TRƯỜNG ……..

KHOA……

Báo cáo tốt nghiệp

Đề tài:

NGHIÊN CỨU MỘT SỐ GIẢI PHÁP AN NINH TRONG MẠNG WLAN 802.11

DANH MỤC THUẬT NGỮ VIẾT TẮT

2G	Post Second Generation
3G	Post Third Generation
AAD	Additional Authentication Data
BSS	Basic Service Set
CBC	cipher block chaining
CCMP	Counter Mode with CBC-MAC protocol
CDPD	Cellular Digital Packet Data
CRC	Cyclic redundancy check
CSMA	carrier sense multiple access
DIFS	Distributed Inter-Frame Space
DSSS	Direct-sequence spread spectrum
EAP	Extensible Authentication Protocol
EAP-KCK	EAPOL Key Confirmation Key
EAP-KEK	EAPOL Key Encryption Key
EIFS	Extended Inter-Frame Space
ERP	Extended Rate PHY
ESS	Extended Service Set
FHSS	Frequency-hopping spread spectrum
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HR/DSSS	High Rate / Direct Sequence Spread Spectrum
IBSS	Independent Basic Service Set
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IR	Infrared
ISM	Industrial, Scientific, and Medical
KGD	Key Generation and Distribution

LAA	locally administered address
LLC	Logical Link Control
MAC	Medium Access Control
MIC	Message Intergrity Check
MPDU	Mac Protocol Data Unit
MSDU	Mac Service Data Unit
NAV	Network Allocation Vector
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Sysems Interconnection
PDA	Personal Digital Assistant
PHY	Physical Layer
PIFS	PCF Inter-Frame space
PLCP	Physical Layer Convergence Procedure
PMD	Physical Medium Dependant (PMD)
PN	Packet Number
PPP	Point to Point Protocol
RADIUS	Remote Access Dial-In User Service
TSC	TKIP sequence counter
UAA	Universally administered address
UNII	Unlicensed National Information Infrastructure
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
PEAP	Protected EAP
EAP-TLS	EAP Transport Layer Security
EAP-TTLS	EAP Tunneled Transport Layer Security
PRGA	Pseudo-Random Generation Algorithm
KSA	Key Scheduling Algorithm

DANH MỤC HÌNH VẼ

MỞ ĐẦU

1. Nền tảng và mục đích

Mạng không dây WLAN 802.11 hiện được áp dụng trong rất nhiều lĩnh vực bởi những ưu thế nổi trội của nó có với mạng LAN hữu tuyến: người dùng có thể di chuyển trong phạm vi cho phép, có thể triển khai mạng ở những nơi mà mạng hữu tuyến không thể triển khai được. Tuy nhiên, khác với mạng có dây truyền thống, mạng không dây WLAN 802.11 sử dụng kênh truyền sóng điện từ, và do đó đặt ra nhiều thách thức trong việc xây dựng đặc tả và triển khai thực tế mạng này. Một trong những thách thức đó và cũng là vấn đề nóng hổi hiện nay là vấn đề an ninh cho mạng.

Đã có nhiều giải pháp an ninh ra đời nhằm áp dụng cho mạng WLAN, trong đó chuẩn 802.11i được đặc tả với tham vọng mang lại khả năng an toàn cao cho mạng WLAN. Tuy vậy, việc hỗ trợ các phần cứng cũ cộng với việc đặc tả cho phép các nhà sản xuất phần cứng được quyết định một số thành phần khi sản xuất khiến cho các mạng 802.11i khi triển khai không những không đồng nhất mà còn có những rủi ro an ninh riêng. Bên cạnh đó, việc bỏ qua tiêu chí tính sẵn sàng khi xây dựng đặc tả an ninh cho 802.11 khiến cho mạng này không chống lại được kiểu tấn công từ chối dịch vụ.

Do đó, mục đích của luận văn này là nghiên cứu, phân tích đặc điểm an ninh của mạng WLAN 802.11 trên các tiêu chí: tính bí mật, tính toàn vẹn, xác thực hai chiều và tính sẵn sàng. Trên cơ sở đó, đề xuất một mô hình mạng WLAN an toàn với khả năng phòng chống kiểu tấn công DoS và khả năng đảm bảo an ninh cao dựa trên việc xác định cụ thể các phương pháp được áp dụng tại từng bước trong mô hình hoạt động của mạng này.

2. Cấu trúc của luận văn

Ngoài phần mở đầu và kết luận, nội dung của luận văn được bố cục như sau:

Chương 1: trình bày các kiến thức tổng quan về mạng không dây và đặc biệt là mạng WLAN sử dụng chuẩn IEEE 802.11 để từ đó có được cái nhìn bao quát về cách thức hoạt động của mạng.

Chương 2: đi sâu nghiên cứu các giải pháp an ninh áp dụng cho mạng 802.11 dựa trên hai khía cạnh: đảm bảo an toàn dữ liệu và toàn vẹn dữ liệu. Bên cạnh việc cung cấp tổng quát về quá trình phát triển cũng như cải tiến của các phương pháp, chương này cũng chỉ ra những rủi ro an ninh phổ biến đối với mạng WLAN.

Chương 3: trình bày và giới thiệu các phương pháp xác thực được áp dụng trong mạng WLAN với mục đích tập trung vào phương pháp xác thực dựa trên 802.1X để có thể thấy được quá trình xác thực và truyền khóa bí mật giữa các bên trong quá trình này.

Chương 4: nghiên cứu, phân tích tính chất sẵn sàng đối với mạng WLAN mà cụ thể là với giao thức an ninh mới nhất 802.11i để có được cái nhìn toàn vẹn về các vấn đề an ninh đối với mạng WLAN. Từ đó, đề xuất một mô hình mạng WLAN với những cải tiến và sửa đổi để đáp ứng được các yêu cầu về an ninh cho mạng này

Cuối cùng là phần phụ lục và tài liệu tham khảo.

CHƯƠNG 1. TỔNG QUAN MẠNG WLAN 802.11

Sự phát triển và gia tăng của các thiết bị di động như máy tính xách tay (laptop), thiết bị trợ giúp cá nhân (PDA), … đã không những mở rộng phạm vi hoạt động vật lý mà còn làm gia tăng tính di động của lĩnh vực điện toán. Cũng như vậy, mạng máy tính ngày nay không chỉ bó hẹp trong lĩnh vực kỹ thuật mà đã vươn ra mọi lĩnh vực của cuộc sống. Điều tất yếu dễ thấy là cần có một công nghệ thỏa mãn được cả hai nhu cầu: mạng và tính di động. Công nghệ mạng không dây được nghiên cứu và ra đời nhằm khắc phục những hạn chế đó.

1.1. Phân loại mạng không dây

1.1.1. Khái niệm

Công nghệ không dây hiểu theo nghĩa đơn giản nhất là công nghệ cho phép các thiết bị giao tiếp với nhau mà không cần sử dụng đến dây dẫn. Phương tiện truyền dẫn ở đây chính là sóng điện từ truyền qua không khí.

Mạng không dây về cơ bản là mạng đóng vai trò phương tiện vận chuyển thông tin giữa các thiết bị và mạng có dây truyền thống (mạng xí nghiệp, Internet) [2].

1.1.2. Phân loại

Mạng không dây chủ yếu được phân thành 3 loại dựa vào phạm vi hoạt động của chúng:

- WWAN (Wireless Wide Area Network) – Mạng không dây diện rộng
  Là mạng sử dụng các công nghệ không dây phủ sóng diện rộng như: 2G, 3G, GPRS, CDPD, GSM, … Vùng phủ sóng của công nghệ này đạt từ vài trăm mét tới vài kilômét.

- WLAN (Wireless Local Area Network) – Mạng không dây cục bộ
  Là mạng sử dụng các công nghệ không dây như: IEEE 802.11, HyperLan, …
  Phạm vi phủ sóng của mạng này nằm trong khoảng dưới 200 mét.

- WPAN (Wireless Personal Area Network) – Mạng không dây cá nhân
  Là mạng sử dụng các công nghệ như: Bluetooth, Sóng hồng ngoại (IR-

InfraRed) với phạm vi phủ sóng nhỏ hơn 10 mét.

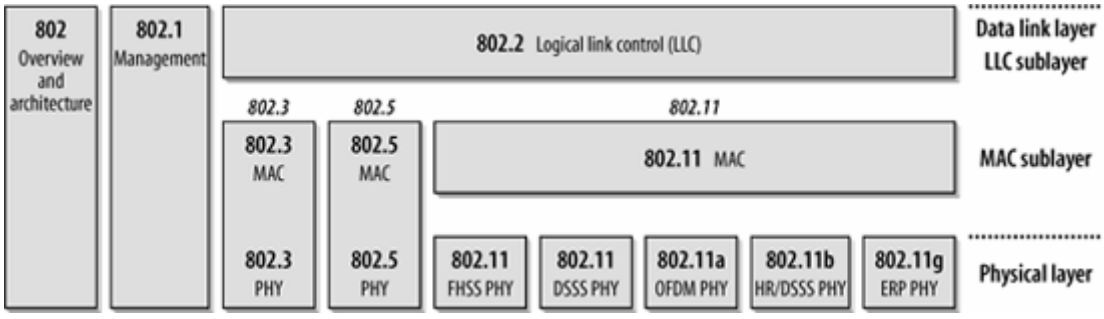
Nội dung của chương này và xuyên suốt toàn bộ luận văn sẽ tập trung vào mạng không dây cục bộ WLAN sử dụng công nghệ IEEE 802.11 của Viện Công nghiệp điện và điện tử Mỹ (IEEE).

1.2. Chuẩn IEEE 802.11

Chuẩn IEEE 802.11 (hay gọi tắt là chuẩn 802.11) là một thành phần của họ IEEE 802 – một tập hợp các đặc tả cho công nghệ mạng cục bộ. Xuất phát điểm chuẩn này được IEEE đưa ra vào năm 1987 như một phần của chuẩn IEEE 802.4 với tên gọi IEEE 802.4L. Năm 1990, nhóm làm việc của 802.4L đã được đổi tên thành Uỷ ban dự án WLAN IEEE 802.11 nhằm tạo ra một chuẩn 802 độc lập. Được chấp thuận vào ngày 26 tháng 6 năm 1997, đến nay chuẩn 802.11 đã có tới 16 đặc tả đã được phê duyệt cũng như đang được hoàn thiện (xem Phụ lục 1).

Các đặc tả của tập chuẩn IEEE 802 tập trung vào hai tầng thấp nhất trong mô hình tham chiếu OSI là tầng liên kết dữ liệu và tầng vật lý. Chuẩn 802.2 đặc tả lớp liên kết dữ liệu chung LLC (Điều khiển liên kết lôgic) được sử dụng bởi các lớp bên dưới thuộc mọi công nghệ LAN nhằm tạo tính tương thích giữa chúng cũng như cung cấp cái nhìn trong suốt từ các tầng bên trên (từ tầng Ứng dụng cho tới tầng Mạng). Bên cạnh đó, tất cả các mạng 802 đều có một tầng con MAC (tầng con Điều khiển truy cập thiết bị) và tầng vật lý (PHY) riêng trong đó:

- Tầng con MAC (thuộc tầng Liên kết dữ liệu) là một tập các luật xác định cách thức truy cập thiết bị phần cứng và gửi dữ liệu.
- Tầng Vật lý (PHY) đảm nhiệm chi tiết việc gửi và nhận dữ liệu bằng thiết bị phần cứng.



Hình 1-1. Quan hệ giữa tập chuẩn IEEE 802 và mô hình tham chiếu OSI

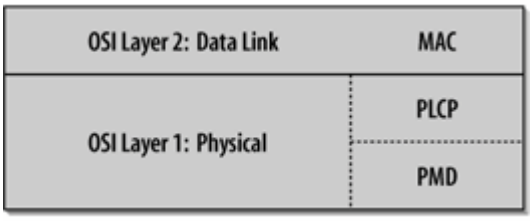
Như vậy, thực chất chuẩn 802.11 là một tập hợp các đặc tả cho hai thành phần: tầng con MAC và tầng Vật lý. Chúng ta sẽ đi xem xét chi tiết hai thành phần này ở các phần tiếp theo.

1.2.1. Tầng vật lý

Tầng vật lý trong chuẩn 802.11 đảm nhiệm việc gửi và nhận dữ liệu trên các thiết bị phần cứng không dây sử dụng ăngten và sóng radio truyền trong không khí. Chuẩn 802.11 sử dụng hai dải tần số radio phục vụ cho việc truyền/ gửi thông tin:

- Dải tần 2,4 ÷ 2,5 GHz (hay còn gọi là dải tần ISM)
- Dải tần ~5GHz (hay còn gọi là dải tần UNII)

Về mặt logic, tầng vật lý được chia ra làm hai lớp con: lớp Thủ tục hội tụ tầng vật lý (PLCP) và lớp Phụ thuộc thiết bị vật lý (PMD). Lớp con PLCP đóng vai trò keo gắn kết giữa các frame từ tầng MAC và việc truyền sóng radio qua không khí. Mọi MAC frame gửi đi và đến sẽ được chuyển tới lớp PLCP. Lớp PMD thực hiện việc gửi mọi bit dữ liệu nó nhận từ lớp PLCP vào không khí thông qua ăng ten.



Hình 1-2. Kiến trúc logic tầng vật lý

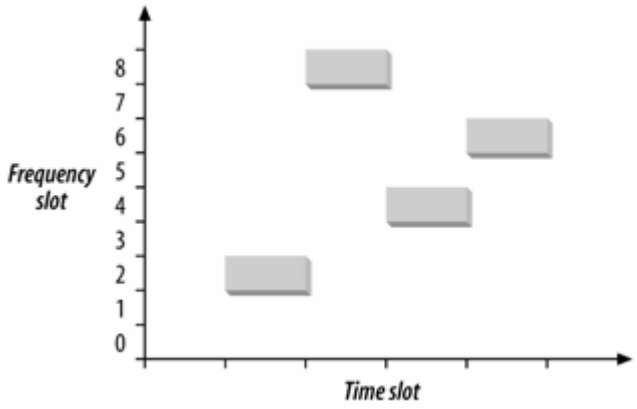
Về mặt vật lý, vào thời điểm mới ra đời (1997), chuẩn 802.11 cơ sở đã đặc tả ba công nghệ dành cho tầng vật lý: Trải phổ nhảy tần (FHSS), Trải phổ trực tiếp (DSSS) và công nghệ sóng hồng ngoại (IR). Tính đến nay, đã có thêm 3 công nghệ được phê chuẩn cho tầng vật lý bao gồm: Trải phổ trực tiếp tốc độ cao (HR/DSSS) – chuẩn 802.11b, Ghép kênh phân chia theo tần số trực giao (OFDM) – chuẩn 802.11a và Tầng vật lý tốc độ mở rộng (ERP) – chuẩn 802.11g.

Các chuẩn 802.11	Khoảng cách hoạt động (m)	Công nghệ tầng vật lý	Tốc độ truyền (Mbps)	Dải tần ISM (GHz)	Dải tần UNII (GHz)
802.11	50-100	DSSS, FHSS, Diffuse IR	1, 2	2,4 – 2,48	
802.11a	50-100	ODFM	6,9,12,18,24,36,48,54		5,15-5,25 5,25-5,35 5,72-5.87
802.11b	50-100	DSSS	1,2,5.5,11	2,4 – 2,48	
802.11g	50-100	DSSS, ODFM	6,9,12,18,24,36,48,54	2,4 – 2,48	

Hình 1-3. Đặc điểm chính của các chuẩn 802.11

1.2.1.1. Công nghệ Trải phổ nhảy tần

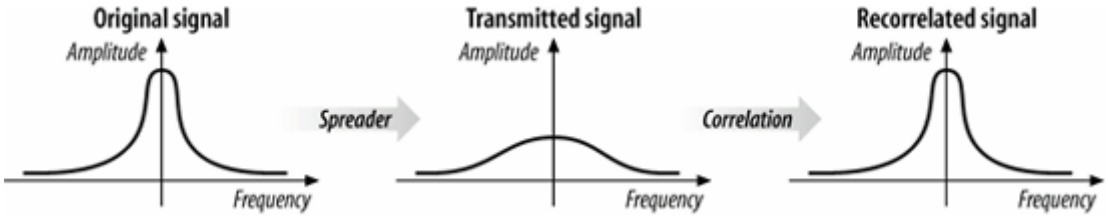
Công nghệ trải phổ nhảy tần (FHSS) cũng giống như tên gọi của nó, thực hiện việc thay đổi ("nhảy") tần số với mẫu nhảy (hopping pattern) xác định theo tốc độ được thiết đặt. FHSS phân chia dải tần số từ 2402 đến 2480 MHz thành 79 kênh không chồng lên nhau, mỗi kênh có độ rộng 1MHz. Số kênh cũng như mẫu nhảy được quy định khác nhau ở một số nước, thông thường là 79 kênh (áp dụng ở Mỹ và nhiều nước châu Âu) [1]. Một bộ tạo số giả ngẫu nhiên được sử dụng để sinh chuỗi tần số muốn "nhảy tới". Miễn là tất cả các trạm đều sử dụng cùng một bộ tạo số giả ngẫu nhiên giống nhau, và được đồng bộ hóa tại cùng một thời điểm, tần số được "nhảy" tới của tất cả các trạm sẽ giống nhau. Mỗi tần số được sử dụng trong một khoảng thời gian gọi là "dwell time". Đây là một tham số có thể điều chỉnh nhưng thường nhỏ hơn 400 ms. Việc sinh ngẫu nhiên chuỗi tần số của FHSS cung cấp một cách để định vị phổ trong dải tần ISM. Nó cũng cung cấp một cách để đảm bảo an ninh dù ít ỏi vì nếu kẻ tấn công không biết được chuỗi bước nhảy hoặc dwell time thì sẽ không thể nghe lén được đường truyền. Đối với khoảng cách xa, có thể có vấn đề giảm âm thì FHSS là một lựa chọn tốt để chống lại điều đó. FHSS cũng giảm giao thoa sóng, do đó phổ biến khi dùng cho liên kết giữa các tòa nhà. Nhược điểm của nó là dải thông thấp, chỉ đạt từ 1 đến 2 Mbps.



