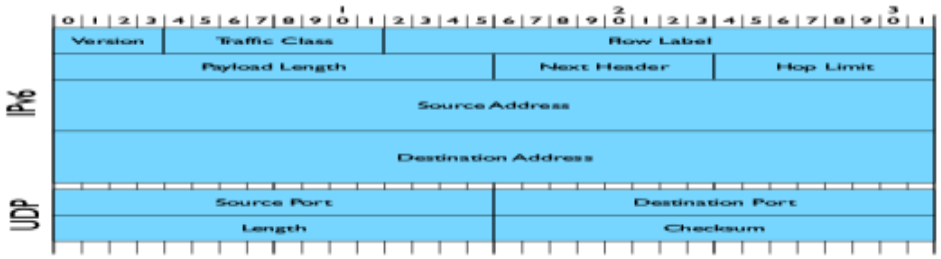
+ Các mảnh được gửi theo thứ tự, đơn giản hóa việc truyền lại tại điểm đích.

+ Chuyển tiếp dọc theo một đường duy nhất cho phép tối ưu hóa lớp liên kết, giảm chi phí truyền dẫn và tăng thông lượng.

+ Lợi dụng các tính tạm thời của liên kết không dây, chuyển tất cả các mảnh dọc theo một đường dẫn.

3. Nén datagram IPv6

Trong khi lớp thích ứng cho phép giao tiếp với datagram IPv6 sử dụng khung IEEE 802.15.4. Nén Header lớp mạng và lớp giao vận là cần thiết để hoạt động hiệu quả. Một chuẩn Header UDP/IPv6 là 48 byte như hình dưới:



Hình 3.1.3. Header UDP/IPv6

3.1. Tổng quát một số loại nén

*** Nén Flow-based**

Nén *flow-based,* dựa trên nén dư thừa trong một và có thể đạt được 1 byte duy nhất cho cả hai Header trong trường hợp tốt nhất.

Nhược điểm của nén *flow-based:* Thứ nhất, cơ chế *flow-based* không thích hợp cho các dòng tốc độ thấp trong sensornet. Thứ hai, *flow-based* thường gánh chịu đáng kể overhead.

***Dòng độc lập, Nén Stateless**

Nén Header Staless không duy trì trạng thái mỗi dòng và do đó dòng độc lập. RFC 4944 nén datagram bằng cách khai thác dư thừa liên lớp, bao gồm cả lớp liên kết, mạng, và giao vận. Trong trường hợp tốt nhất, RFC 4944 có thể nén một tiêu đề UDP/IPv6 xuống 6 byte.

*** Nén shared-context**

Nén *shared-context* đòi hỏi tất cả các node thiết lập một bối cảnh được chia sẻ. 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 bối cảnh được chia sẻ này để nén tiền tố phổ biến thường xuất hiện trong Header.

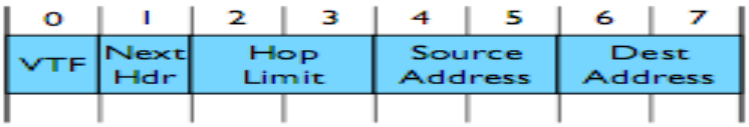
*** Nén kết hợp**

Nén stateless và nén shared-context hoạt động tốt tại lớp mạng. Nén kết hợp là nén stateful cho Header lớp giao vận kết hợp với nén stateless và shared-context tại lớp mạng.

3.2. 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 sử dụng nén kết hợp, nhưng mở rộng để hỗ trợ cả 2 cơ chế stateless và stateful 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; trường *Payload Length* được lược đi; 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. LOWPAN HC hỗ trợ nén tùy ý trường *Next Header* (như UDP hoặc Header mở rộng IPv6).

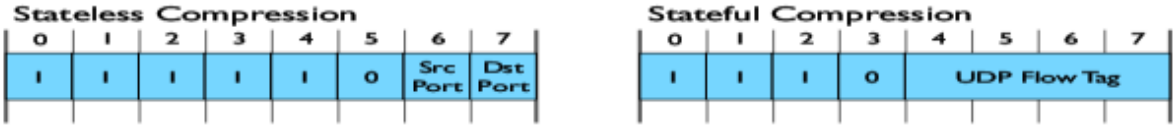


Hình 3.1.4. Kết quả nén Header Ipv6

Như vậy, một Header IPv6 dài 40 byte, nhưng có thể được nén xuống chỉ còn 1 byte duy nhất cho các trường *Version, Traffic Class, Flow Label, Next Header, Hop Limit, Source Address* và *Destination Address.*

3.3. Nén Next Header

LOWPAN HC cho phép nén trường Next Header. Nén Next 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* vì được xác định từ Header lớp thấp hơn.