Hình 1-4. Trải phổ nhảy tần với mẫu nhảy {2,4,6,8}

1.2.1.2. Công nghệ Trải phổ trực tiếp và Trải phổ trực tiếp tốc độ cao

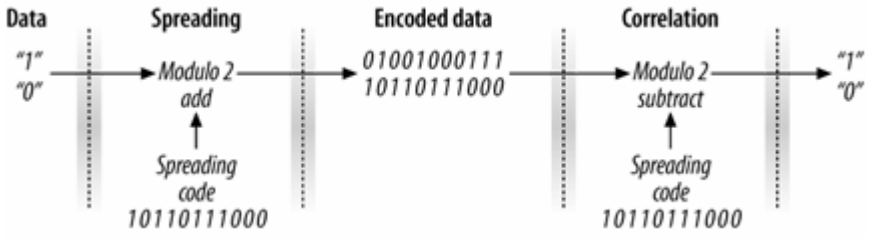
Trải phổ trực tiếp (DSSS) là một công nghệ cho phép truyền tín hiệu trên một dải tần số rộng hơn. Dữ liệu được truyền qua các kênh có độ rộng 30MHz với giới hạn chỉ cho phép 3 kênh không chồng nhau trong dải tần 2.4GHz. Khi mới ra đời, công nghệ này chỉ hỗ trợ tốc độ 1-2 Mbps giống như FHSS. Tuy nhiên, đến năm 1999, công nghệ này đã được cải tiến với tốc độ tăng lên 5,5-11Mbps (cái tên tốc độ cao – High Rate - được sử dụng để phân biệt với công nghệ đầu tiên) và được sử dụng trong chuẩn 802.11b. Cơ chế làm việc cơ bản của công nghệ DSSS là trải (spreader) năng lượng tín hiệu lên một dải tần rộng hơn để truyền tải tốt hơn, sau đó bên nhận sẽ thực hiện các xử lý tương quan (correlation processes) để thu được tín hiệu ban đầu.



Hình 1-5. Kỹ thuật DSSS cơ bản

Việc biến điệu trực tiếp được thực hiện bằng cách đưa chuỗi chipping vào dòng dữ liệu. Cụ thể là: bit dữ liệu ban đầu được XOR với "chipping code" (hay còn gọi là hệ số trải phổ). Kết quả, bit dữ liệu ban đầu được phân thành nhiều "bit con" (được gọi là các "chip") – như hình vẽ bên dưới. Mỗi chip được biểu diễn bởi 1 hoặc 0. Tất cả các chip này sau đó được truyền đi qua dải tần số lớn hơn rất nhiều so với dải tần số của luồng dữ liệu gốc. Phía nhận (với cùng mã "chipping code" như vậy), khi nhận được chuỗi chip, thực hiện giải mã để lấy ra dữ liệu ban đầu: nếu chuỗi mã hóa giống chuỗi chipping thì bit đó có giá trị 1, ngược lại có giá trị 0. Quá

trình chipping sử dụng chuỗi chipping có độ dài 11bit được biểu diễn như sau:



Hình 1-6. Quá trình chipping

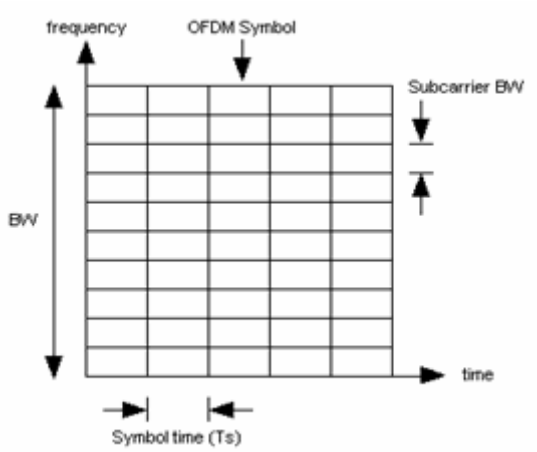
Trong DSSS, số chip được sử dụng để truyền 1 bit được gọi là hệ số trải phổ (trong hình 1-6, hệ số trải phổ là 11). Hệ số trải phổ lớn sẽ đảm bảo khả năng thu được dữ liệu gốc nhưng đòi hỏi dải tần lớn và chuỗi chipping lớn hơn. Có thể coi quá trình "chipping" là một dạng mã hóa nhằm tăng tính an toàn của dữ liệu trên đường truyền. Một kẻ nghe lén phải tìm ra được dải tần được sử dụng để truyền tin và mã "chipping code" mới có thể lấy ra được thông tin thực.

1.2.1.3. Công nghệ Ghép kênh phân chia theo tần số trực giao

Dải tần 2.4GHz (còn được gọi là dải tần ISM), được đưa ra nhằm mục đích phục vụ cho công nghiệp, khoa học và y tế. Do vậy các mạng không dây hoạt động ở dải tần này dễ bị nhiễu từ các thiết bị không phải thành phần 802.11, nghĩa là thông lượng mạng sẽ bị hạn chế. Từ nguyên do đó, nhóm chuẩn hóa 802.11 với mong muốn nâng cao tốc độ dữ liệu đã ra đưa chuẩn tầng vật lý sử dụng dải tần không cấp phép 5GHz (chuẩn 802.11a). Chuẩn 802.11a hoạt động dựa trên công nghệ Ghép kênh phân chia theo tần số trực giao (OFDM).

Ý tưởng chính trong công nghệ OFDM là việc chia lượng dữ liệu trước khi phát đi thành N luồng dữ liệu song song có tốc độ thấp hơn và phát mỗi luồng dữ liệu đó trên một sóng mang con khác nhau. Các sóng mang này là trực giao với nhau, điều này được thực hiện bằng cách chọn độ dãn cách tần số giữa chúng một cách hợp lý. Trực giao có nghĩa là tần số trung tâm của một sóng mang con nhất định sẽ rơi đúng vào các điểm bằng 0 của các sóng mang con khác. OFDM tạo ra lưới theo thời gian và tần số. Mỗi hình chữ nhật là một kênh độc lập và có thể cấp cho những người sử dụng khác nhau. Sử dụng các tần số trực giao sẽ tránh được sự ảnh hưởng lẫn nhau giữa các sóng mang con khác nhau khi sắp xếp vị trí các sóng

mang với mật độ lớn trong miền tần số do đó sẽ đạt được hiệu quả quang phổ cao. [4]



Hình 1-7. Kỹ thuật OFDM

Trong chuẩn 802.11a, dải tần hoạt động được chia thành 8 các kênh con không chồng nhau, mỗi kênh có có độ rộng 20MHz. Mỗi kênh con chứa 52 sóng mang con, trong đó 48 sóng mang được sử dụng để truyền dữ liệu. Dữ liệu được truyền đi được chứa trong các sóng mang con. Các kênh sau đó được sử dụng để truyền dữ liệu một cách đồng thời. Do đặc tính trực giao, thông lượng truyền dữ liệu tổng hợp của tất cả các kênh tăng lên (các sóng trực giao không ảnh hưởng lên nhau), thông lượng lý thuyết của chuẩn 802.11a đạt tới 54Mbps.

1.2.1.4. Công nghệ Tầng vật lý tốc độ mở rộng

Khi được ứng dụng vào thực tế, chuẩn 802.11b tỏ ra vượt trội hơn 802.11a bởi giá thành rẻ, công nghệ dễ áp dụng vào việc sản xuất phần cứng. Tuy nhiên, thông lượng đạt được của chuẩn 802.11a khiến việc nghiên cứu mở rộng 802.11b tiếp tục được mở rộng. Và chuẩn 802.11g đã ra đời, cho phép có được thông lượng lên tới 54Mbps, đồng thời có khả năng tương thích ngược với các thiết bị 802.11b đang được sử dụng rất phổ biến.

Thực chất, 802.11g không sử dụng công nghệ tầng vật lý nào mới. Các đặc tả tầng vật lý của 802.11g được dựa trên các công nghệ đã có sẵn DSSS, OFDM với các sửa đổi cần thiết và được đặt tên là Tầng vật lý Tốc độ mở rộng (ERP) để phân biệt với các công nghệ gốc. Các đặc tả ERP trong 802.11g có thể kể đến bao gồm:

- *ERP-DSSS* và *ERP-CCK*: được đặc tả để hỗ trợ tương thức ngược với chuẩn

802.11b, hỗ trợ tốc độ 11Mbps.

- *ERP-OFDM*: đây là chế độ hoạt động chính của 802.11g. Ở đặc tả này, tầng vật lý sử dụng công nghệ OFDM trên dải tần 2.4GHz. Nó cũng cung cấp thông lượng giống như chuẩn 802.11a: 6, 9, 12, 18, 24, 36, 48, 54Mbps.
- *DSSS-OFDM*: là cơ chế lai, thực hiện việc mã hóa gói tin sử dụng đoạn mào đầu (header) của DSSS và sử dụng OFDM để mã hóa dữ liệu cần gửi đi. Nguyên do là để đảm bảo tính tương thích ngược. Mặc dù, phần thân được mã hóa bởi OFDM và không sử dụng được cho 802.11b nhưng thông tin trong phần mào đầu có thể cung cấp thông tin trong quá trình truyền tải và xử lý gói tin. Là cơ chế tùy chọn, không bắt buộc áp dụng, DSSS-OFDM không được triển khai rộng rãi.

Bằng việc sử dụng dải tần nhỏ xấp xỉ 2 lần so với 802.11a, các thiết bị 802.11g cho phép phạm vị phủ sóng rộng hơn mà vẫn đảm bảo tốc độ ngang ngửa với 802.11a.

1.2.1.5. Công nghệ sóng hồng ngoại

Chuẩn 802.11 ban đầu cũng đặc tả sóng hồng ngoại (IR) 900nm như một môi trường vật lý riêng rẽ phục vụ mục đích truyền dẫn thông tin. Dữ liệu được truyền đi với tốc độ 1-2 Mbps sử dụng kỹ thuật biến điệu vị trí 16 xung (PPM) – có nghĩa là 4 bit dữ liệu được mã hóa thành 16 bit trước khi truyền. Lợi điểm của tầng vật lý loại này là nó làm việc tốt trong môi trường có nhiễu, khi các thiết bị không dây (máy vi sóng, thiết bị y tế, …) phát ra cùng tần số radio. Tuy nhiên, phạm vi hoạt động giới hạn từ 10-20 mét cộng với yêu cầu đường kết nối không bị ngăn cản (sóng hồng ngoại truyền theo đường thẳng và dễ bị cản bởi các chướng ngại vật) đã khiến cho công nghệ này không được áp dụng rộng rãi trong công nghiệp và thương mại.

1.2.2. Tầng con MAC

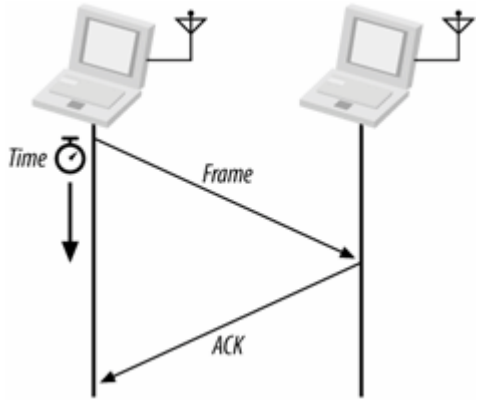
Trong đặc tả chuẩn 802.11, tầng con MAC đóng vai trò then chốt bởi nó thực hiện việc điều khiển việc truyền dữ liệu người dùng và tương tác với mạng hữu tuyến. Là một thành phần của họ chuẩn 802, đặc tả cho tầng MAC trong chuẩn

802.11 không tách biệt một cách rõ rệt. Tầng MAC trong chuẩn 802.11 cũng sử dụng cơ chế đa truy cập có phát hiện sóng mang (CSMA) giống như chuẩn Ethernet. Cũng như vậy, 802.11 sử dụng mô hình truy cập phân tán, không có điểm quản lý tập trung. Có nghĩa là các trạm sử dụng cùng một cách thức để truy cập vào môi trường truyền dẫn. Tuy nhiên, do sự phức tạp của môi trường không dây, tầng MAC trong chuẩn 802.11 có những đặc thù cần lưu ý.

Truyền dẫn sóng điện từ trong môi trường không khí, đặc biệt khi dải tần số sử dụng thuộc dải ISM, các thiết bị 802.11 cần phải chấp nhận được nhiễu gây ra từ các thiết bị khác (các thiết bị cùng loại hay khác loại) và làm việc được. Do đó, 802.11 sử dụng giao thức trao đổi khung tin (FEP – Frame Exchange Protocol) để điều khiển việc truyền khung tin nhằm loại bỏ các vấn đề có thể xảy ra khi truyền dữ liệu trong môi trường truyền dẫn chia sẻ và không tin cậy này.

1.2.2.1. Biên nhận khung tin

FEP được triển khai đồng thời ở các trạm và điểm truy cập để đảm bảo tính tin cậy cho quá trình truyền dẫn. Theo đó, mọi khung tin được gửi đi đều phải được biên nhận bởi phía nhận trong một khoảng thời gian hệ thống gọi là NAV (Network Allocation Vector).



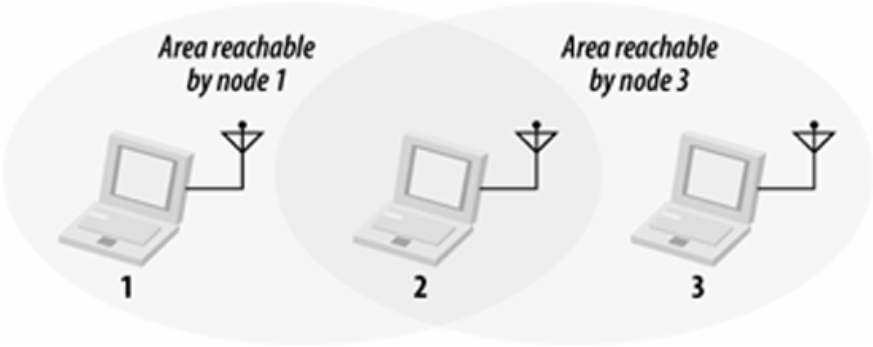
Hình 1-8. Biên nhận tích cực trong quá trình truyền dữ liệu

Chuỗi hành động được mô tả trong hình 1-8 được gọi là một thao tác nguyên tử. Mặc dù trong thao tác nguyên tử còn có thêm nhiều bước khác, nó vẫn được coi là một thao tác không thể phân chia. Điều đó có nghĩa là mọi bước trong thao tác nguyên tử phải được hoàn thành, nếu không thao tác sẽ bị coi là thất bại hay khung tin được coi là gửi đi bị lỗi.

1.2.2.2. Các hàm điều phối (Coordination Functions)

a. Vấn đề trạm ẩn (hidden station)

Trong chuẩn 802.11, các nút chỉ có thể truyền thông được với nhau nếu chúng nằm trong vùng phủ sóng của nhau. Các nút nằm ngoài vùng phủ sóng được coi là không nhìn thấy được (invisible). Vấn đề trạm ẩn xảy ra khi hai nút ở bên ngoài phạm vi hoạt động của nhau (nút 1 và nút 3) truyền dữ liệu tại cùng một thời điểm tới một nút thứ ba (ở trong phạm vi hoạt động của hai nút kia - ở đây là nút 2). Do hai nút này ở ngoài phạm vi hoạt động của nhau nên không thể "cảm nhận" được tình huống này. Xung đột sẽ xảy ra tại nút 2 (hình 1-9).



Hình 1-9. Vấn đề trạm ẩn

Tác động của vấn đề trạm ẩn là cả nút 1 hoặc nút 3 không thể dò tìm được xung đột do chúng ở ngoài phạm vi hoạt động của nhau. Việc thiếu ACK cho mỗi khung tin sẽ làm cho hai nút giả thiết rằng khung tin bị mất vì một vài lý do nào đó. Kết quả là cả hai sẽ truyền lại khung tin của chúng cho tới khi thành công.

FEP cũng được sử dụng để giải quyết vấn đề trạm ẩn hay là xung đột khung tin. Để giải quyết vấn đề này, FEP cung cấp hai hàm điều phối:

- *DCF* (hàm điều phối phân tán) – không sử dụng bất cứ điều khiển tập trung nào (ở khía cạnh này, cách giải quyết tương tự như Ethernet)
- *PCF* (hàm điều phối điểm) – sử dụng một trạm cơ sở để điều khiển tất cả các hoạt động trong tế bào (cell) của nó.

Tất cả các cài đặt đều yêu cầu phải hỗ trợ DCF nhưng PCF là tùy chọn.

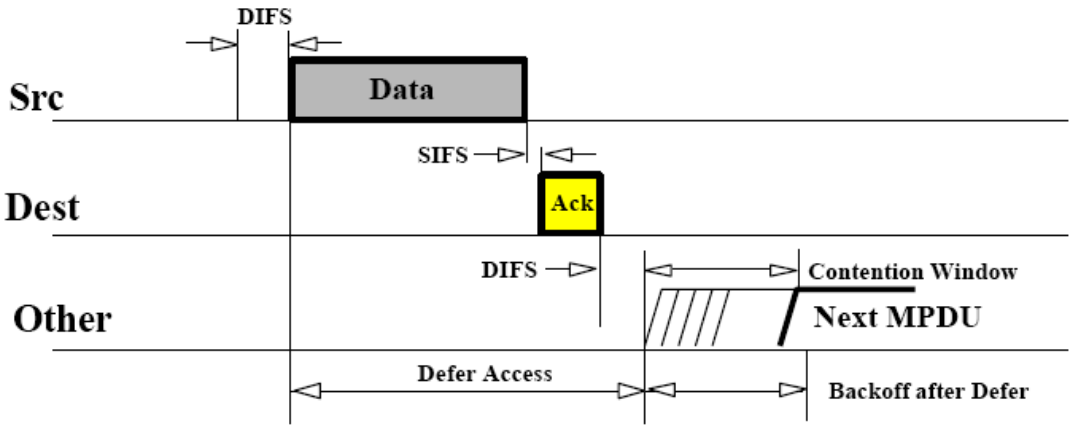
b. Hàm điều phối phân tán (DCF)

Hàm điều phối phân tán (DCF – Distributed Co-ordination Function) về cơ bản là cơ chế đa truy cập cảm nhận sóng mang tránh xung đột hay còn gọi là

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Giao thức CSMA làm việc như sau: Khi một trạm muốn truyền tin, trạm phải cảm nhận kênh truyền. Nếu kênh truyền là bận (ví dụ có một trạm khác đang truyền tin), trạm sẽ chờ trong một khoảng thời gian. Sau đó nếu kênh truyền được cảm nhận là rỗi, khi đó trạm được phép truyền tin. Những giao thức như vậy là hiệu quả khi kênh truyền không phải tải lưu lượng quá lớn. Tuy nhiên xung đột luôn có thể xảy ra vì các trạm đều cùng cảm nhận kênh truyền là rỗi và quyết định truyền tin tại cùng một thời điểm. Chính vì vậy trong Ethernet đã sử dụng CSMA kết hợp với việc dò tìm xung đột (Collision Detection - CD). Dò tìm xung đột là một ý tưởng tốt đối với mạng LAN hữu tuyến, tuy nhiên không thể sử dụng kỹ thuật này trong môi trường không dây do hai lý do chính sau:

- Triển khai kỹ thuật dò tìm xung đột đòi hỏi sóng vô tuyến phải có khả năng truyền song công (full duplex) – nhận và truyền tin tại cùng một thời điểm. Điều này làm cho giá thành sản phẩm tăng;
- Trong môi trường không dây, không thể giả thiết rằng tất cả các trạm đều nghe thấy nhau – đây là giả thiết cơ bản trong chiến lược dò tìm xung đột. Ngoài ra khi một trạm muốn truyền tin và cảm nhận kênh truyền là rỗi, điều đó không có nghĩa là kênh truyền là rỗi xung quanh khu vực của trạm nhận tin.

Để khắc phục những vấn đề này, chuẩn 802.11 sử dụng kỹ thuật tránh xung đột (Collision Avoidance - CA) cùng với chiến lược biên nhận tích cực (Phần 1.2.2.1) như sau (hình 1-10): Trạm muốn truyền tin cảm nhận kênh truyền. Nếu kênh truyền được cảm nhận là bận, nó sẽ chờ. Nếu kênh truyền là rỗi trong một khoảng thời gian xác định (được gọi là DIFS – Distributed Inter Frame Space), trạm được phép truyền tin. Bên nhận khi nhận được khung tin sẽ thực hiện thuật toán CRC để dò tìm lỗi, sau đó đợi trong một khoảng thời gian được gọi là SIFS (Short InterFrame Space) (SIFS < DIFS) và gửi khung tin biên nhận (ACK). ACK sẽ không được gửi đi nếu khung tin do trạm nguồn gửi bị lỗi hoặc bị mất trên đường truyền. Nếu bên gửi không nhận được ACK, nó sẽ giả thiết có xung đột (hoặc khung tin gửi đi bị lỗi) và lập kế hoạch truyền lại.



Hình 1-10. Cơ chế CSMA/CA

Khi bên nhận giả thiết khung tin bị lỗi (hoặc có xung đột), nó sẽ chờ thêm một khoảng thời gian là EIFS (Extended InterFrame Space). Nếu không nhận được khung tin ACK sau khoảng thời gian này, bên gửi sẽ tiếp tục truyền lại khung tin đã gửi trước đó cho tới khi thành công hoặc tới khi các tầng trên hủy nó.

Để làm giảm xác suất xung đột, 802.11 sử dụng kỹ thuật back-off: Khi trạm S muốn truyền tin đi cảm nhận thấy kênh truyền đang bận, nó sẽ chờ cho đến khi kết thúc khoảng thời gian DIFS. Tại thời điểm kết thúc DIFS, trạm S khởi tạo một bộ đếm (gọi là back-off timer) bằng cách chọn một khoảng thời gian ngẫu nhiên (back-off interval) để lập lịch cho việc truyền tin của nó. Bộ đếm sẽ giảm trong thời gian kênh truyền được cảm nhận là rỗi, dừng lại khi có phát hiện thấy kênh truyền đang truyền tin và được kích hoạt lại khi kênh truyền được cảm nhận là rỗi trong một khoảng thời gian lớn hơn DIFS. Khi bộ đếm bằng 0, trạm được phép truyền tin. Ở đây DCF sử dụng kỹ thuật back-off hàm mũ hai theo khe thời gian. Thời gian theo sau DIFS được gọi là cửa sổ back-off (Back-off Window/Contention Window). Cửa sổ này được phân chia thành khe thời gian (Slot Time[1]), độ dài mỗi khe tùy thuộc vào tầng vật lý – tầng vật lý tốc độ cao sử dụng các khe thời gian ngắn hơn. Các trạm sẽ chọn lấy một khe bất kỳ, và chờ đến thời điểm bắt đầu khe đó để truyền tin. Tại thời điểm thử truyền tin lần đầu tiên, $CW = CW_{min}$. Giá trị CW được tăng lên sau mỗi lần thử truyền tin lại ($CW_i = 2^{k+i-1} - 1$, trong đó i là số lần thử truyền tin – tính cả lần đang xét, k là hằng số xác định giá trị CW_{min}), tới giá trị tối đa là CW_{max}.

[1] Một khe thời gian tương đương với thời gian cần thiết để bất kỳ trạm nào cũng dò tìm được việc truyền tin của bất cứ trạm nào khác.

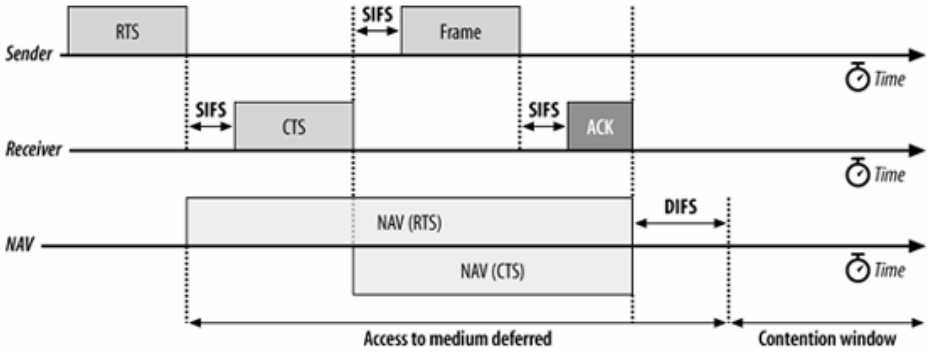
Giá trị cụ thể của CW_{min} và CW_{max} phụ thuộc vào từng kiểu tầng vật lý, ví dụ nếu tầng vật lý là FHSS thì CW_{min} = 16 khe và CW_{max} = 1024 khe. Khi cửa sổ back-off đạt tới giá trị tối đa, nó sẽ giữ nguyên và sẽ được đưa về giá trị tối thiểu CW_{min} khi khung tin được truyền thành công hoặc bị hủy bởi tầng trên.

Việc cảm nhận kênh truyền như trên là cảm nhận vật lý kênh truyền (physical carrier sense), chức năng cảm nhận do tầng vật lý cung cấp. Tuy nhiên, trong nhiều trường hợp cảm nhận vật lý kênh truyền không cung cấp đủ các thông tin cần thiết, ví dụ như vấn đề trạm ẩn. Do đó, trong chuẩn 802.11 còn hỗ trợ một chiến lược cảm nhận sống mang ảo được cung cấp bởi NAV (Network Allocation Vector).

Phần lớn các khung tin 802.11 có một trường "duration", được dùng để để dành kênh truyền trong một khoảng thời gian cố định. NAV là một bộ định thời (timer) cho biết kênh truyền được để dành trong thời gian bao lâu. Các trạm thiết lập giá trị NAV bằng thời gian chúng muốn sử dụng kênh truyền – là khoảng thời gian cần để truyền đi tất cả các frame cần thiết để hoàn thành hành động hiện tại. Các trạm khác sẽ thực hiện đếm ngược từ giá trị NAV tới 0. Khi NAV khác 0, chức năng cảm nhận sóng mang ảo cho biết kênh truyền là bận, khi NAV được giảm tới 0, chức năng cảm nhận sóng mang ảo cho biết kênh truyền là rỗi.

Với NAV, cơ chế cảm nhận sóng mang ảo (hay còn gọi là RTS/CTS) được thực hiện như sau:

Sau khi giành được quyền truy cập kênh truyền, trước khi bắt đầu truyền tin, trạm phải gửi đi một khung tin yêu cầu gửi RTS (Request To Send) tới trạm nhận để thông báo về việc truyền tin sắp tới. Phía nhận sẽ trả lời lại khung tin RTS bằng khung tin CTS (clear to send) để cho biết đã sẵn sàng nhận tin. Cả RTS và CTS đều chứa độ dài dự kiến của việc truyền tin (thời gian truyền khung tin và ACK). Tất cả các trạm khi nhận được RTS hoặc CTS sẽ thiết lập chỉ số cảm nhận sóng mang ảo của nó hay còn gọi là NAV bằng khoảng thời gian dự kiến truyền tin. Thông tin này sẽ được sử dụng cùng với cảm nhận vật lý kênh truyền khi cảm nhận kênh truyền.



Hình 1-11. CSMA/CA với cảm nhận sóng mang ảo.

Cơ chế này giải quyết được vấn đề trạm ẩn vì tất cả các trạm ở trong phạm vi hoạt động của trạm gửi hoặc trạm nhận đều biết được kênh truyền sẽ được sử dụng cho việc truyền tin hiện tại trong bao lâu, đảm bảo được rằng không một nút nào có thể làm dừng quá trình truyền tin cho đến khi nút nhận đã gửi ACK cho nút gửi. Tuy nhiên, do sử dụng RTS và CTS nên tổng phí truyền tin tăng, xuất hiện dưới dạng độ trễ trước khi dữ liệu thực được truyền đi. Vì vậy truyền đi một gói dữ liệu lớn có lợi hơn là gửi nhiều gói dữ liệu nhỏ. Chuẩn IEEE 802.11còn định nghĩa một tham số gọi là ngưỡng RTS cho phép các khung tin nhỏ được truyền đi không cần quá trình trao đổi RTS/CTS.

c. Hàm điều phối điểm (Point Co-ordination Function)

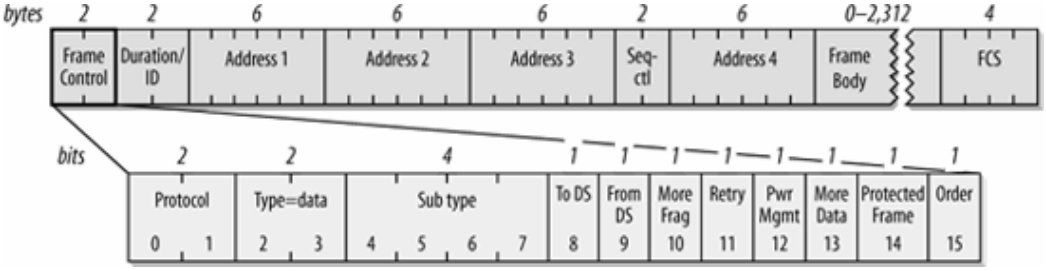
PCF là một chiến lược tùy chọn hỗ trợ cho quá trình DCF. Nó cung cấp một cơ chế cảm nhận sóng mang ảo thông qua chức năng bỏ phiếu (poll) và đáp trả (response) của FEP. PCF sử dụng PIFS (Priority Interframe Space) để gán cho điểm truy cập quyền điều khiển môi trường truyền dẫn thay vì các trạm sử dụng DIFS để xác định quyền truy cập môi trường. Các trạm tham gia được phép gửi một khung tin đáp trả cho khung tin poll của điểm truy cập nhằm mục đích cập nhật giá trị NAV của chúng. Để có thể cung cấp dịch vụ cho các trạm tham gia không sử dụng PCF, điểm truy cập thay thế PIFS bằng DIFS.

Như vậy, trong chiến lược PCF cần phải có một điểm truy cập đóng vai trò như một trạm điều phối BSS/ESS. Điều này có nghĩa là không thể sử dụng chiến lược này khi các nút mạng hoạt động ở chế độ ad-hoc (IBSS).

1.2.2.3. Cấu trúc khung tin

Các khung tin tầng MAC được sử dụng trong quá trình truyền tin bao gồm:

khung tin quản lý (management frame), khung tin điều khiển (control frame) và khung tin dữ liệu. Các khung tin này có cùng một trường gọi là trường điều khiển khung tin (Frame control field) có độ dài 16 bit được mô tả trong hình vẽ bên dưới.

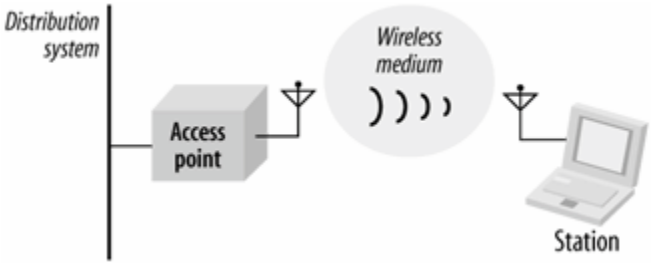


Hình 1-12. Trường điều khiển khung tin

1.2.3. Kiến trúc mạng

1.2.3.1. Các thành phần của mạng

Mạng WLAN 802.11 bao gồm bốn thành phần vật lý chính được mô tả trong hình 1-13 bên dưới [1]:



Hình 1-13. Các thành phần của mạng WLAN 802.11

a. Các trạm (Stations)

Mạng không dây được xây dựng để truyền thông tin giữa các trạm. Các trạm thực chất là các thiết bị điện toán có gắn giao diện mạng không dây. Các trạm này có thể là cố định hoặc di động.

b. Điểm truy cập (Access Point)

Điểm truy cập thực chất là một thiết bị phần cứng cố định thực hiện chức năng cầu nối giữa mạng không dây và có dây (hữu tuyến), thực hiện việc chuyển tiếp gói tin cho các trạm không dây. Vùng phủ sóng của điểm truy cập cho phép các trạm tham gia trao đổi thông tin.

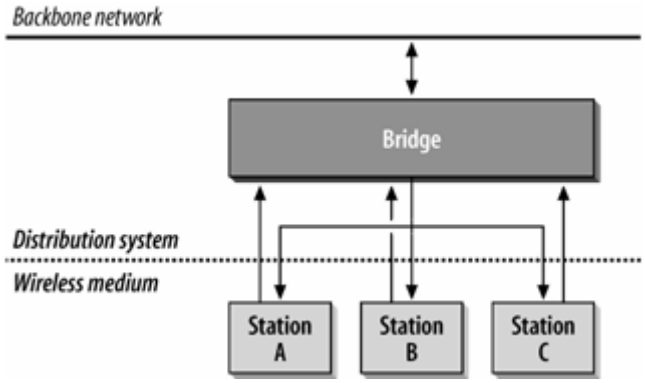
c. Phương tiện truyền dẫn không dây (Wireless Medium)

Để truyền thông tin giữa các trạm với nhau, chuẩn 802.11 quy định sử dụng

phương tiện truyền dẫn không dây. Như ở trên đã trình bày, chuẩn 802.11 quy định bốn công nghệ tầng vật lý chính làm phương tiện truyền dẫn không dây.

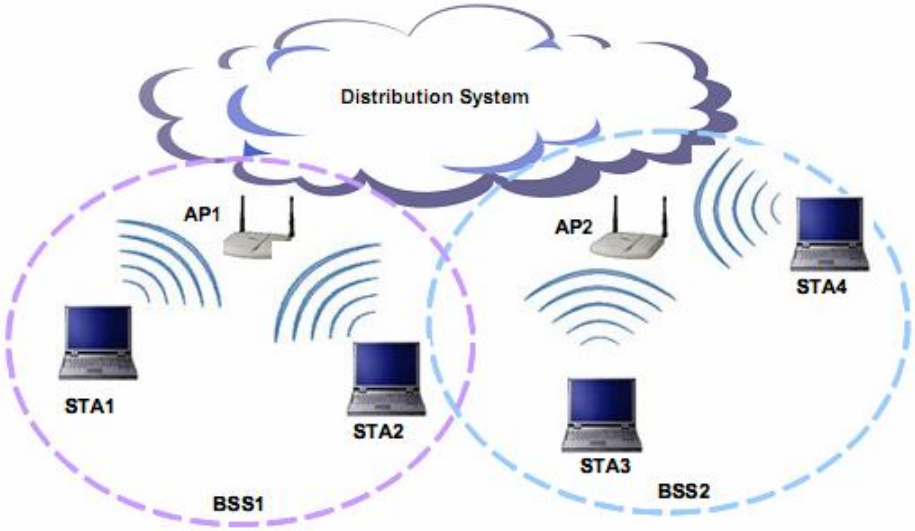
d. Hệ thống phân phối (Distribution System)

Khi nhiều điểm truy cập được kết nối với nhau để tạo ra vùng phủ sóng rộng hơn, chúng cần liên lạc với nhau để theo dõi sự di chuyển của các trạm di động. Hệ thống phân phối là thành phần logic của chuẩn 802.11 được sử dụng để truyền các khung tin tới đúng đích. Chuẩn 802.11 không quy định một công nghệ cụ thể nào cho hệ thống phân phối. Tuy nhiên, trong phần lớn các thiết bị thương mại, hệ thống phân phối là sự kết hợp giữa một thiết bị cầu nối (brigde) và mạng đường trục (mạng hữu tuyến) để chuyển tiếp các khung tin giữa các điểm truy cập.



Hình 1-14. Mô hình logic hệ thống phân phối được sử dụng phổ biến

Mạng WLAN 802.11 theo kiến trúc cơ sở hạ tầng mạng (infrastructure mode) bao gồm hai kiến trúc con: Tập dịch vụ cơ bản (BSS-Basic Service Set), và Tập dịch vụ mở rộng (ESS-Extended Service Set) .