Hình 3.1.5. Nén Header UDP

Nén Next Header 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.

4. Tổng kết

Trong phần này, đã trình bày một lớp thích ứng để truyền thông các datagram IPv6 sử dụng khung IEEE 802.15.4. Lớp thích ứng hỗ trợ ba chức năng: (i) nén header IPv6 (LOWPAN HC) để giảm tiêu đề overhead, (ii) phân mảnh datagram để hỗ trợ MTU tối thiểu IPv6, và (iii) hỗ trợ cho lớp 2- Chuyển tiếp. Các cơ chế được thể hiện bằng cách sử dụng một định dạng Header dạng ngăn xếp. LOWPAN HC nén Header sử dụng cả hai cơ chế nén kết hợp.

Tuy nhiên, đầu tiên phải xác định một cơ chế tự động cấu hình địa chỉ IPv6 bằng cách sử dụng tiền tố định tuyến toàn cầu và định danh giao diện bắt nguồn từ địa chỉ liên kết. Giải quyết vấn đề tự động cấu hình trong phần sau.

II. CẤU HÌNH VÀ QUẢN LÝ

Lớp mạng IPv6 gồm có ba thành phần: (i) cấu hình và quản lý, (ii) chuyển tiếp, và (iii) định tuyến. Phần này sẽ giới thiệu thành phần đầu tiên, nó rất cần thiết trong việc hình thành và duy trì một mạng IPv6.

1. Cấu hình số lượng lớn các node

Các node phải cấu hình một địa chỉ IPv6 cục bộ để liên lạc với các node láng giềng trên cùng một liên kết IP và một địa chỉ unicast toàn cầu với một tiền tố định tuyến toàn cầu để giao tiếp với các node không nằm trong liên kết IP ở cùng một sensornet hoặc được kết nối với các mạng IP khác. Tất cả các địa chỉ IP phải là duy nhất trong phạm vi tương ứng của chúng.

2. Phát hiện láng giềng (Neighbor Discovery - ND)

2.1. Bối cảnh

IP6-ND cung cấp cơ chế cần thiết cho các node để liên lạc với các node láng giềng và các thiết bị IPv6 khác. IP6-ND được hỗ trợ bởi 5 loại thông điệp:

Quảng bá Router, *Trưng cầu Router*, *Quảng bá Láng giềng*, *Trưng cầu Láng giềng*, và *Chuyển hướng*.

IP6-ND đạt năng lượng thấp <=> LP6-ND (đây là giao thức phát hiện láng giềng được thiết kế cho sensornet). Với LP6-ND, chỉ sử dụng 3 thông điệp *Quảng bá Router*, *Trưng cầu Láng giềng* và *Quảng bá Láng giềng*. So với IP6-ND, LP6-ND chỉ cung cấp các cơ chế cơ bản, giảm IP6-ND đến mức tối thiểu để hỗ trợ nguồn lực hạn chế của sensornet.

2.2. Tìm kiếm Router

a. Quảng bá Router

LP6-ND sử dụng thông điệp *Quảng bá Router* để thông báo sự hiện diện của bộ định tuyến và thông tin cấu hình mạng. Các node láng giềng nghe thông điệp *Quảng bá Router* để tìm kiếm Router cấu hình các tuyến đường mặc định, và tìm các thông số cấu hình. Nó gồm 4 trường như hình dưới đây:

Hình 3.2.1.Định dạng thông điệp Quảng bá Router

b. MultiHop Information Option -Tùy chọn thông tin đa Hop

LP6-ND sử dụng thông điệp *Quảng bá Router* để truyền thông tin từ Router biên giới cho tất cả các node trong sensornet. Các node truyền định kỳ thông điệp *Quảng bá Router* bao gồm *1 tùy chọn* với số thứ tự chỉ thị thông tin. Sau đó, Router phát tán lại thông tin để tuyên truyền ra xa hơn. LP6-ND sử dụng Trickle để quản lý truyền thông điệp *Quảng bá Router*.

Để hỗ trợ Trickle, xác định một tùy chọn cho thông điệp *Quảng bá Router* đó là *MultiHop Information Option*, gồm 2 trường như hình dưới đây:

Hình 3.2.2. Định dạng MultiHop Information Option

c. Time Information Option

Để hỗ trợ đồng bộ hóa thời gian, chúng ta xác định một *Time Information Option* cho thông điệp *Quảng bá Router*. Lựa chọn đại diện cho "giây" sử dụng một trường 4 byte và "phần nghìn giây" sử dụng một trường 2 byte.