Hình 1-15. Các kiến trúc mạng của chuẩn 802.11

1.2.3.2. Kiến trúc Tập dịch vụ cơ bản (BSS)

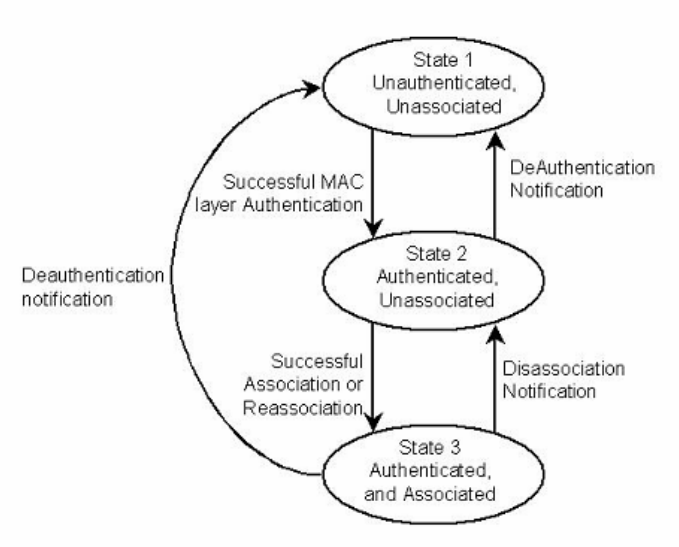
Mỗi tập dịch vụ cơ bản được cấu thành từ tổ hợp của một điểm truy cập (có thể kết nối vào mạng hữu tuyến hoặc không) và các trạm không dây. Mọi trạm tham gia vào kiến trúc này sẽ không truyền thông trực tiếp với nhau mà truyền thông qua thiết bị trung gian là điểm truy cập. Điểm truy cập là không di động và là một phần của cơ sở hạ tầng mạng hữu tuyến.

1.2.3.3. Kiến trúc Tập dịch vụ mở rộng (ESS)

Cung cấp hạ tầng mạng cho nhiều tập dịch vụ cơ bản. Kiến trúc này được cài đặt bằng cách kết hợp nhiều điểm truy cập (có cùng một kênh truyền) có các vùng phủ sóng chồng lên nhau. Dịch vụ phân phối trong một điểm truy cập đảm nhiệm việc chuyển tiếp các khung tin dữ liệu từ các trạm không dây liên kết với điểm truy cập khác tới các trạm trong tập dịch vụ cơ bản của nó. Nhờ đó, tập dịch vụ mở rộng xuất hiện như là một mạng con cố định đối với các thực thể bên ngoài mạng. Thêm vào đó, tập dịch vụ mở rộng cho phép các trạm di động có thể di chuyển một cách tự do (chế độ roaming trong suốt) trong vùng phủ sóng tổng hợp của tập này.

1.2.4. Quá trình kết nối

Quá trình thiết lập kết nối giữa các trạm và điểm truy cập trong đặc tả 802.11 ban đầu bao gồm bốn pha theo thứ tự thực hiện là Dò tìm (Scanning), Đồng bộ hóa (Synchronization), Xác thực (Authentication), và Liên kết (Association) tương ứng với ba trạng thái kết nối (như hình vẽ bên dưới). Các trạng thái kết nối xác định mối quan hệ giữa các trạm và điểm truy cập. Quá trình được thực hiện một cách tuần tự khi các trạm chuyển từ trạng thái này sang trạng thái kế tiếp:



Hình 1-16. Các trạng thái kết nối

1.2.4.1. Trạng thái 1: Chưa xác thực và liên kết

Bắt đầu từ trạng thái kết nối chưa xác thực (unauthenticated) và chưa liên kết (unassociated), các trạm thực hiện hai bước để thiết lập mối quan hệ khách (client) với điểm truy cập: Dò tìm và Đồng bộ hóa.

Pha 1. Dò tìm

Dò tìm là một quá trình mà một trạm thực hiện việc tìm kiếm các trạm khác hoặc điểm truy cập để thiết lập kết nối. Quá trình này có thể được thực hiện theo hai cách:

- *Chủ động*: Trạm muốn kết nối tự gửi khung tin dò tìm để thu được khung tin phản hồi từ các trạm khác hoặc điểm truy cập.
- *Thụ động*: Trạm muốn kết nối chỉ đơn thuần lắng nghe các khung tin hướng dẫn (beacon management frame) được phát quảng bá từ các điểm truy cập. Các khung tin này chứa thông tin về điểm truy cập, SSID (Service Set ID – ID tập dịch vụ) và các tốc độ dữ liệu cho phép. Các trạm (thực chất là card mạng không dây) sẽ sử dụng các thông tin này cùng với cường độ tín hiệu (signal strength) để thiết lập kết nối từ các trạm vào điểm truy cập đó.

Pha 2. Đồng bộ hóa

Quá trình đồng bộ hóa được hoàn thành bởi các khung tin hướng dẫn thực hiện việc thiết lập và cập nhật các thông số mạng chung nhằm giảm thiểu việc xung

đột các khung tin. Chức năng này được thực hiện bởi điểm truy cập. Sau khi hoàn thành bước đồng bộ hóa, các trạm chuyển sang bước xác thực.

1.2.4.2. Trạng thái 2: Xác thực

Xác thực là quá trình một trạm hoặc một điểm truy cập chấp thuận nhận dạng (identity) của một trạm khác. Trong kết nối không dây có sử dụng phương pháp mã hóa WEP, quá trình xác thực được thực hiện thông qua việc trao đổi các gói tin thách (challenge) và trả lời (response). Nếu quá trình kết nối sử dụng phương pháp xác thực mở (open authencation), điểm truy cập chỉ đơn thuần gửi khung tin chấp nhận cho bất cứ khung tin yêu cầu xác thực nào từ các trạm.

1.2.4.3. Trạng thái 3: Liên kết

Liên kết là trạng thái kết nối cuối cùng trong quá trình kết nối giữa trạm và điểm truy cập. Trạm sẽ khởi tạo pha liên kết bằng cách gửi gói tin yêu cầu liên kết có chứa các thông tin như SSID, tốc độ dữ liệu mong muốn. Điểm truy cập trả lời bằng cách gửi một khung tin trả lời có chứa mã liên kết (asscociation ID) cùng với cac thông tin về điểm truy cập đó. Sau khi quá trình liên kết thành công, trạm và điểm truy cập có thể trao đổi các khung tin dữ liệu cho nhau.

Mặc dù một trạm có thể đồng thời được xác thực ở nhiều điểm truy cập khác nhau, nó chỉ có thể liên kết với một điểm truy cập duy nhất tại một thời điểm. Quy tắc này nhằm ngăn chặn sự nhập nhằng trong việc xác định điểm truy cập nào cung cấp dịch vụ cho trạm trong kiến trúc tập dịch vụ mở rộng (ESS).

Như hình 1-16 chỉ ra, việc sử dụng các khung tin hủy xác thực (deauthentication) và hủy liên kết (deassociation) cho phép một điểm truy cập thay đổi trạng thái kết nối của một hay nhiều trạm. Nhờ đó, các điểm truy cập có thể chuyển tiếp dữ liệu cũng như chuyển dịch vụ sang các điểm truy cập khác trong kiến trúc ESS.

1.3. Tổng kết

Nội dung chương này đã trình bày các kiến thức tổng quan về mạng không dây và đặc biệt là mạng WLAN sử dụng chuẩn IEEE 802.11. Tính đến nay, sau gần 10 năm kể từ khi ra đời, việc áp dụng mạng WLAN 802.11 rộng rãi trong nhiều lĩnh

vực đã chứng tỏ được tính ưu việt và hiệu quả của nó. Cũng giống như mọi công nghệ mạng khác, vấn đề an ninh trong WLAN 802.11 cũng được đặt ra và đặc biệt trong hoàn cảnh được sử dụng rộng rãi như hiện nay thì vấn đề an ninh cho WLAN 802.11 trở nên một vấn đề nóng hổi trong lĩnh vực điện toán. Do đó, nội dung chương tiếp theo sẽ đi giới thiệu các giải pháp an ninh cho mạng WLAN 802.11 và nghiên cứu chi tiết phương bảo mật và đảm bảo toàn vẹn dữ liệu bên trong các giải pháp đó.

Để tiện cho việc trình bày, từ chương sau trở đi, khái niệm chuẩn 802.11 được hiểu là chuẩn IEEE 802.11, khái niệm mạng 802.11 được hiểu là mạng WLAN sử dụng chuẩn IEEE 802.11.

CHƯƠNG 2. MỘT SỐ GIẢI PHÁP AN NINH CHO MẠNG WLAN 802.11

Giống như mạng hữu tuyến truyền thống, mạng 802.11 cũng kế thừa những yêu cầu về an ninh cần có từ mạng hữu tuyến. Tuy nhiên, nếu ở mạng hữu tuyến môi trường truyền dẫn là mở có hạn chế (nghĩa là các thiết bị có thể truy cập nhưng yêu cầu phải có kết nối vật lý vào đường dây dẫn) thì ở mạng 802.11, môi trường truyền dẫn (sóng điện từ trong không khí) là hoàn toàn mở. Điều đó có nghĩa là các thiết bị không dây đều có thể truy cập không hạn chế vào môi trường này. Vì đặc điểm đó, mạng không dây cần có những phương pháp đảm bảo an ninh riêng bên cạnh những phương pháp truyền thống. Như đã trình bày, chuẩn 802.11 chỉ đặc tả cho hai tầng là: Liên kết dữ liệu và Vật lý. Do đó, các phương pháp an ninh cho chuẩn 802.11 chủ yếu được xây dựng ở tầng con MAC thuộc tầng Liên kết dữ liệu trong mô hình OSI.

Chuẩn IEEE 802.11 quy định ba mục tiêu an ninh [2] cần có cho mạng 802.11 bao gồm:

- *Tính xác thực* (authentication): nhằm đảm bảo chỉ những thiết bị được phép (đã xác thực) mới có thể truy cập vào điểm truy cập và sử dụng dịch vụ.
- *Tính bí mật* (confidentiality): tính bí mật (hay còn gọi là tính riêng tư – privacy) yêu cầu dữ liệu là không thể đọc được bởi bất cứ đối tượng nào không được phép.
- *Tính toàn vẹn* (Integrity): đảm bảo dữ liệu được giữ nguyên vẹn, không bị sửa đổi trong quá trình truyền qua mạng.

Với ba mục tiêu này, chuẩn 802.11 sử dụng ba phương pháp là xác thực, mã hóa và kiểm tra tính toàn vẹn nhằm đảm bảo tính an toàn cho môi trường mạng.

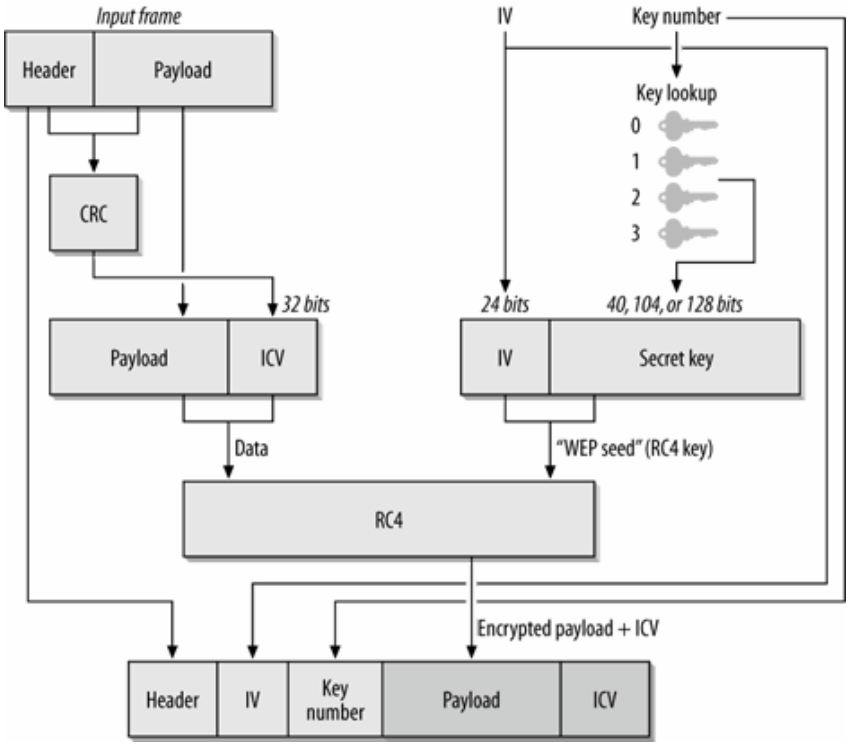
Nội dung chương này sẽ tập trung trình bày các phương pháp mã hóa được áp dụng để đảm bảo an ninh cho mạng WLAN 802.11 cũng như những hạn chế còn tồn tại của các phương pháp này.

2.1. WEP

WEP (Wired Equivalent Privacy – Tính bí mật tương đương mạng hữu tuyến) là cơ chế bảo mật đầu tiên khi chuẩn 802.11 ra đời. Thực tế ứng dụng đã cho thấy WEP có nhiều lỗ hổng an ninh cần khắc phục. Tuy nhiên, việc hiểu rõ cơ chế WEP cũng như những lỗ hổng của cơ chế này giúp ta có được cái nhìn tổng thể về những yêu cầu an ninh cần áp dụng cho mạng không dây.

2.1.1. Mã hóa/Giải mã WEP

WEP hoạt động ở tầng con MAC với lược đồ mã hóa như sau:

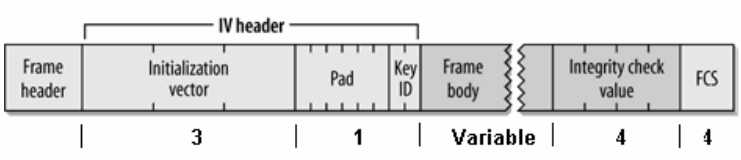


Hình 2-1. Lược đồ mã hóa WEP

Theo lược đồ, WEP sử dụng 3 thành phần đầu vào để thực hiện việc mã hóa:

- Thông tin cần bảo vệ (payload) được đưa xuống từ ngăn xếp giao thức tầng trên MAC (cụ thể ở đây là tầng con Điều khiển liên kết logic –LLC- trong tầng Liên kết dữ liệu).
- Khóa bí mật (secret key) hay còn gọi là khóa chia sẻ (shared key) được sử dụng để mã hóa khung tin. WEP cho phép có thể lưu 4 khóa đồng thời.
- Véc tơ khởi tạo (IV – Initialization Vector): được sử dụng cùng với khóa bí mật để mã hóa khung tin.

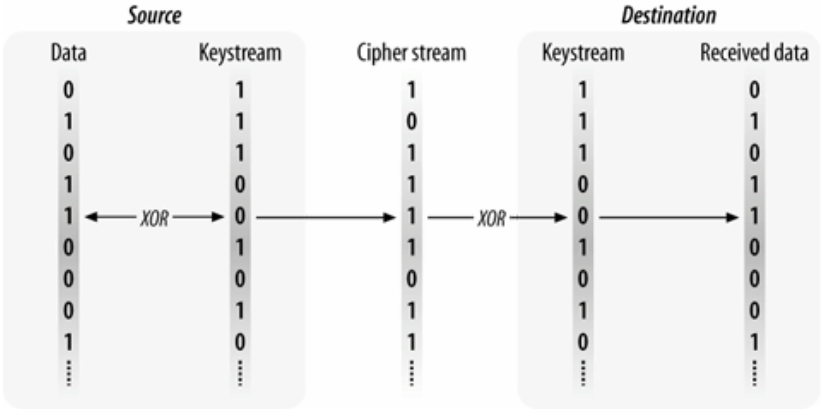
Sau khi mã hóa WEP sinh ra một khung tin MAC duy nhất với đầy đủ thông tin cần thiết để có thể giải mã được tại bên nhận. Bên nhận sau khi nhận được khung tin, sử dụng khóa bí mật cùng với véc tơ khởi tạo, thực hiện giải mã khung tin sau khi đã kiểm tra khung tin không bị sửa đổi trên đường truyền (kiểm tra CRC).



Hình 2-2. Cấu trúc khung tin WEP

a. Thuật toán RC4

WEP sử dụng phương pháp mã hóa RC4 được phát triển bởi Ron Rivest của tổ chức RSA Sercurity (1987). RC4 là thuật toán mã hóa luồng đối xứng, thực hiện phép toán XOR từng bit giữa khóa dòng (keystream) và dữ liệu gốc/dữ liệu đã mã hóa để đạt được kết quả mong muốn



Hình 2-3. Mã hóa/Giải mã RC4

Với phương pháp mã hóa đối xứng, khóa dòng được sử dụng cần phải được đảm bảo bí mật tối đa bởi khóa này cũng được sử dụng trong quá trình giải mã. Để đạt được điều đó, khóa này cần phải có tính ngẫu nhiên hoàn toàn – hay còn được gọi là khóa dùng một lần. Tuy nhiên, khó có thể có được khóa ngẫu nhiên hoàn toàn nên hầu hết các phương pháp mã hóa dòng sử dụng một khóa bí mật (được chia sẻ) có độ dài ngắn và mở rộng nó thành một khóa dòng giả ngẫu nhiên (pseudo-random) có độ dài bằng độ dài của dữ liệu cần được mã hóa.

Để tạo ra khóa dòng mong muốn trước khi XOR với dữ liệu cần mã hóa, RC4 sử dụng véc tơ khởi tạo, khóa bí mật và thuật toán sinh số giả ngẫu nhiên (PRGA).

Ở bước giải mã, do đặc tính của phép toán XOR, bên nhận cũng sử dụng véc tơ khởi tạo, khóa bí mật và thuật toán giả ngẫu nhiên để sinh ra khóa dòng, sau đó thực hiện XOR khóa dòng này với dữ liệu mã hóa để thu được nội dung thông điệp gốc.

b. Véc tơ khởi tạo (IV)

Véc tơ khởi tạo là một giá trị có độ dài 24 bit được WEP sử dụng trong RC4 nhằm tạo ra khóa dòng hoàn toàn khác cho từng gói tin được truyền đi. Véc tơ khởi tạo được thay đổi liên tục trong quá trình mã hóa, do đó với cùng một dữ liệu đầu vào thì dữ liệu đã mã hóa vẫn hoàn toàn khác nhau. Chuẩn 802.11 không quy định cách thức khởi tạo và thay đổi véc tơ khởi tạo trong quá trình mã hóa. Trong thực tế, véc tơ khởi tạo thường được khởi tạo từ một giá trị mặc định (giá trị 0), sau đó được thay đổi bằng cách tăng tuyến tính với bước tăng bằng 1 hoặc chọn ngẫu nhiên trong quá trình mã hóa.

Véc tơ khởi tạo được đính vào đầu hoặc cuối khung tin MAC (hình vẽ 2-2) mà không được mã hóa. Bên nhận sẽ sử dụng véc tơ khởi tạo nhận được kết hợp với khóa chia sẻ để sinh ra khóa dòng nhằm giải mã dữ liệu.

c. Khóa WEP và thuật toán PRGA

Khóa WEP (hay còn gọi là khóa chia sẻ, khóa bí mật) là khóa tĩnh được chia sẻ giữa các trạm và điểm truy cập. Tuy nhiên, khóa này không được sử dụng trực tiếp để mã hóa dữ liệu. Khi muốn mã hóa hay giải mã dữ liệu, các trạm và điểm truy cập kết hợp véc tơ khởi tạo, khóa WEP và thuật toán sinh số giả ngẫu nhiên (PRGA) để tạo ra khóa dòng cuối cùng.

Chuẩn 802.11 quy định khóa WEP có độ dài 40 bit nhưng các nhà sản xuất thiết bị thường cung cấp khả năng hỗ trợ khóa WEP có độ dài lên tới 104 bit. Để sử dụng, khóa WEP cần phải được khai báo tĩnh trong thiết bị (trạm không dây, điểm truy cập). Như đã trình bày, WEP hỗ trợ khai báo và lưu trữ 4 khóa WEP cùng một lúc.

Để mã hóa/giải mã dữ liệu, WEP thực hiện sử dụng hai thuật toán:

Thuật toán lập danh mục khóa (KSA)

Mục đích của thuật toán này nhằm tạo ra một mảng hoán vị các giá trị phục vụ cho thuật toán PRGA về sau. WEP sử dụng 8-bit RC4 và do đó, sẽ tạo ra một mảng hoán vị gồm 256 giá trị. Thuật toán KSA được mô tả như sau:

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := (j + S[i] + K[i mod keylength]) mod 256
    swap(S[i],S[j])
endfor
```

Theo đó, ban đầu WEP khởi tạo một mảng S gồm 256 giá trị được sắp lần lượt từ 0 tới 255. Sau đó, việc hoán vị các giá trị được thực hiện sử dụng mảng K và độ dài khóa (keylength). Mảng K có keylength phần tử, mỗi phần tử là một byte của chuỗi kết hợp bởi véc tơ khởi tạo và khóa WEP. Mảng K trong WEP thường có độ dài 8 byte (64 bit) hoặc 16 byte (128bit).

Thuật toán sinh số giả ngẫu nhiên (PRGA)

Dựa trên mảng S có được từ KSA, PRGA thực hiện việc tạo khóa dòng (keystream) giả ngẫu nhiên dùng để mã hóa dữ liệu. Thuật toán PRGA được mô tả như sau:

```
i := 0
j := 0
while GeneratingOutput:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap(S[i],S[j])
    z = S[(S[i] + S[j]) mod 256]
endwhile
```

Tại mỗi vòng lặp, PRGA sinh ra một byte của khóa dòng (giá trị z). Sau đó, giá trị z được XOR với một byte trong dữ liệu nhằm mã hóa/giải mã dữ liệu. Quá trình lặp kết thúc khi byte cuối cùng trong dòng dữ liệu cần mã hóa/giải mã đã được mã hóa/giải mã.

Trong thực tế, dữ liệu được truyền đi thường được chia thành nhiều gói tin (packet). Để đảm bảo an toàn, với các gói tin khác nhau WEP sử dụng các véc tơ khởi tạo khác nhau, và do đó, tạo ra một mảng KSA và khóa dòng hoàn toàn khác.

2.1.2. Đảm bảo tính toàn vẹn dữ liệu

Để đảm bảo dữ liệu không bị thay đổi trên đường truyền, WEP sử dụng thuật toán Kiểm tra dư thừa vòng CRC (Cyclic redundancy check) [21] để sinh ra một giá trị kiểm tra toàn vẹn ICV (Integrity Check Value) có độ dài 32 bit. Giá trị ICV này được đính vào dữ liệu trước khi được mã hóa bởi khóa dòng (hình 2-1). Bên nhận sau khi thực hiện giải mã, sẽ tách riêng giá trị ICV được đính kém rồi so sánh với giá trị ICV nó tính được trên dữ liệu (payload) đã được giải mã. Thông tin được coi là toàn vẹn khi hai giá trị này hoàn toàn khớp với nhau.

2.1.3. Những điểm yếu an ninh của WEP

a. Phương pháp mã hóa yếu

Cơ chế WEP sử dụng RC4 làm phương pháp mã hóa chính. Tuy nhiên, khi 802.11 được áp dụng rộng rãi thì những nghiên cứu cho thấy RC4 không đủ đảm bảo những yêu cầu an ninh cho truyền thông qua mạng không dây. Những điểm yếu trong RC4 thể hiện ở 3 điểm chính:

- Sử dụng lại véc tơ khởi tạo
- Sử dụng khóa yếu
- Khả năng tấn công khóa trực tiếp

Sử dụng lại véc tơ khởi tạo

Như trên đã trình bày, RC4 sử dụng véc tơ khởi tạo nhằm mục đích tạo ra mã dòng khác nhau cho các gói tin khác nhau. Để đạt được điều đó, véc tơ khởi tạo phải có được giá trị khác nhau ở mỗi lần sử dụng.

Tuy nhiên, với độ lớn 24 bit thì trong trường hợp xấu nhất (áp dụng cách tăng tuyến tính), không gian véc tơ khởi tạo sẽ được sử dụng hết sau $2^{24} \sim 17$ triệu khung tin. Điều đó đồng nghĩa với việc nếu sử dụng công nghệ 802.11b (có tốc độ thấp nhất là 11Mbps) thì sau khoảng 9h, vec tơ khởi tạo quay lại giá trị ban đầu (802.11b có khả

năng gửi 500 khung tin/giây). Hiện tượng này được gọi là xung đột véc tơ khởi tạo. Thực tế cho thấy, hiện tượng này xảy ra nhanh hơn khi có nhiều trạm tham gia vào quá trình truyền thông.

Một khi véc tơ khởi tạo được sử dụng lại, nguy cơ kẻ tấn công có thể dò ra một phần của khóa dòng càng cao. Khi kẻ tấn công thu thập được càng nhiều mẫu véc tơ khởi tạo bị trùng lặp, khả năng dò ra được từng phần của khóa dòng càng cao. Độ dài khóa dòng bị phát hiện tỷ lệ thuận với lượng dữ liệu mà kẻ tấn công có thể giải mã được. Vấn đề này được phát hiện lần đầu tiên bởi tác giả Jesse Walker [9].

Tuy nhiên, đây không phải là điểm yếu chính của WEP bởi để có thể thực hiện dò tìm khóa dòng và giải mã dữ liệu đòi hỏi công sức và thời gian rất lớn. Thêm vào đó, còn đòi hỏi trí tuệ từ con người, điều không thể đạt được từ các công cụ tự động.

Sử dụng khóa yếu

Điểm chính trong thuật toán mã hóa RC4 nằm ở thuật toán sinh số giả ngẫu nhiên. Việc hoán vị dựa vào hai chỉ số i, j cho tới 512*256! khả năng, một con số rất lớn. Và các nghiên cứu của các nhà mật mã trên 1GB dữ liệu liệu liên tục cho thấy rất khó phân biệt dãy số giả ngẫu nhiên với dãy số hoàn toàn ngẫu nhiên.

Mặc dù vậy, cách áp dụng RC4 một cách đơn giản như trong WEP lại gây ra một vấn đề lớn. Đó là, không có nhiều sự hoán vị giữa bảng KSA được thiết lập ban đầu và byte đầu tiên trong khóa dòng. Vấn đề này đã được Fluhrer và các đồng sự chỉ ra trong [10]. Các tác giả đã chỉ ra rằng một số bit trong khóa có vai trò quan trọng hơn các bit còn lại và điều này là một rủi ro bởi hai nguyên nhân: thứ nhất là khi số bit quan trọng được giảm đi thì khả năng tìm ra khóa là càng cao, thứ hai là một vài byte đầu của dữ liệu cần mã hóa thường rất dễ đoán. Ví dụ, trong khung tin WEP có header của gói tin LLC luôn bắt đầu bởi giá trị 0xAA.

Để giải quyết vấn đề này, cách tốt nhất là bỏ qua các byte đầu tiên trong của RC4 và khuyến cáo từ tổ chức RSA là bỏ qua 256 byte đầu của khóa dòng. Tuy nhiên WEP lại không làm theo cách này.

Khả năng tấn công khóa trực tiếp

Cũng trong [10], các tác giả chỉ ra rằng, khi giá trị véc tơ khởi tạo nối vào đầu khóa WEP trong quá trình sinh khóa dòng cũng tạo ra một lỗ hổng lớn bởi kẻ tấn

công có thể chờ đến khi bắt gặp khóa yếu và trực tiếp tấn công vào khóa (lấy khóa một cách trực tiếp). Thật không may, tình huống này lại rất hay xảy ra bởi sự xung đột véc tơ khởi tạo và một thực tế là có rất nhiều thông tin dễ đoán như IP header, SNAP header, IPX header, v.v.. Để minh chứng cho điểm yếu này, đã có rất nhiều công cụ tự động như WEPcrack, Airsnort đã ra đời cho phép kẻ tấn công dễ dàng thực hiện ý đồ của mình.

Một điểm cần chú ý là ở đây, độ dài khóa chỉ là tỷ lệ tuyến tính với thời gian tấn công cho nên việc tăng độ dài khóa là không thể giải quyết được điểm chính của vấn đề.

b. Cơ chế phân phối khóa "tĩnh"

Khóa bí mật được sử dụng trong WEP được khai báo và phân phối tĩnh. Điều đó có nghĩa là việc khai báo, sửa đổi và phân phối khóa được thực hiện bằng tay bởi người quản trị. Đây là một công việc tốn nhiều thời gian, khó quản lý nhất là khi số lượng trạm tham gia vào mạng là lớn. Một khi khóa bí mật bị lộ và không được sửa đổi kịp thời, hậu quả của rủi ro càng lớn.

c. Dữ liệu có thể bị sửa đổi

WEP sử dụng kỹ thuật CRC để tính mã kiểm tổng (ICV) cho dữ liệu gốc nhằm đảm bảo tính toàn vẹn của dữ liệu. Tuy nhiên, trong [12], các tác giả đã chỉ ra rằng, phương pháp CRC là một phương pháp tuyến tính. Theo đó, có thể đoán được vị trí bit sẽ bị sửa đổi trong ICV khi thay đổi một bit trong dữ liệu gốc và do đó có thể thực hiện sửa đổi dữ liệu trong khung tin mà không bị phát hiện.

Phương pháp tấn công được các tác giả đặt tên là "bit flipping" – sửa đổi bit. Ở phương pháp này, không cần thiết phải biết được dữ liệu gốc, kẻ tấn công chỉ cần biết nếu sửa đổi các bit trong dữ liệu gốc thì vẫn có thể đảm bảo ICV đúng nếu sửa đổi các bit tương ứng trong nó [3].

d. Không có cơ chế chống tấn công kiểu "replay"

Kiểu tấn công "thực hiện lại" (replay) được thực hiện bằng cách: kẻ tấn công thực hiện "nghe lén" tất cả thông tin (đã mã hóa) từ mạng. Từ thông tin này, kẻ tấn công có thể xác định được địa chỉ MAC của nạn nhân cũng như biết được gói tin

nào dùng để xác thực. Khi biết được nạn nhân đã rời khỏi mạng, bằng cách sửa đổi địa chỉ MAC và thực hiện gửi lại các thông điệp cũ. Bởi WEP không có cơ chế phản ứng với trường hợp này, nó vẫn giải mã gói tin và cho phép kẻ tấn công đăng nhập vào mạng. Việc kẻ tấn công có làm được thêm gì từ việc đăng nhập này hay không thì theo quan điểm về bảo mật, đó là một lỗ hổng nghiêm trọng.

2.2. Chuẩn an ninh IEEE 802.11i

Như đã trình bày, giải pháp an ninh WEP không đảm bảo được an ninh cho mạng 802.11 bởi có quá nhiều lỗ hổng. Nhóm chuẩn hóa 802.11 của IEEE đã sớm nhận ra điều này và sau ba năm rưỡi nỗ lực, chuẩn IEEE 802.11i ra đời (6/2004). Chuẩn IEEE 802.11i (gọi tắt là chuẩn 802.11i) tập trung vào vấn đề an ninh cho mạng 802.11, hỗ trợ cơ chế WEP (được sử dụng trong nhiều thiết bị 802.11 hiện tại) cũng như đưa ra giải pháp an ninh mới thay thế cho WEP.

Chuẩn an ninh 802.11i đưa ra hai cơ chế nhằm đảm bảo tính an toàn và toàn vẹn của dữ liệu là TKIP và CCMP. Chuẩn IEEE 802.1X được sử dụng để điều khiển truy cập vào mạng và thực hiện việc phân phối khóa. Cung cấp nhiều giao thức mã hóa, chuẩn 802.11i cung cấp một quá trình thương lượng (negociation process) nhằm lựa chọn giao thức mã hóa và khóa dòng cho từng loại dữ liệu. Những chức năng khác còn bao gồm lưu đệm khóa (key caching) và tiền xác thực (pre-authentication).

2.2.1. TKIP

TKIP (Temporal Key Intergrity Protocol – giao thức toàn vẹn khóa phiên) là giao thức mã hóa tầng liên kết trong chuẩn 802.11i được thiết kế để nâng cấp khả năng an ninh cho WEP nhưng vẫn hoạt động được trên các thiết bị phần cứng cũ hỗ trợ WEP. Nguyên nhân chính của việc sử dụng TKIP là các chip xử lý hỗ trợ WEP trong các thiết bị 802.11 cũ cung cấp khả năng mã hóa/giải mã RC4 (phần công việc nặng nhất) trên phần cứng.Thực chất, TKIP là giải pháp nâng cấp phần mềm cho các thiết bị sử dụng WEP. TKIP giữ nguyên kiến trúc cũng như các thao tác trong WEP.

2.2.1.1. Khác biệt giữa TKIP và WEP

Để cải thiện những điểm yếu của WEP, TKIP đưa vào một số các chức năng giao thức mới:

Cây phân cấp khóa và quản lý khóa tự động

Khác với WEP sử dụng chỉ một khóa chính duy nhất, TKIP sử dụng nhiều khóa chính. Khi cần mã hóa các khung tin, các khóa sẽ được sinh ra từ các khóa chính này. Các khóa này được sinh và quản lý bởi kiến trúc Mạng an toàn ổn định (RSN – Robust Security Network).

Khóa cho từng frame

Mặc dù TKIP vẫn giữ cơ chế mã hóa RC4 của WEP, nó sinh ra các khóa RC4 duy nhất cho mỗi khung tin từ khóa chính. Quá trình này được gọi là trộn khóa (key mixing).

Thứ tự khung tin

Mỗi khung tin trong TKIP được đánh số thứ tự nhằm giảm thiểu loại hình tấn công replay.

Sử dụng MIC thay thế CRC

TKIP thay thế thuật toán băm tuyến tính CRC bằng một thuật toán băm ổn định hơn gọi là Michael. Thuật toán này sinh ra mã toàn vẹn thông điệp gọi là MIC (Message Intergrity Code). Thêm vào đó, địa chỉ nguồn của khung tin cũng được bảo vệ bởi mã toàn vẹn nhằm phát hiện các khung tin bị giả mạo địa chỉ nguồn.

Phản ứng khi mã MIC sai

Được thiết kế để hoạt động trên các thiết bị phần cứng đã có, do đó TKIP cũng có những hạn chế của nó. Giống như mã CRC, mã MIC cũng có thể bị sửa đổi khi bị tấn công chủ động. Do đó, TKIP sử dụng cơ chế gọi là phản ứng (countermeasure) để hạn chế rủi ro khi mạng bị tấn công một cách chủ động.

2.2.1.2. Véc tơ khởi tạo

Để giảm thiểu nguy cơ tấn công vào véc tơ khởi tạo, TKIP tăng độ dài véc tơ khởi tạo từ 24 bit lên 48 bit. Với việc mở rộng này, không gian véc tơ khởi tạo tăng từ 16 triệu lên tới khoảng 280 nghìn tỷ véc tơ và do đó loại bỏ khả năng không gian

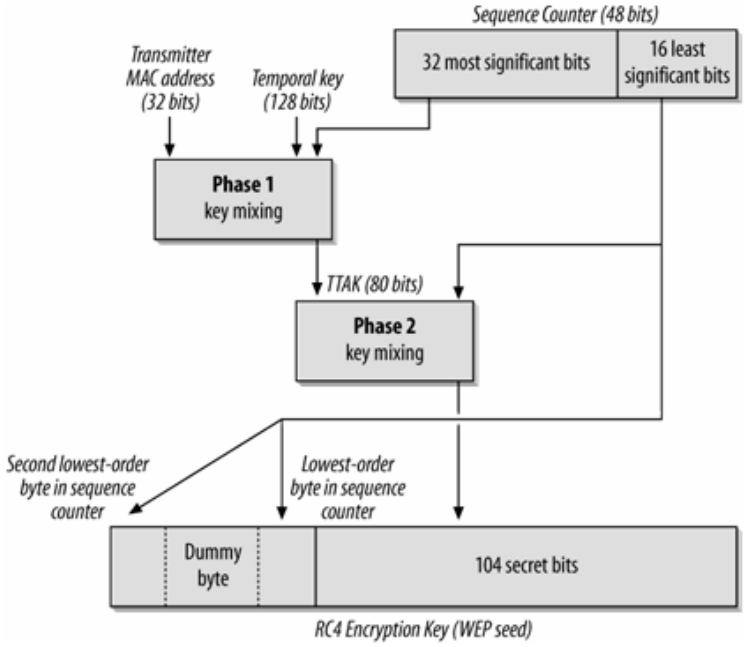
véc tơ bị sử dụng hết trong thời gian sống của một khóa. Để tiện trình bày và tránh sự nhầm lẫn, từ đây, véctơ khởi tạo của TKIP được gọi là TKIP IV, còn véctơ khởi tạo của WEP sẽ được gọi là WEP IV.

TKIP còn sử dụng TKIP IV để đánh số thứ tự khung tin (gọi là TSC). Mỗi khi một khóa chính mới được sử dụng, TKIP IV (số thứ tự khung tin) được đưa về 1. Mỗi khung tin được truyền đi sẽ tăng tuần tự giá trị này lên 1 đơn vị.

Để chống lại hình thức tấn công replay, với mỗi trạm không dây, TKIP lưu giá trị thứ tự khung tin gần nhất nhận được từ trạm đó. Mỗi khi nhận được một khung tin, số thứ tự của khung tin đó được so sánh với giá trị đã lưu. Nếu giá trị này lớn hơn hoặc bằng giá trị đã lưu thì khung tin được chấp nhận, ngược lại khung tin bị từ chối. Do đó, trường hợp khung tin cần phải gửi lại (do thất lạc khung tin hoặc gói tin biên nhận) cũng không bị coi là dấu hiệu bị tấn công.

2.2.1.3. Quá trình trộn khóa

Để đảm bảo mỗi khung tin được truyền đi được mã hõa bởi một khóa RC4 duy nhất, TKIP thực hiện quá trình trộn khóa. Quá trình này sử dụng TKIP IV, địa chỉ nguồn và khóa phiên theo thời gian. Địa chỉ nguồn của khung tin được đưa vào quá trình trộn khóa nhằm mục đích đảm bảo rằng nếu hai khung tin có cùng một TKIP IV thì vẫn được mã hóa bởi hai khóa RC4 khác nhau.



Hình 2-4. Quá trình trộn khóa

Theo như hình vẽ, TKIP chia quá trình trộn khóa ra làm hai pha (Phụ lục 2). Nguyên do là bởi năng lực xử lý thấp của các thiết bị không dây hỗ trợ WEP.

Pha thứ nhất lấy địa chỉ MAC nguồn, 128-bit khóa phiên theo thời gian, và 32 bit đầu của TKIP IV để sinh ra một giá trị 80 bit. Quá trình tính toán này chỉ sử dụng các phép toán như cộng, dịch chuyển bit (shift) và XOR để làm giảm khối lượng tính toán. Kết quả là giá trị sinh ra từ pha này là một hằng số khi 32 bit đầu của TKIP IV là một hằng số. Do vậy, sau 2^{16} = 65.536 khung tin pha thứ nhất mới cần phải thực hiện lại.

Pha thứ hai của quá trình trộn khóa (ít phức tạp hơn) thực hiện việc tính toán cho mỗi khung tin được gửi đi. Pha này lấy giá trị sinh ra từ pha 1, khóa phiên theo thời gian và 16 bit cuối của TKIP IV làm giá trị đầu vào. Sau quá trình tính toán, khóa RC4 được sinh ra có độ dài 128 bit (hình vẽ 2-4). Trong đó, 16 bit thấp của TKIP IV được sử dụng để tạo ra WEP IV (24-bit). Byte giữa của WEP IV là bản sao của byte đầu trong đó hai bit thứ 4 và 5 được đặt giá trị cố định là 0 và 1. Cách làm này tránh được việc sinh ra khóa RC4 yếu, phía nhận sẽ bỏ qua byte giữa trong quá trình giải mã. Toàn bộ khóa RC4 này (bao gồm WEP IV và 104 bit khóa bí mật) được chuyển xuống cho WEP thực hiện việc mã hóa và gửi khung tin.

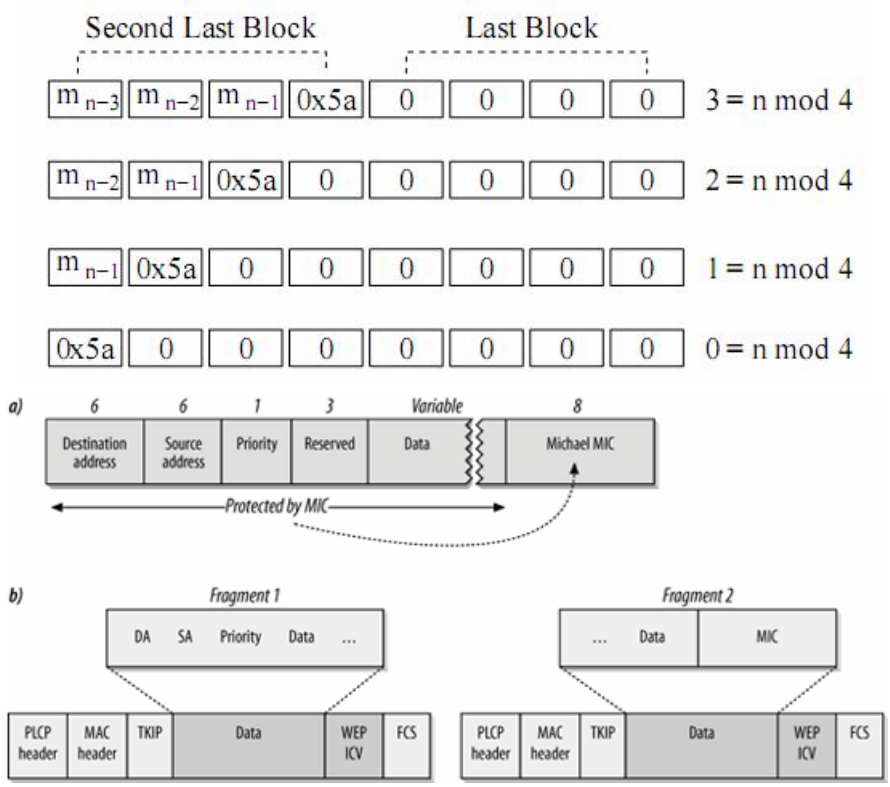
2.2.1.4. Mã kiểm tra toàn vẹn Michael

Để thay thế cho mã kiểm tra toàn vẹn CRC vốn dễ bị tấn công, TKIP sử dụng thuật toán Michael để tạo mã toàn vẹn cho thông điệp.

Được phát triển bởi Neils Ferguson (2002) [20] với mục đích xây dựng một thuật toán tạo mã kiểm tra toàn vẹn phục vụ cho TKIP, thuật toán Michael chỉ sử dụng các phép toán bit như tráo đổi, dịch chuyển và loại trừ nên việc áp dụng không gây ảnh hưởng tới năng lực xử lý thấp của các phần cứng trước đó.

Thuật toán Michael thực hiện việc tính toán ở tầng trên trước khi khung tin được chuyển cho tầng MAC. Thuật toán sử dụng khóa có độ dài 64 bit, thực hiện tính toán trên các khối 32-bit của toàn bộ nội dung thông điệp (bao gồm cả địa chỉ nguồn và đích) (hình 2-5). Trước khi thực hiện, thuật toán sẽ nối một byte có giá trị 0x5a và từ 4 đến 7 byte có giá trị 0 vào đuôi thông điệp để đảm bảo nội dung được tính toán là bội số của 4. Sau khi tính toán, mã MIC có độ dài 8 byte, được nối vào