Hình 3.2.3. Định dạng Time Information Option

Router chứa *Time Information Option* trong thông điệp *Quảng cáo Router* để thiết lập căn cứ thời gian trên toàn mạng. Trong nhiều ứng dụng sensornet, đồng bộ hóa thời gian là một dịch vụ cần thiết.

d. Trưng cầu Router

Các node có thể gửi thông điệp *Trưng cầu Router* yêu cầu Router láng giềng ngay lập tức tạo ra và truyền thông điệp *Quảng bá Router*.

Hình 3.2.4. Định dạng thông điệp Trưng cầu Router

2.3. Tìm kiếm láng giềng

LP6-ND sử dụng thông điệp *Trưng cầu Router* và *Quảng bá Router* để hỗ trợ phát hiện láng giềng vô cận và láng giềng tiếp cận được. LP6-ND loại bỏ các thông tin láng giềng vô cận do tài nguyên hạn chế. Các giao thức sensornet thường duy trì khả năng tiếp cận cho một subnet láng giềng.

3. Tự động cấu hình địa chỉ

3.1. Bối cảnh

Để giao tiếp với các node láng giềng trên cùng một liên kết, đầu tiên các node phải cấu hình một địa chỉ liên kết cục bộ. Để giao tiếp với các node ở các Hop khác, và node phải cấu hình một địa chỉ toàn cầu.

Cơ chế SLAAC cho phép các node hình thành một địa chỉ IPv6 mà không cần một server trung tâm, nhưng lại không có khả năng cấu hình tập trung hoặc quản lý địa chỉ. Ngoài SLAAC, DHCPv6 được phát triển để hỗ trợ cấu hình tập trung và quản lý địa chỉ IPv6.

3.2. Staless (SLAAC)

SLAAC là stateless vì nó cho phép các node cấu hình địa chỉ của riêng chúng mà không cần một thực thể trung tâm duy trì danh sách địa chỉ IPv6.

Thiết lập tính duy nhất của tất cả các địa chỉ, bao gồm: địa chỉ liên kết cục bộ + địa chỉ phạm vi sensornet.

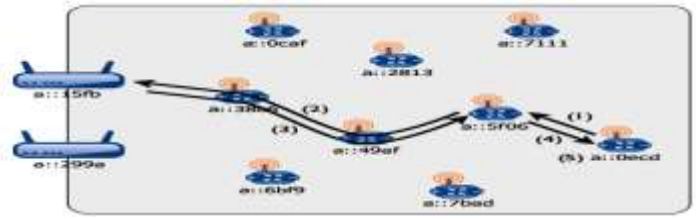
Cơ chế *Phát hiện địa chỉ trùng lặp* sử dụng multicast để duy trì tính duy nhất của địa chỉ mà không cần một server trung tâm. Tuy nhiên, truyền thông multicast qua nhiều bước rất tốn kém với sensornet nguồn tài nguyên hạn chế.

Trong khi DHCPv6 đại diện cho tiếp cận cơ chế stateful, nó cho phép các node tránh giao tiếp multicast khi thiết lập tính duy nhất.

3.3. Stateful (DHCPv6)

DHCPv6 đại diện cho phương pháp tiếp cận stateful với địa chỉ tự động cấu hình. Các node yêu cầu địa chỉ IPv6 từ một server DHCPv6 trung tâm.

Một node chỉ có thể sử dụng duy nhất một DHCP (mặc dù trong mạng có nhiều DHCP) điều này tránh địa chỉ bị trùng lặp.



Hình 3.2.5. DHCPv6 phân phối địa chỉ trong sensornet

4. Thông điệp Thông tin và Thông điệp Lỗi ICMPv6

Ngoài việc cung cấp các quy định cấu hình lớp mạng và các giao thức quản lý, ICMPv6 (Internet Control Message Protocol – Giao thức thông điệp kiểm soát mạng) cung cấp thông tin chung về tình trạng của mạng thông qua Thông điệp Thông tin và Thông điệp Lỗi.

Thông điệp Lỗi ICMPv6 chứa những lỗi gây ra bởi datagram IPv6 để nơi phát datagram có thể xác định tốt hơn nguyên nhân gây ra lỗi.