đuôi gói tin MSDU trước khi truyền dữ liệu đi. Dữ liệu này khi truyền đi có thể bị chia nhỏ, tuy nhiên tại phía nhận, mã MIC chỉ được tính toán khi khung tin đã được tập hợp lại.



Hình 2-5. Tính toán mã MIC

Tuy nhiên, nhận thấy mã kiểm tra MIC là chưa đủ để chống chọi lại khả năng bị tấn công, chuẩn 802.11i còn đưa thêm vào một bước vào gọi là Michael Countermeasure (tạm dịch là Phản ứng khi mã MIC sai). Quy trình được thực hiện như sau:

- Mỗi khi phát hiện ra mã MIC sai, giá trị này được đánh dấu và ghi lại. Tuy nhiên, trước khi được kiểm tra toàn vẹn, khung tin phải đi qua hai quá trình: kiểm tra toàn vẹn của WEP và kiểm tra chống tấn công replay của TKIP. Do đó, bất kỳ một lỗi MIC nào cũng được coi là nghiêm trọng và cần được sự can thiệp của quản trị viên hệ thống.
- Nếu trong 60 giây, hệ thống bắt gặp mã MIC sai lần thứ 2, counter measure sẽ thực hiện việc ngắt kết nối trong vòng 60 giây tiếp theo. Việc ngắt kết nối sẽ khiến cho kẻ tấn công không thể thực hiện một cách nhanh chóng. Mặc dù 802.11i quy định thời gian phản ứng khi mã MIC sai là 60 giây, một số nhà

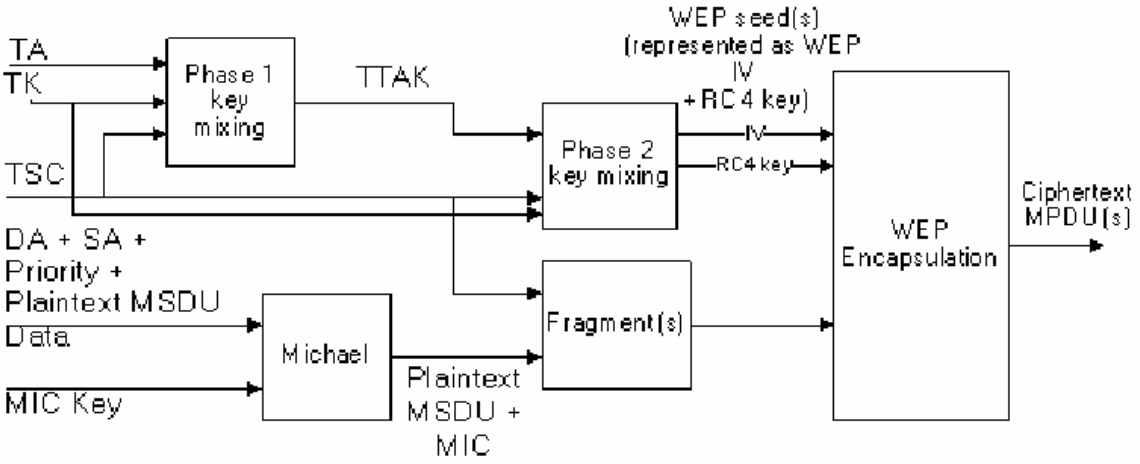
sản xuất vẫn cho phép cấu hình lại khoảng thời gian này.

- Các trạm sẽ xóa khóa chính trong bộ nhớ và yêu cầu khóa mới từ phía bộ phận xác thực. Bộ phận xác thực sẽ thực hiện việc sinh lại và phân phối khóa cho các bên.

Thuật toán Michael -theo thiết kế- cung cấp mức độ an ninh 20 bit. Theo đó, sau khoảng 2^{19} lần, kẻ tấn công có thể giả mạo được giá trị MIC. Với giá trị này, trên một mạng 802.11b có khả năng truyền 2^{12} gói tin trong 1 giây, kẻ tấn công chỉ mất khoảng 2 phút (2^7 giây) để thu được giá trị MIC giả mạo hợp lệ. Tuy nhiên, cơ chế phản ứng khi MIC sai chỉ cho phép tối đa 2 gói tin giả mạo trong 1 phút, và do đó thời gian để kẻ tấn công có thể tạo được một gói tin giả mạo có MIC hợp lệ là 2^{18} phút (tương đương với 6 tháng). Do đó, cơ chế phản ứng khi MIC sai được coi là an toàn với kiểu tấn công giả mạo thông điệp.

2.2.1.5. Quá trình hoạt động của TKIP

Tại phía gửi, khi một khung tin được chuyển xuống cho TKIP để truyền đi, quá trình xử lý được mô tả như sau:



Hình 2-6. Quá trình gửi dữ liệu của TKIP

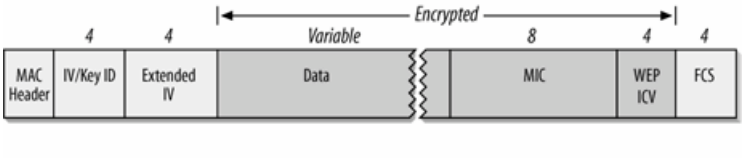
1. Khung tin 802.11 được đưa vào hàng đợi để gửi đi. Mỗi khung tin bao gồm phần mào đầu và phần dữ liệu. TKIP chỉ thực hiện mã hóa phần dữ liệu.

2. Mã kiểm tra MIC được tính toán dựa trên khóa bí mật. Bên cạnh dữ liệu của khung tin, MIC thực hiện tính toán bao gồm cả địa chỉ nguồn và đích.

3. Số thứ tự khung tin (TSC) được gán vào mỗi mảnh dữ liệu của khung tin.

4. Dựa vào các thông tin đầu vào, TKIP thực hiện quá trình trộn khóa. Khóa này được thay đổi liên tục theo từng frame.

5. Khung tin sẽ được nối với mã MIC ở bước 2 rồi gửi xuống tầng WEP cùng với khóa RC4 sinh ra ở bước 4. WEP sẽ thực hiện việc mã hóa dữ liệu rồi gửi đi.



Hình 2-7. Cấu trúc khung tin TKIP

Tại phía nhận, sau khi nhận được khung tin mã hóa, sẽ thực hiện quá trình giải mã để lấy được dữ liệu gốc.

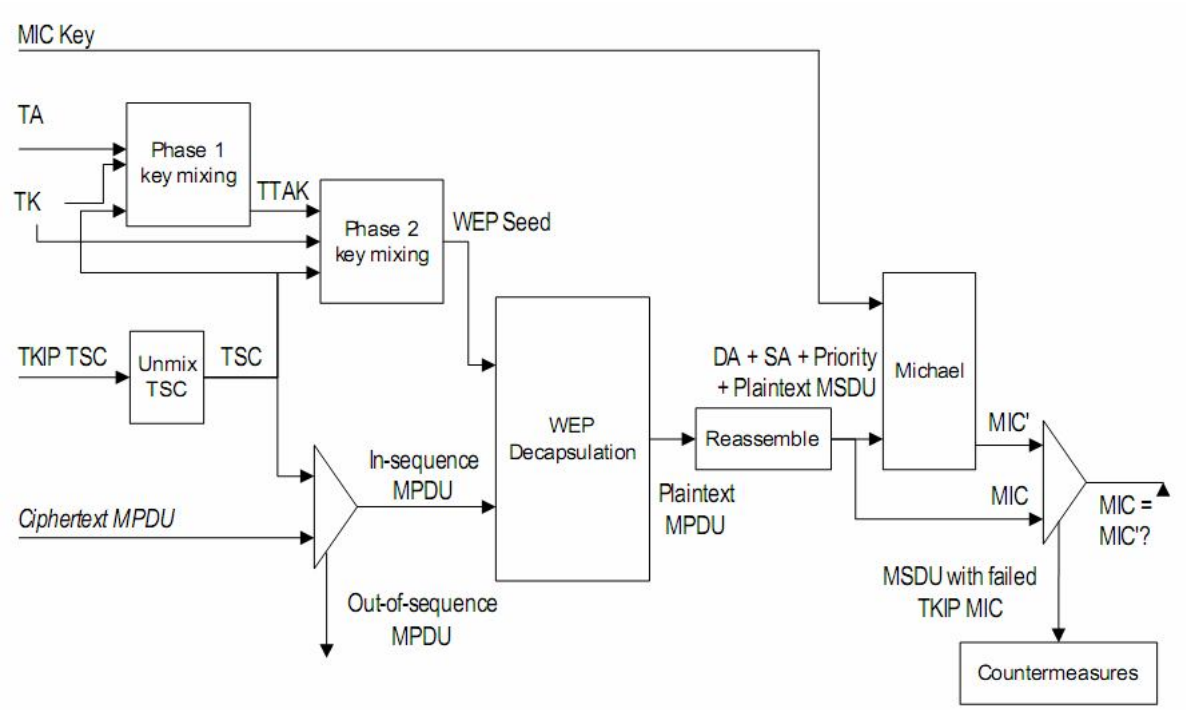
1. Khi giao diện không dây nhận được 1 khung tin, nó thực hiện kiểm tra toàn vẹn dữ liệu để tin chắc rằng khung tin không bị lỗi trên đường truyền. Tiếp đó khung tin được chuyển cho TKIP để kiểm tra.

2. TKIP sẽ kiểm tra số thứ tự khung tin để ngăn chặn kiểu tấn công replay.

3. TKIP thực hiện tính toán khóa WEP. Với dữ liệu đầu vào giống như bên gửi, khóa WEP sẽ được phục hồi lại để phục vụ quá trình giải mã.

4. WEP thực hiện kiểm tra mã toàn vẹn CRC. Tiếp đó, WEP sẽ thực hiện giải mã. Nếu như khung tin đã bị phân nhỏ, quá trình sẽ chờ để nhận đủ các mảnh nhỏ của khung tin trước khi kết hợp lại thành một khung tin hoàn chỉnh. Tuy vậy, việc phân mảnh khung tin ít khi được sử dụng trong chuẩn 802.11.

5. Sau khi khung tin đã được kết hợp lại (nếu cần thiết), mã MIC được tính lại trên toàn bộ nội dung khung tin, sau đó được so sánh với mã MIC được gửi kèm theo khung tin. Nếu như mã MIC không khớp, bước Phản ứng khi mã MIC sai được kích hoạt.



Hình 2-8. Quá trình tiếp nhận và giải mã của TKIP

2.2.2. CCMP

Khi bắt đầu công việc vào năm 2000, nhóm chuẩn hóa 802.11 nhận ra rằng chuẩn WEP là không an toàn, mặc dù những điểm yếu nghiêm trọng của WEP vào thời điểm này vẫn chưa bị phát hiện ra. Nhiệm vụ của nhóm là cần phải lựa chọn một thuật toán mã hóa cho chuẩn mới. Vào thời điểm này, viện chuẩn và công nghệ Mỹ đã lựa chọn thuật toán mã hóa AES (chuẩn mã hóa nâng cao – Advance Encryption Standard) để áp dụng cho các cơ quan liên bang nhằm bảo vệ những dữ liệu nhạy cảm. Chuẩn AES được xây dựng từ thuật toán Rijndael ([17], [18]) được lựa chọn trong số 15 thuật toán mã hóa gửi tới cơ quan này.

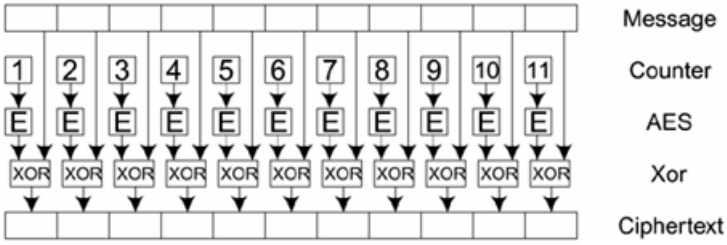
Thuật toán AES là thuật toán mã hóa khối có thể hoạt động trên nhiều khóa và khối có độ lớn khác nhau. Để tránh sự nhập nhằng, chuẩn 801.11i quy định kích thước khóa là 128 bit và độ lớn khối là 128 bit.

Giao thức an ninh hoạt động ở tầng liên kết dữ liệu sử dụng AES được gọi là CCMP (giao thức Chế độ đếm kết hợp CBC-MAC). CCMP là chế độ hoạt động kết hợp trong đó cùng một khóa vừa được sử dụng để mã hóa và đảm bảo toàn vẹn cho dữ liệu.

2.2.2.1. Chế độ đếm kết hợp CBC-MAC (CCM)

Trong thuật toán mã hóa AES, thuật ngữ chế độ hoạt động (mode of operation) được sử dụng để chỉ phương thức chia khối, mã hóa và tập hợp lại thành thông điệp gốc.

Chế độ đếm (counter mode) hay còn gọi chế độ CTR hoạt động theo phương thức: sử dụng một giá trị bình thường (gọi là số đếm), thực hiện mã hóa giá trị này rồi XOR với khối dữ liệu để tạo ra dữ liệu đã mã hóa (hình 2-9).



Hình 2-9. Mã hóa theo chế độ đếm (Counter Mode)

Trong hình minh họa, số đếm được bắt đầu từ 1 và bước tăng là 1. Tuy nhiên, trong triển khai thực tế, số đếm khởi nguồn thường được sinh ra từ một giá trị thay đổi theo từng thông điệp. Điều này sẽ tránh được việc sinh ra giá trị mã hóa giống nhau cho hai thông điệp riêng biệt giống nhau. Cả phía nhận và phía gửi đều phải biết giá trị bắt đầu và quy luật tăng cho số đếm để có thể thực hiện mã hóa và giải mã.

Với cách hoạt động như vậy, thì phía mã hóa hay giải mã chỉ cần thực thi thuật toán mã hóa khối AES với số đếm được đồng bộ ở 2 phía bởi việc XOR hai lần cùng một giá trị của một toán hạng sẽ cho ta giá trị dữ liệu ban đầu của toán hạng còn lại. Thêm vào đó, nếu dữ liệu cần mã hóa có độ rộng không là bội số của kích thước khối, thì việc mã hóa chỉ đơn giản là XOR giá trị mã hóa giá trị đếm với dữ liệu, và do đó, kích thước của khối dữ liệu đã mã hóa sẽ bằng với kích thước dữ liệu trước khi mã hóa.

Mã hóa AES theo chế độ đếm đã được sử dụng hơn 20 năm và đạt được niềm tin ở cộng đồng bảo mật về độ an toàn của nó. Tuy vậy phương pháp chỉ phục vụ cho mục đích mã hóa dữ liệu, do đó cần một phương pháp đảm bảo tính toàn vẹn cho dữ liệu.

Phương thức đảm bảo toàn vẹn dữ liệu sử dụng trong CCMP gọi là phương

thức chuỗi khối mã hóa (CBC). CBC được sử dụng để tạo ra mã toàn vẹn (MIC) cho thông điệp được gửi đi. Trong cộng đồng bảo mật, MIC được gọi là mã xác thực thông điệp (MAC – Message Authentication Code) cho nên CBC còn được gọi là CBC-MAC [19]. Cách hoạt động của CBC-MAC tương đối đơn giản:

- Lấy khối đầu tiên trong thông điệp và mã hóa (sử dụng AES)
- XOR kết quả thu được với khối thứ 2 và tiếp tục mã hóa kết quả thu được
- XOR kết quả thu được với khối tiếp theo rồi mã hóa nó. Cứ như vậy tiếp tục cho đến hết.

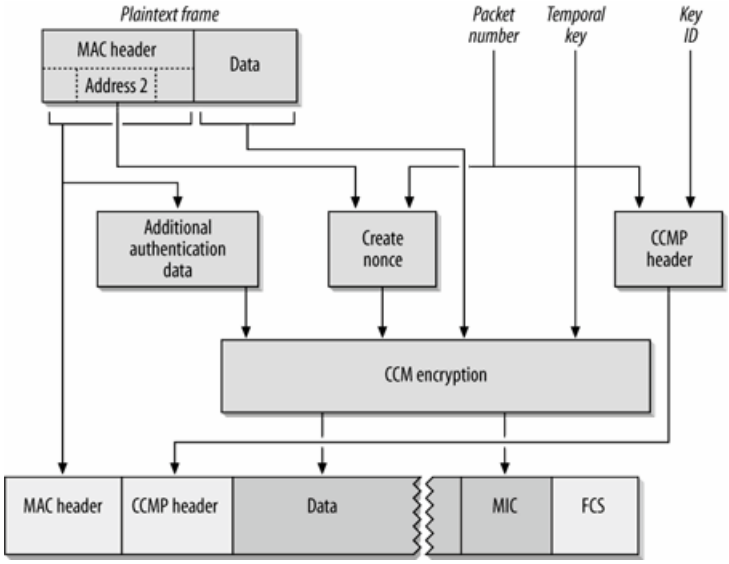
Cách hoạt động của CBC-MAC tương đối đơn giản nhưng không thể song song hóa như chế độ đếm. Với những thông điệp mà độ lớn không là bội số của kích thước khối, CCMP đưa thêm các bit 0 vào cuối thông điệp để CBC-MAC có thể hoạt động được. Ngoài ra, CBC-MAC còn cho phép đảm bảo tính toàn vẹn cho những dữ liệu không được mã hóa (AAD) chẳng hạn như địa chỉ MAC của khung tin.

2.2.2.2. Quá trình hoạt động của CCMP

Tại phía gửi, khi thông điệp cần gửi đi được chuyển xuống CCMP, quá trình diễn ra như sau:

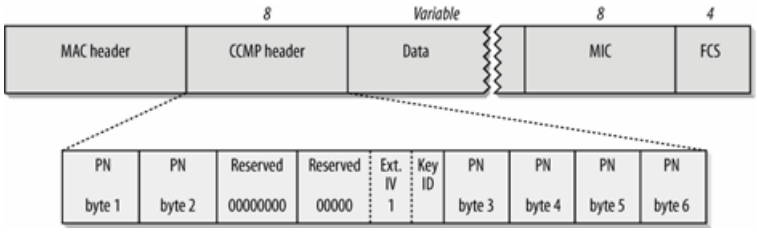
- Mỗi thông điệp được gán một số thứ tự gói (PN) có độ lớn 48bit. Số thứ tự gói cũng giống như TKIP IV, là duy nhất và không được sử dụng lại cho từng khóa phiên.
- Trường Dữ liệu xác thực bổ sung được tạo ra chứa giá trị những thông tin trong khung tin 802.11 cần được kiểm tra tính toàn vẹn nhưng không được mã hóa (AAD) bao gồm phiên bản giao thức, loại khung tin, các bit hệ thống, số hiệu mảnh, các bit thứ tự, địa chỉ MAC …
- Tiếp đó, giá trị CCMP nonce được tạo ra. Giá trị này được hình thành từ số thứ tự gói cùng với địa chỉ nguồn để đảm bảo việc mã hóa chỉ thực hiện trên dữ liệu duy nhất. Đây chính là số đếm sử dụng trong chế độ đếm để mã hóa dữ liệu

- Các giá trị này cùng với phần dữ liệu của thông điệp được chuyển vào bộ CCM, trong đó phần thân thông điệp được mã hóa AES sử dụng khóa phiên và CCMP nonce, còn trường AAD và dữ liệu được tạo mã kiểm tra toàn vẹn 8 byte MIC nhờ CBC-MAC sử dụng khóa phiên.



Hình 2-10. Quá trình mã hóa CCMP

Khung tin CCMP được tạo ra và chuyển xuống tầng vật lý để gửi đi.



Hình 2-11. Cấu trúc khung tin CCMP

Tại phía nhận, khi nhận được khung tin, quá trình giải mã và kiểm tra diễn ra như sau:

- Khung tin nhận được bởi tầng MAC sẽ được kiểm tra giá trị FCS trước khi chuyển xuống cho CCMP xử lý.
- Trường AAD được tạo ra từ khung tin nhận được.
- Giá trị CCMP nonce được tính toán.
- Phía nhận giải mã dữ liệu sử dụng khóa phiên và CCMP nonce.
- Giá trị MIC được tính toán trên trường AAD và dữ liệu đã giải mã rồi so sánh với giá trị MIC trong khung tin nhận được. Nếu 2 giá trị này khác nhau,

quá trình xử lý dừng.

- Giá trị số thứ tự gói được kiểm tra để chống lại hình thức tấn công replay. Khung tin nguyên thuỷ được hình thành.

2.2.3. RSN

Bên cạnh TKIP và CCMP, chuẩn 802.11i định nghĩa một kiểu mạng không dây mới gọi là mạng an toàn ổn định (RSN – Robust Security Network) – về bản chất là định nghĩa cây phân cấp khóa và tập các thủ tục sinh khóa (bên cạnh các phương pháp mã hóa đã được lựa chọn). Như vậy, về khía cạnh nào đó, RSN cũng tương tự như mạng không dây sử dụng WEP.

Ở một mạng RSN thực sự, điểm truy cập chỉ cho phép các thiết bị có khả năng hoạt động với RSN được truy cập vào mạng, đồng thời áp dụng các ràng buộc an ninh chặt chẽ trong quá trình truyền thông. Tuy vậy, với cùng yêu cầu giống như ở TKIP, rất nhiều thiết bị phần cứng cũ cần được hỗ trợ trong một thời gian trước khi được chuyển hoàn toàn sang RSN. Do đó, 802.11i định nghĩa kiểu mạng an toàn quá độ (TSN – Transition Security Network), cho phép RSN và WEP có thể hoạt động đồng thời. Đó là trường hợp của TKIP đã được trình bày ở trên.

2.2.3.1. Cây phân cấp khóa

Trong kiến trúc RSN, có hai loại khóa được sử dụng cho việc mã hóa ở tầng liên kết dữ liệu. Loại thứ nhất được gọi là khóa cặp (pairwise key) được sử dụng để mã hóa luồng thông tin unicast giữa điểm truy cập và thiết bị sau khi đã kết nối. Loại thứ hai được gọi là khóa nhóm (group key) được sử dụng để mã hóa luồng thông tin broadcast và multicast giữa điểm truy cập và thiết bị.

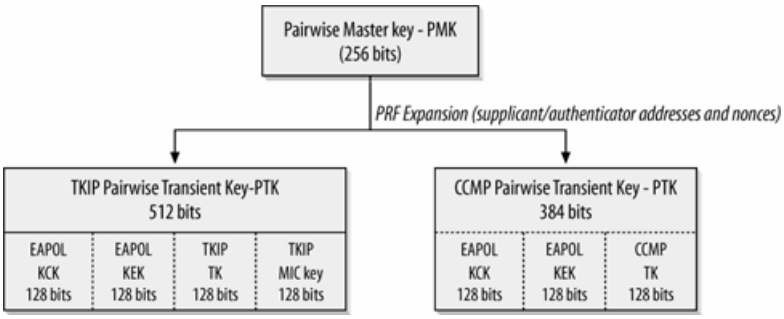
a. Cây phân cấp khóa cặp

Cây phân cấp khóa được xây dựng bắt đầu bởi khóa cặp chính (PMK – Pairwise Master Key). Chuẩn 802.11i cho phép khóa cặp chính có thể được tạo ra theo hai cách. Một là nhờ quá trình xác thực giữa điểm truy cập và thiết bị, PMK được tạo ra bởi máy chủ xác thực, sau đó được phân phối tới điểm truy cập và thiết bị. Cách thứ hai là PMK có thể được cấu hình sẵn ở cả điểm truy cập và thiết bị dưới dạng khóa chia sẻ trước (PreShared Key - PSK).

Khóa chia sẻ là một mật khẩu có độ dài 20 đến 63 byte được cấu hình sẵn trong thiết bị và điểm truy cập. Khóa chia sẻ có thể được cấu hình theo từng thiết bị hoặc cấu hình toàn cục cho cả mạng không dây. Từ PSK này, PMK được sinh ra ra. Tuy vậy, chuẩn 802.11i không đặc tả cách thức sinh PMK từ PSK mà để mở cho các nhà sản xuất phần cứng. Theo đó, phần lớn các nhà sản xuất thiết bị (tuân theo quy định của hiệp hội WiFi) sử dụng hàm PBKDFv2 [30] để sinh ra khóa PMK có độ dài 256 bit từ PSK.

Cả hai giao thức mã hóa TKIP và CCMP đều hoạt động theo cùng một nguyên tắc: sử dụng khóa bí mật chính này để tạo ra các khóa khác nhau sử dụng trong quá trình mã hóa khung tin. Theo cách này, các thiết bị có thể thay đổi khóa sử dụng khóa bí mật chính mà không cần thực hiện lại quá trình xác thực với điểm truy cập.

Khóa cặp chính có độ lớn 256-bit, được giữ ở cả điểm truy cập và thiết bị. Khóa cặp chính này là duy nhất giữa các luồng truyền thông từ điểm truy cập tới thiết bị. Từ khóa cặp chính này, thông qua hàm sinh số giả ngẫu nhiên PRF (phụ lục 3) được định nghĩa sẵn, cây phân cấp khóa cặp được hình thành.



Hình 2-12. Cây phân cấp khóa cặp

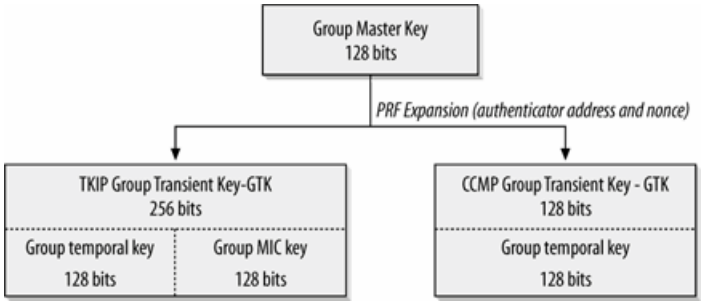
Như trên hình vẽ, cả TKIP và CCMP đều sử dụng hàm sinh số giả ngẫu nhiên tạo ra các khóa cặp quá độ (TKIP PTK và CCMP PTK). Cả TKIP PTK và CCMP PTK sử dụng hai khóa 128 bit (KCK và KEK) để mã hóa dữ liệu thông điệp khóa được truyền giữa điểm truy cập và thiết bị. Khóa đầu tiên, KCK (EAPOL Key Confirmation Key), được sử dụng để tính mã kiểm tra toàn vẹn của thông điệp khóa. Còn khóa KEK (EAPOL Key Encryption Key) được sử dụng để mã hóa thông điệp khóa. Khóa thứ 2 có độ rộng 128 bit chính là khóa phiên được sử dụng trong cả hai phương pháp mã hóa. Khác với CCMP PTK, TKIP PTK có độ dài 512 bit, trong đó 128 bit cuối cùng được sử dụng để tính toán mã toàn vẹn MIC trong

quá trình hoạt động của TKIP.

Các thông điệp khóa được mã hóa bởi khóa EAP-KEK sử dụng một trong hai thuật toán mã hóa là RC4 và thuật toán mã hóa khóa AES [36]. Còn phương pháp đảm bảo tính toàn vẹn cho thông điệp khóa được chuẩn 802.11i chỉ định một trong hai hàm băm là HMAC-MD5 và HMAC-SHA-1.