VD: Thông điệp Lỗi = 0 : không có tuyến đường đến điểm đích

= 3 : địa chỉ không thể truy cập

= 4 : Port không thể truy cập

5. Tổng kết

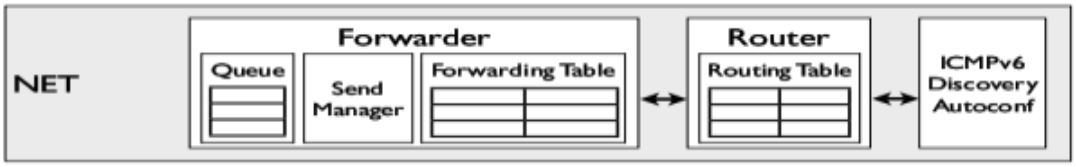
Trong phần này, tập trung vào các dịch vụ thiết yếu để hình thành và duy trì một mạng IPv6. Phần này đã cho thấy làm thế nào để khám phá láng giềng để hỗ trợ sensornet. Phần này cũng trình bày phương pháp tự động cấu hình địa chỉ cho cả địa chỉ IPv6 liên kết cục bộ và toàn cầu, để các node IPv6 có thể giao tiếp

với Host láng giềng IPv6 và các thiết bị IPv6 có thể kết nối với các mạng IP khác. Mục 3 của phần này, bao gồm cơ chế SLAAC và DHCPv6, làm cho chúng khả thi trong sensornet.

III. CHUYỂN TIẾP

1. Chuyển tiếp Datagram với Năng lượng-hiệu quả

Kiến trúc IP truyền thống tách biệt bộ chuyển tiếp và bộ định tuyến. Cơ chế này ngược lại với cơ chế trong sensornet - thường tích hợp chuyển tiếp và định tuyến với nhau, IPv6 dựa trên kiến trúc sensornet duy trì sự tách biệt.



Hình 3.3.1. Tách biệt giữa bộ chuyển tiếp và bộ định tuyến

2. Chuyển tiếp Unicast

2.1. Bối cảnh

Mở rộng hỗ trợ cho mạng là cần thiết để nâng cao hiệu suất tổng thể mạng, đó là việc hỗ trợ end-to-end bằng cách phát hiện và thông báo tắc nghẽn trong hệ thống mạng.

Cơ chế kiểm soát Hop-by-Hop, ngoài việc phát hiện và thông báo tắc nghẽn nó còn kiểm soát mạng. Cơ chế Hop-by-Hop rất thích hợp trong mạng không dây đa Hop với phạm vi rộng, nguồn tài nguyên hạn chế.

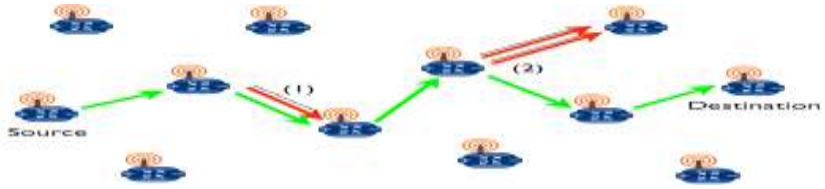
2.2. Phục hồi Hop-by-Hop

Các datagram mà không đi được tới đích đồng nghĩa với việc lãng phí năng lượng. Bộ chuyển tiếp thực hiện phục hồi Hop-by-Hop để tăng tốc độ truyền dẫn end-to-end khi phân chia datagram. So với truyền lại End-to-end, truyền lại Hop-by-Hop chỉ xảy ra tại các node và nơi xảy ra sự cố truyền dẫn, đồng thời nó cũng thích nghi nhanh chóng với phạm vi cục bộ. Tuy nhiên, truyền lại end-to-end lại xảy ra cho tất cả các node từ phạm vi xảy ra sự cố tới node nguồn, điều này làm tăng độ trễ phục hồi và chi phí năng lượng.

a. Truyền lại

Để giảm gói tin "drop", bộ chuyển tiếp áp dụng phương pháp truyền tin cậy các thông điệp ra khỏi hàng đợi, sau đó việc nhận sẽ được xác nhận được bởi đích cuối cùng.

Để đảm bảo các lỗi xuất hiện bất ngờ sẽ ngăn cản việc phân phát gói tin, thì bộ chuyển tiếp lấy thông điệp từ hàng đợi sau để truyền lại dưới một ngưỡng số gói tin nào đó.



Hình 3.3.2 Phục hồi Hop by Hop

b. Hỗ trợ tái định tuyến

Với truyền thông không dây, thì chất lượng liên kết là rất khác nhau và có tính cục bộ tạm thời do tác động môi trường và node di động. Khi liên kết thất bại xảy ra thì tái định tuyến là phương pháp giải quyết tối ưu.

Tái định tuyến có thể nhân bản các datagram trong khi chuyển tiếp. Để ngăn chặn các bản sao, node nguồn đánh dấu mỗi gói tin được tạo ra với một số thứ tự duy nhất. Sử dụng địa chỉ nguồn và số thứ tự, đảm bảo bộ chuyển tiếp có thể phát hiện và ngăn chặn các thông điệp trùng lặp trong hàng đợi chuyển tiếp.

2.3. Streaming

Bộ chuyển tiếp thực hiện luồng dữ liệu để giảm chi phí năng lượng truyền thông điệp. Việc tối ưu hóa luồng dữ liệu ở lớp liên kết sẽ giảm việc truyền overhead, tăng thông lượng và tăng tính hiệu quả.

Để tăng cơ hội cho luồng dữ liệu, bộ chuyển tiếp làm trễ việc truyền thông điệp mà bị đánh dấu là chịu trễ. Trong khi lưu giữ thông điệp chịu trễ trong hàng đợi thì việc tối ưu luồng lớp liên kết cho phép bộ chuyển tiếp truyền đa gói một cách nhanh chóng. Sau đó bộ chuyển tiếp sẽ rỗi để nhận luồng chuyển tiếp từ các node láng giềng.

2.4. Kiểm soát tắc nghẽn

Nguyên nhân tắc nghẽn mạng do: chiếm lĩnh hành đợi chuyển tiếp hoặc cạnh tranh kênh truyền. Phát hiện tắc nghẽn theo 2 cách:

+ Bộ chuyển tiếp phát hiện tắc nghẽn khi nó không nhận được sự xác nhận từ các Hop đích tiếp theo hoặc tổn hao liên kết không dây. Trong cả 2 trường hợp bộ chuyển tiếp phải giảm lan truyền để tránh cạnh tranh và va chạm mở rộng.

+ Bộ chuyển tiếp phát hiện tắc nghẽn bằng cách giám sát sự chiếm dụng hàng đợi, chỉ ra tắc nghẽn khi hàng đợi đầy.

3. Chuyển tiếp multicast

3.1. Truyền thông Multicast

Các phương pháp truyền thống tạo ra cây phân phối Multicast, nó làm việc tốt nhất khi topo mạng tương đối tĩnh. Node di động trong liên kết không dây thường làm việc duy trì cây phân phối multicast tốn kém và khó khăn.

Để hỗ trợ IP multicast trong các mạng ad-hoc là cơ chế loang. Ở dạng cơ bản, tất cả các node trong phạm vi nhận tất cả các datagram multicast. Node chuyển tiếp nhận được một datagram rồi tiếp tục chuyển tiếp datagram này và các datagram ở các lớp bên trên nếu là thành viên với nhóm multicast. Do vậy, Router không cần phải duy trì cây phân phối hoặc thành viên nhóm multicast.

3.2. Trickle dựa trên Multicast

Trickle cung cấp bộ chuyển tiếp hiệu quả, cũng như phân phát tin cậy thông qua các thuộc tính của nó. Chuyển tiếp thông điệp multicast có thể được xem như là vấn đề thống nhất trạng thái, nơi mà tất cả các node có được những thông điệp multicast mới nhất. Một node tiếp nhận số thứ tự cũ hơn chỉ ra rằng một láng giềng không có thông điệp multicast mới nhất, bộ chuyển tiếp sẽ sắp xếp việc truyền lại thông điệp multicast sau đợt quảng bá tiếp theo. Thông điệp multicast mới hơn ghi đè lên các thông điệp multicast cũ. Bằng cách thực thi một kênh chuyển tiếp duy nhất, sự chuyển tiếp multicast hỗ trợ năng lượng hiệu quả và đáng tin cậy với trạng thái chuyển tiếp tối thiểu.

4. Tổng kết

Trong phần này, trình bày việc thiết kế bộ chuyển tiếp với năng lượng hiệu quả cho cả datagram unicast và multicast. Bộ chuyển tiếp unicast sử dụng truyền lại Hop-by-Hop, Streaming, kiểm soát tắc nghẽn để chuyển tiếp năng lượng hiệu quả với end-to-end tỉ lệ thành công cao. Bộ chuyển tiếp multicast sử dụng các thuật toán Trickle để đạt được hiệu quả năng lượng và nhận biết được mật độ loang.

Sự tương tác giữa bộ chuyển tiếp và bộ định tuyến có thể hỗ trợ để nâng cao thực hiện giao thức định tuyến trong khi vẫn tiết kiệm năng lượng. Phần sau, sẽ nói về một giao thức định tuyến hiệu quả cho sensornet.

IV. ĐỊNH TUYẾN

1. Bối cảnh

Giao thức định tuyến có trách nhiệm phát hiện các tuyến đường tới điểm đích. Giao thức định tuyến thường rơi vào 2 loại: *Vector khoảng cách* và *trạng thái liên kết*.

2. Các tuyến đường mặc định

Phần này, mô tả cách thức giao thức định tuyến lựa chọn và duy trì các tuyến đường mặc định.

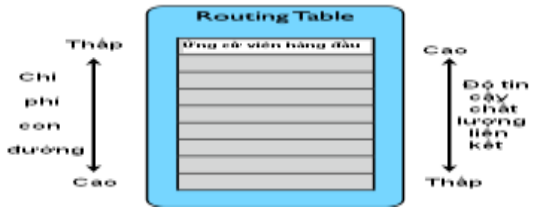
2.1. Khám phá các tuyến đường tiềm năng

Router sử dụng thông điệp *Quảng bá Router* để thông báo sự hiện diện của Router và cho phép các node khám phá các Router láng giềng.

Để phát hiện ra các node nhanh chóng, Router có thể truyền tải thông điệp *Trưng cầu Router* để yêu cầu thông điệp *Quảng bá Router* từ các node láng giềng.

2.2. Quản lý Bảng định tuyến

Gồm 3 thao tác: + Chèn vào bảng định tuyến.
+ Thúc đẩy trong bảng định tuyến.
+ Loại bỏ khỏi bảng định tuyến.



Hình 3.4.1. Quản lý bảng định tuyến

2.3. Lựa chọn một tuyến đường mặc định

Router thường lựa chọn *mục đầu* trong bảng định tuyến để sử dụng như là tuyến đường mặc định. Tuy nhiên, Router có thể chọn các *mục* khác vì hai lý do:

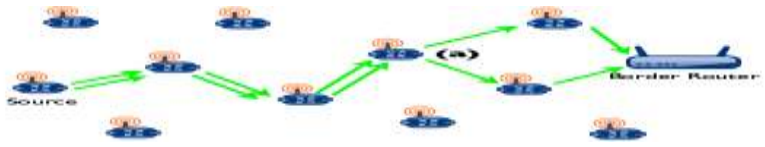
+ Để hỗ trợ tái định tuyến khi cố gắng truyền liên tục *mục đầu* không thành công.

+ Để thăm dò các ứng cử viên khác, làm tăng sự tin cậy tỷ lệ liên kết thành công, và tìm kiếm ứng cử viên để thúc đẩy bảng định.

Trong một số trường hợp, vòng lặp định tuyến (*số Hop hiện hành* ≤ *số Hop trong mục*) có thể xảy ra. Việc ngẫu nhiên lựa chọn các *mục* trong khi tái định tuyến sẽ giúp giảm thiểu sự xuất hiện của vòng lặp định tuyến.

Hình 3.4.2. Tái định tuyến

Thỉnh thoảng, Router cấu hình các tuyến đường mặc định với các *mục khác* để tiếp tục tìm kiếm các tuyến đường với chi phí tương tự hoặc thấp hơn, ngay cả khi các ứng cử viên hàng đầu vẫn hoạt động tốt. Vì lấy ngẫu nhiên thông điệp để sử dụng là tuyến đường mặc định, bộ định tuyến cấu hình mặc định các tuyến có các Hop ít hơn hoặc bằng toàn bộ các Hop như trong hình vẽ:



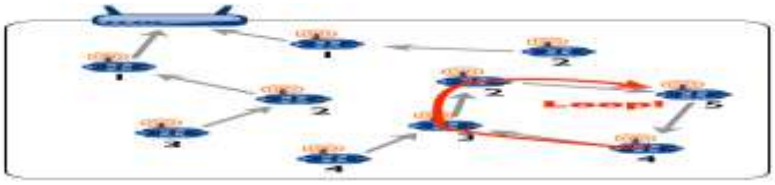
Hình 3.4.3. Cập nhật ước tính liên kết chất lượng

Router (a) trong hình trên chuyển tiếp datagram theo hai liên kết khác nhau.

2.4. Duy trì nhất quán tuyến đường

Thông tin định tuyến trở nên không phù hợp khi các thay đổi này chưa được truyền đến các node khác trong mạng.

(1) Router có thể phát hiện các vòng lặp định tuyến bằng cách sử dụng thông tin số Hop của Router biên giới. Chuyển tiếp thông điệp với số Hop > số Hop hiện hành của node cho ta biết sự không thống nhất và khả năng xảy ra một vòng lặp định tuyến, như trong hình 3.4.4.



Hình 3.4.4. Phát hiện vòng lặp định tuyến

(2) Các Router có thể phát hiện đường dẫn không hiệu quả và cải thiện đường bằng dẫn này bằng cách quan sát sự khác biệt đáng kể trong chi phí quảng cáo đường dẫn.

Trong cả hai trường hợp, Router phản ứng bằng cách đặt lại thời điểm *Quảng bá Router* để nhanh chóng cập nhật thông tin định tuyến cho các node láng giềng.

3. Tuyến đường Host

Các tuyến đường mặc định cung cấp khả năng tiếp cận giữa node sensornet đến Router biên giới và bất kỳ thiết bị IP khác kết nối với mạng IP. Các node sensornet báo cáo tuyến đường mặc định của chúng tới các Router biên giới gần nhất. Router biên giới sau đó đảo ngược những tuyến đường để hình thành *tuyến đường Host* cho mỗi node sensornet. Các node sensornet đều không phải duy trì bất kỳ trạng thái nào cho các *tuyến đường host,* mà nó được thực hiện bởi Router.

3.1. Kiến thức tuyến đường Host

Các node sensornet cung cấp thông tin tuyến đường mặc định của chúng bằng cách gửi định kỳ thông điệp *ghi-tuyến đường* tới Router biên giới sử dụng các tuyến đường mặc định của chúng.

Thông điệp *ghi-tuyến đường* chứa danh sách các node chuyển tiếp thông điệp đó. Mỗi node chuyển tiếp thông điệp đều gắn địa chỉ của mình vào danh sách.

3.2. Định tuyến biên giới

Sử dụng thông tin tuyến đường mặc định được cung cấp bởi mỗi node sensornet, Router biên giới có thể tạo ra một cây bao trùm cho toàn bộ mạng và sử dụng nó để tạo ra *các tuyến đường Host* trở lại cho mỗi node. Khi Router biên giới nhận được một datagram, nó sẽ tra cứu trong cây bao trùm để xác định một tuyến đường đến đích. Nếu không có tuyến đường hợp lệ có sẵn cho node đó, Router biên giới tạo ra một "lỗi không tiếp cận Host ICMP". Nếu đích đến trong phạm vi sóng radio, Router biên giới sẽ chuyển tiếp datagram đó như bình thường. Nếu đích đến phải qua nhiều Hop, Router biên giới sẽ chèn một tiêu đề định tuyến có chứa một danh sách các địa chỉ trong gói tin để đi đến đích cuối cùng. Các node chuyển tiếp gói tin bằng cách xử lý tiêu đề định tuyến để xác định đích đến Hop tiếp theo cho gói tin.

4. Tổng kết

Trong phần này, đã trình bày một giao thức định tuyến đường cơ sở được thiết kế cho những khó khăn điển hình về tài nguyên và khối lượng công việc của sensornet. Giao thức định đường cơ sở tập trung trạng thái tại Router biên giới để giảm thiểu yêu cầu tài nguyên giữa các node sensornet.

V. TỔNG KẾT

Như vậy, trong chương III này đã phát triển lớp mạng IPv6 hoàn chỉnh cho sensornet bao gồm cấu hình và quản lý, chuyển tiếp và định tuyến. Sử dụng kiến trúc và các cơ chế thực hiện, lớp mạng có thể cung cấp cách tiếp cận phân phát datagram với "nỗ lực cao nhất" giữa một node sensornet và bất kỳ thiết bị IP khác.

CHƯƠNG IV: NÉN HEADER CỦA IPV6 ÁP DỤNG CHO WSN

I. GIỚI THIỆU

Với quy mô hiện tại và sự tăng trưởng nhanh chóng 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 sự can thiệp tất cả các node phải liên quan đến các địa chỉ IP. Khi IPv4 ra khỏi các ứng dụng và không gian toàn cầu của mình, thì địa chỉ IP này không thể coi là hữu hiệu đối với mạng cảm biến. Trong bối cảnh đó, 6LoWPAN (*Mạng cá nhân không dây năng lượng thấp*) 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.

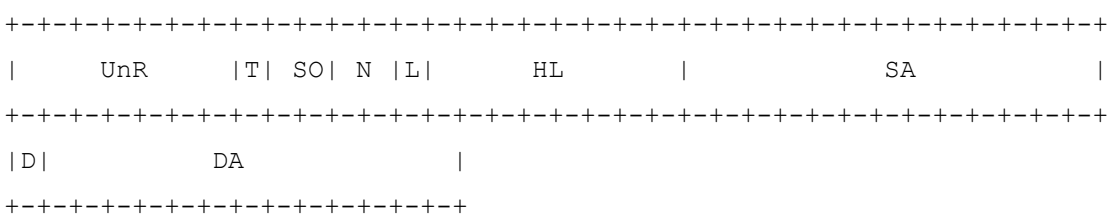
II. BỐI CẢNH CỦA VẤN ĐỀ

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. Tiếp sau, sử dụng 8 byte cho UDP, như vậy chỉ còn 33 byte cho dữ liệu ứng dụng. Tình hình này, rõ ràng phải nhấn mạnh nhu cầu nén Header và phân mảnh.

Sử dụng phân mảnh và kết hợp mảnh sẽ dẫn đến lãng phí không cần thiết về năng lực tính toán và năng lượng.

Vì vậy, để tránh sử dụng phân mảnh và kết hợp mảnh do tiêu tốn năng lượng. Nén Header đưa ra như một cách giải quyết hợp lý để giảm tiêu tốn năng lượng bằng cách lược bỏ hoặc giảm thiểu một số tính năng nhất định của IPv6.

III. ĐỊNH DẠNG HEADER IPv6 ĐƯỢC NÉN XUỐNG 6 BYTE



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

*** SO: Security Option: 2 bit** SO=00: Không bảo mật

SO=01: Chứng thực

SO=10: Mật mã

SO=11: Để dành

*** 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

*** L: Loose Source Routing: 1 bit:** thiết lập để xác định gói tin được gửi bởi Header Định tuyến mở rộng.

*** HL: Hop Limit: 8 bit :** 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 nguồn được nén xuống 13 bit.

*** D: Destination Address Type: 1 bit** D=0: Unicast

D=1: Multicast

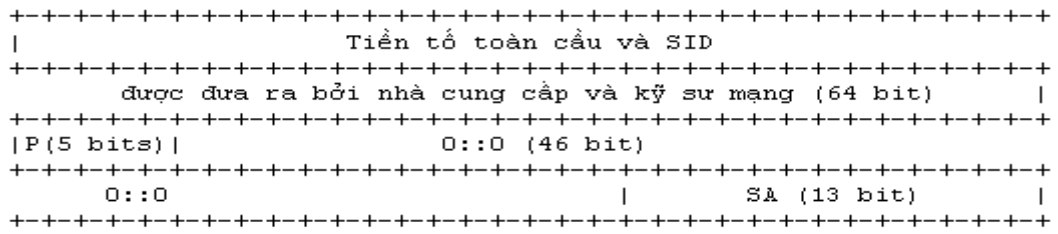
Nó xác định xem địa chỉ đích là Anycast hay Multicast.

*** DA: Destination Address: 13 bit:** Địa chỉ đích được nén xuống 13 bit.

IV. ĐÁNH ĐỊA CHỈ

Phần này xác định mô hình đánh địa chỉ của địa chỉ nén IPv6.

1. Địa chỉ Unicast toàn cầu



P: 5 bit tiền tố 6LoWPAN. Trường này chỉ ra rằng địa chỉ này là một địa chỉ 6LoWPAN, và được thiết lập là 11111b.

SA: 13-bit địa chỉ ngắn

2. 13-bit địa chỉ ngắn

Các node trong cùng mạng sẽ có một địa chỉ 13-bit. Ngoài ra, 256 địa chỉ được dành riêng cho các máy ngoài mạng 6LoWPAN. Các địa chỉ ngắn này được chỉ định bởi một tiền tố 5-bit là 11111b.

VI. 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 Phần IV;

1. Sơ đồ nén 40 byte thành 6 byte

2. Mã 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;
}
```

3. Sơ đồ giải nén 6 byte thành 40 byte

4. Mã 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
}
```

VII. NHẬN XÉT VÀ HƯỚNG PHÁT TRIỂN

1. Nhận xét

- Kết quả thu được: Header 6 byte thay cho 40 byte như thiết kế ban đầu.
- Thuật toán nén và giải nén đơn giản và dễ hiểu và dễ dàng triển khai.
- Làm giảm đáng kể một số tính năng nhất định của IPv6 không cần thiết cho WSN.
- Đặc biệt, tiết kiệm nguồn năng lượng hạn chế của WSN.

=> tính năng IPv6 + nén Hader IPv6 <=> thành công trong việc triển khai IPv6 trên kiến trúc WSN

2. Hướng phát triển

- Phần trên, em đã trình bày mô hình nén thành công trên phần mềm ứng dụng.
- Trong tương lai, hi vọng rằng đây không phải là một hướng nghiên cứu, mà nó sẽ được tích hợp thực tế trong phần cứng. Để từ đó, có thể triển khai ứng dụng này trong thực tế. Và đây cũng chính là nền móng cho những phương pháp nén hiệu quả hơn sau này.

CÁC TÀI LIỆU THAM KHẢO

[1] http://www.cisco.com

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

[3] Giới thiệu về thế hệ địa chỉ Internet mới IPv6 – Nhà xuất bản bưu điện

[4] Sensor Networks của Thomas Haenselmann

[5] Wireless Sensoe Network design and implement của Jonathan W. Hui