b. Cây phân cấp khóa nhóm

Giống như cây phân cấp khóa cặp, cây phân cấp khóa nhóm cũng được xây dựng bắt đầu từ đỉnh với khóa nhóm chính (GMK – Group Master Key). GMK có độ lớn 128bit được tạo ra và duy trì bởi điểm truy cập. Điểm truy cập sẽ tạo ra và duy trì GMK (có độ lớn 128 bit). Từ GMK, điểm truy cập sử dụng hàm sinh số giả ngẫu nhiên PRF để sinh ra khóa quá độ GTK. Với TKIP, GTK có độ lớn 256 bit bao gồm 128 bit khóa phiên và 128 bit khóa toàn vẹn (MIC key). Với CCMP, GTK có độ lớn 128 bit – chính là khóa phiên được sử dụng để mã hóa luồng dữ liệu broadcast và multicast.



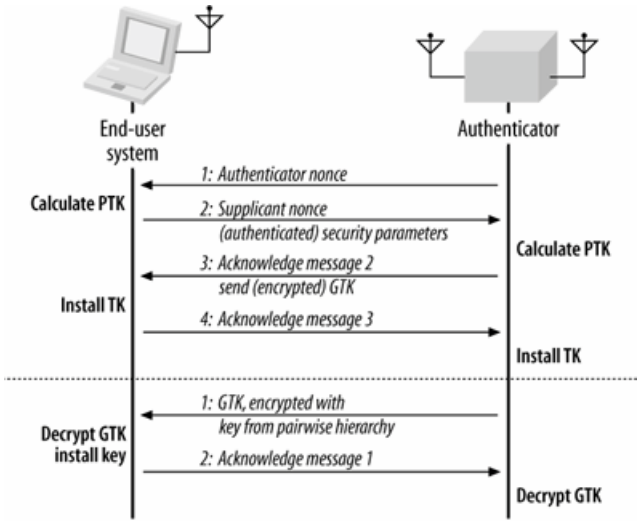
Hình 2-13. Cây phân cấp khóa nhóm

2.2.3.2. Sinh khóa và phân phối khóa

Thay vì sử dụng ngay khóa cặp chính vào mục đích mã hóa, chuẩn 802.11i đặc tả một cơ chế sinh khóa (hay cơ chế sinh cây phân cấp khóa) gọi là KGD. Mục đích của KGD là nhằm:

- Xác nhận sự tồn tại khóa cặp chính ở cả điểm truy cập và thiết bị
- Sinh cây phân cấp khóa và đồng bộ việc thiết đặt khóa phiên ở cả điểm truy cập và thiết bị
- Phân phối khóa cặp dùng để mã hóa luồng truyền thông multicast và broadcast

Để chống lại kiểu tấn công replay, KGD sử dụng các số ngẫu nhiên và quá trình "bắt tay". KGD bao gồm hai quá trình bắt tay diễn ra tuần tự: bắt tay 4 bước (4-way handsshake) dành cho khóa cặp chính và bắt tay nhóm (group handshake) dành cho khóa nhóm.



Hình 2-14. Quá trình bắt tay trao đổi khóa

Quá trình trình bắt tay 4 bước được thực thi khi cả thiết bị và điểm truy cập đều đã có khóa cặp chính (được phân phối bởi máy chủ xác thực hoặc được cấu hình sẵn):

- Điểm truy cập gửi tới thiết bị một giá trị ngẫu nhiên. Tại thời điểm này, thiết bị có thể sinh ra cây phân cấp khóa sử dụng 2 giá trị ngẫu nhiên (1 giá trị nhận từ điểm truy cập), địa chỉ MAC của hai bên và khóa cặp chính.
- Thiết bị gửi lại một thông điệp chứa giá trị ngẫu nhiên mà nó sinh ra cùng với các tham số an ninh có từ bước liên kết ban đầu. Điểm truy cập nhận được thông điệp, thu lấy giá trị ngẫu nhiên và sinh ra cây phân cấp khóa cặp của nó. Thông điệp này được kiểm tra toàn vẹn nhờ khóa EAPOL-KCK.
- Tại thời điểm này, cây phân cấp khóa đều đã được hình thành ở hai phía tuy nhiên vẫn cần sự xác nhận. Để làm được điều đó, điểm truy cập gửi tới thiết bị một thông điệp chỉ định số thứ tự được sử dụng. Thông điệp này cũng chứa giá trị GTK. Toàn bộ nội dung thông điệp được mã hóa bởi EAPOL-KEK và tính giá trị toàn vẹn nhờ EAPOL-KCK.
- Thiết bị gửi thông điệp xác nhận cuối cùng tới điểm truy cập. Sau đó, cả hai

bên có thể sử dụng cây phân cấp khóa đã sinh ra để phục vụ quá trình mã hóa. Thông điệp xác nhận cuối cùng này được kiểm tra toàn vẹn nhờ khóa EAPOL-KCK.

Khác với khóa cặp, khóa nhóm chính (GMK) được tạo ra bởi chính điểm truy cập. Từ GMK, điểm truy cập thực hiện sinh ra GTK và phân phối tới thiết bị. Thông điệp chứa khóa GTK được mã hóa và kiểm tra toàn vẹn nhờ hai khóa KEK và KCK (được sinh ra trong cây phân cấp khóa cặp).

Mỗi khi muốn rời khỏi mạng, thiết bị sẽ gửi gói tin thông báo tới điểm truy cập, điểm truy cập sẽ thực hiện xóa toàn bộ khóa cặp liên quan tới thiết bị đó đồng thời ngừng gửi thông điệp tới thiết bị đó. Cây phân cấp khóa nhóm cũng được xóa đi và sinh lại. Tuy nhiên, khóa cặp chỉ được sinh lại và phân phối khi thiết bị gia nhập trở lại vào mạng. Với khóa nhóm, việc sinh và phân phối lại phải được thực hiện ngay sau khi một thiết bị rời khỏi mạng để đảm bảo các thiết bị khác trong mạng vẫn có khả năng gửi và nhận các thông điệp broadcast và multicast.

Quá trình sinh và phân phối lại được thực hiện qua hai bước:

- Điểm truy cập gửi khóa GTK mới tới tất cả các thiết bị còn trong mạng.
- Các thiết bị gửi gói tin biên nhận về điểm truy cập.

Khi điểm truy cập nhận được gói tin biên nhận của tất cả thiết bị, nó thực hiện chuyển sang cây phân cấp khóa nhóm mới. Tuy nhiên, khóa nhóm được sinh và phân phối lại thường xuyên nên cần có một cách làm việc đó mà không làm ảnh hưởng tới mạng hiện thời. Với yêu cầu đó, cần có một phương pháp để việc sinh và phân phối lại không làm ảnh hưởng tới hoạt động của mạng không dây hiện thời. Rất may là từ chuẩn WEP đã cho phép nhiều khóa được lưu trên mỗi thiết bị. Cụ thể là trong mỗi khung tin đều có trường KeyID có độ lớn 2 bit cho phép xác định khóa nào trong 4 khóa (được lưu trên thiết bị) được sử dụng. Bên cạnh việc điểm truy cập điều khiển việc cập nhật khóa nhóm, thiết bị cũng có thể yêu cầu sử dụng một khóa nhóm mới bằng cách gửi một thông điệp tới điểm truy cập.

Bên cạnh việc sinh lại và phân phối khóa cặp, chuẩn 802.11i cũng định nghĩa trong RSN một cơ chế cho phép lưu đệm khóa cặp chính. Nguyên do là quá trình

xác thực và sinh ra khóa cặp chính mất tương đối nhiều thời gian và năng lực xử lý.

2.2.3.3. Mạng hỗn hợp

Mạng hỗn hợp là khái niệm trong 802.11i dùng để chỉ một mạng trong đó có nhiều thiết bị có khả năng mã hóa khác nhau. Để làm được điều đó, chuẩn 802.11i tạo ra một cây phân cấp các giao thức mã hóa, bắt đầu từ WEP 40-bit là yếu nhất, tiếp sau là WEP 104-bit, TKIP và CCMP. Và kết quả là ở bước liên kết đầu tiên, mỗi thiết bị sẽ tự thương lượng với điểm truy cập về giao thức mã hóa được áp dụng cho truyền thông unicast và broadcast. Tuy nhiên, có một hạn chế là khóa nhóm được sử dụng phải có cùng độ dài hoặc sử dụng cùng một giao thức mã hóa (của thiết bị có khả năng mã hóa yếu nhất trong mạng).

RSN cho phép hầu như bất kỳ tổ hợp các phương pháp mã hóa nào ngoại trừ một ngoại lệ là nếu thiết bị sử dụng CCMP cho thông tin broadcast thì bắt buộc phải hỗ trợ CCMP cho thông tin unicast. Tuy vậy, không phải trình điều khiển thiết bị nào cũng hỗ trợ cho tất cả các tổ hợp phương pháp mã hóa này.

2.2.3.4. Các pha hoạt động của RSN

Chuẩn 802.11i đặc tả quá trình hoạt động của RSN bao gồm 5 giai đoạn [8] như sau:

Pha 1. Phát hiện:

Thiết bị không dây gửi các thông điệp dò tìm (Probe) và dẫn đường (Beacon) để xác định điểm truy cập. Điểm truy cập sử dụng các thông điệp trả lời để thông báo chính sách an ninh 802.11i mà nó áp dụng. Thiết bị thực hiện liên kết tới điểm truy cập với thuật toán mã hóa và xác thực mà nó được thông báo.

Pha 2. Xác thực

Trong pha này, cả điểm truy cập và thiết bị tham gia vào quá trình xác thực để chứng tỏ định danh của mình.

Pha 3. Sinh và phân phối khóa

Sau quá trình xác thực, điểm truy cập và thiết bị thực hiện việc sinh và đồng bộ các cây phân cấp khóa.

Pha 4. Truyền dữ liệu đã mã hóa

Các khung tin truyền giữa điểm truy cập và thiết bị được mã hóa sử dụng khóa sinh ra sau pha xác thực.

Pha 5. Ngắt kết nối

Khi muốn ngắt kết nối, thiết bị trao đổi thông điệp tới điểm truy cập yêu cầu ngắt kết nối. Điểm truy cập có thể thực hiện xóa toàn bộ cây phân cấp khóa liên quan tới thiết bị hoặc giữ lại phục vụ cho mục đích lưu đệm khóa.

2.2.4. Những điểm yếu an ninh của 802.11i

Chuẩn 802.11i xây dựng một khung an ninh chuẩn cho mạng 802.11 nhằm mục đích nâng cao khả năng bảo mật cũng như khắc phục những điểm yếu mà chuẩn WEP đã gặp phải. Tuy vậy, giống như mọi giải pháp an ninh khác, 802.11i cần một thời gian dài để minh chứng được khả năng an ninh của nó. Nội dung phần này sẽ trình bày một số kết quả của các nghiên cứu về 802.11i.

Trong [23], ba tác giả chỉ ra rằng khóa phiên được sử dụng để mã hóa trong TKIP hoàn toàn có thể thu được nếu như lấy được nhiều hơn 2 khóa RC4 (được sinh ra với cùng một giá trị của 32 bit đầu trong TKIP IV). Với bộ xử lý sử dụng có tốc độ 2.53 Ghz, và 4 khóa RC4 thử nghiệm, thực nghiệm của các tác giả cho thấy sau 7 phút, kẻ tấn công có thể thu được khóa phiên. Tuy vậy các tác giả cũng chưa chỉ ra cách làm thế nào để thu được nhiều hơn 1 khóa RC4 với cùng một giá trị của 32 bit đầu trong TKIP IV.

Ta biết rằng trong TKIP, khóa cặp chính được cung cấp bởi máy chủ xác thực hoặc được cấu hình sẵn ở điểm truy cập và thiết bị (chế độ khóa chia sẻ trước PSK). Chế độ sử dụng PSK mặc dù cho phép đơn giản hóa việc triển khai TKIP trên phạm vi nhỏ, nhưng khả năng an toàn lại không cao hơn WEP [24], [15]:

- Nếu ở ngay bên trong mạng, sử dụng PSK và giá trị địa chỉ MAC nguồn, đích và hai giá trị nonce thu được nhờ nghe lén thông tin trên mạng, kẻ tấn công có thể sinh ra khóa phiên PTK và từ đó giải mã thông tin truyền thông của các thiết bị khác.
- Trường hợp không biết giá trị PSK, kẻ tấn công có thể thực hiện tấn công bằng phương pháp sử dụng từ điển ngoại tuyến. Theo đó, sử dụng một từ

điển các passphrase đã biết, kẻ tấn công sinh ra danh sách các PMK có thể và thực hiện dò tìm cho đến khi tìm được passphrase đúng. Đây là một phương pháp tấn công truyền thống bởi đặc điểm của người sử dụng là hay lựa chọn các cụm từ phổ dụng, dễ nhớ làm mật mã.

Bên cạnh đó, việc sử dụng mã Michael làm mã toàn vẹn cho thông điệp cũng không đảm bảo được khả năng giả mạo khung tin. Tác giả Seberry [16] đã chứng minh rằng không gian mã MIC mà thuật toán tạo ra là xung đột. Nghĩa là với hai thông điệp khác nhau, thuật toán Michael cho ra hai mã toàn vẹn giống nhau. Thêm vào đó, tác giả cũng đề xuất một phương pháp xây dựng một bảng các giá trị cố định mà theo đó, nếu giá trị đầu ra của thuật toán nằm trong bảng này, việc giả mạo gói tin mà mã Michael không thay đổi là có thể.

Chế độ mạng hỗn hợp trong 802.11i cho phép kẻ tấn công thực hiện kiểu tấn công quay lui mức độ an ninh (Security Level Rollback attack). Một ví dụ điển hình là kẻ tấn công có thể giả mạo điểm truy cập, gửi các khung tin dẫn đường giả mạo tới thiết bị thông báo rằng chỉ hỗ trợ giao thức WEP. Hoặc ngược lại, kẻ tấn công giả mạo thiết bị và gửi thông điệp dò tìm hoặc yêu cầu liên kết theo cách như vậy tới điểm truy cập. Kết quả là mặc dù cả điểm truy cập và thiết bị có thể hỗ trợ các giải pháp an ninh cao hơn WEP, chúng vẫn kết nối với nhau sử dụng WEP. Từ đó, kẻ tấn công thực hiện tấn công vào WEP.

2.3. WPA / WPA2

Chuẩn WPA (Truy cập Wi-Fi có bảo vệ) được liên minh Wi-Fi đề xuất (2002) nhằm tạo ra một giải pháp an ninh tạm thời cho mạng không dây trong điều kiện WEP thì quá yếu còn 802.11i vẫn đang trong giai đoạn xây dựng. Về thực chất, chuẩn WPA là một tập con của RSN, sử dụng phương pháp mã hóa TKIP thay thế cho WEP.

Sau khi chuẩn 802.11i ra đời (2004), nhận thấy trong đặc tả có nhiều giải pháp nhằm hỗ trợ cho cả các thiết bị phần cứng cũ, hiệp hội WiFi một lần nữa cho ra đời chuẩn WPA2 mới (2006) những yêu cầu chặt chẽ hơn 802.11i với các thiết bị áp dụng nó. Cụ thể là WPA2 yêu cầu các thiết bị không dây phải hỗ trợ một trong hai kiểu xác thực PSK hoặc xác thực dựa trên 802.1X (hai kiểu xác thực này sẽ được

trình bày chi tiết trong chương 3), đồng thời các thiết bị không dây phải sử dụng phương pháp CCMP để đảm bảo an toàn và toàn vẹn dữ liệu dữ liệu. Do đó cũng giống WPA, WPA2 là một tập con của chuẩn 802.11i.

2.4. Các giải pháp khác

Bên cạnh đó, các giải pháp an ninh khác dành cho mạng hữu tuyến cũng được áp dụng hoặc được sửa đổi để áp dụng vào mạng không dây như: mạng riêng ảo (VPN), Ipsec, SSH, hệ thống phát hiện xâm nhập (IDS)… Các giải pháp này một mặt thường hoạt động ở tầng trên so với tầng liên kết dữ liệu, mặt khác đòi hỏi nhiều chi phí để triển khai nên khó thích hợp cho việc triển khai rộng rãi. Tuy vậy, chúng vẫn được các tổ chức sử dụng như là các biện pháp tăng cường.

2.5. Tổng kết

Chương này đã giới thiệu các giải pháp an ninh chủ yếu được áp dụng cho mạng 802.11. Việc tập trung đi sâu vào nghiên cứu các phương pháp mã hóa và đảm bảo tính toàn vẹn trong các phương pháp này nhằm đưa ra một cái nhìn tổng quát về quá trình phát triển cũng như cải tiến của các phương pháp này. Trong đó, chuẩn an ninh WEP được coi là không đủ để đảm bảo an ninh cho mạng 802.11, chuẩn TKIP được đưa ra như một giải pháp chuyển đổi trong khi chờ các phần cứng 802.11 cũ được nâng cấp để hỗ trợ cho CCMP. Giải pháp CCMP được đưa như một giải pháp mới, toàn diện để tránh những rủi ro kế thừa từ chuẩn WEP – điều mà TKIP vẫn bị ảnh hưởng. CCMP sử dụng thuật toán mã hóa AES để mã hóa dữ liệu và thuật toán CBC-MAC để tính toán và kiểm tra tính toàn vẹn của dữ liệu - là hai thuật toán đã đạt được niềm tin trong cộng đồng bảo mật về tính an toàn của chúng.

Tuy nhiên, để có thể thực hiện được quá trình mã hóa/giải mã và tính toán toàn vẹn, cần phải có một phương pháp an toàn để vận chuyển khóa PMK tới cả hai phía để chúng có thể thực hiện việc sinh và đồng bộ cây phân cấp khóa. Phương pháp khóa chia sẻ trước (PreShared Key) được 802.11i đưa ra nhằm áp dụng cho các mạng có quy mô nhỏ. Đối với các mạng quy mô lớn, 802.11i sử dụng phương pháp xác thực dựa trên 802.1X, qua đó khóa bí mật sẽ được chuyển tới hai phía thay vì được cấu hình tĩnh ở cả hai phía.

Với lý do đó, chương tiếp theo sẽ đi nghiên cứu các phương pháp xác thực

được áp dụng cho mạng 802.11 với nội dung tập trung sâu vào phương pháp xác thực dựa trên 802.1X. Trên cơ sở đó, ở chương cuối chúng ta sẽ nghiên cứu, đánh giá các mặt còn tồn tại đối với việc đảm bảo an ninh cho mạng 802.11 rồi từ đó đề xuất một mô hình mạng WLAN an toàn với những yêu cầu cụ thể.

CHƯƠNG 3. XÁC THỰC TRONG WLAN 802.11

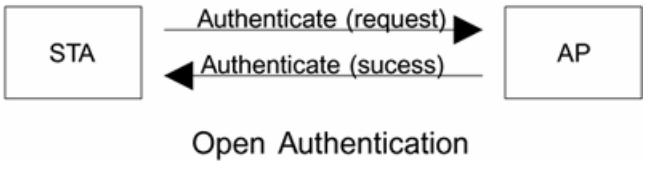
Để đảm bảo an ninh cho mạng không dây, bên cạnh giải pháp mã hóa nhằm đảm bảo thông tin không bị lộ trên đường truyền, phương pháp xác thực được sử dụng để cấp quyền truy cập vào mạng cho các trạm trước khi tham gia truyền thông. Đặc điểm chung của các phương pháp xác thực là trong pha kết nối, các trạm phải cung cấp các nhận dạng số cho điểm truy cập để chứng minh rằng nó có đủ điều kiện để tham gia vào truyền thông.

Các phương pháp xác thực áp dụng cho 802.11 là các phương pháp xác thực một chiều, nghĩa là chỉ có các trạm cần được xác thực. Khi kết nối vào một điểm truy cập, trạm mặc nhiên coi điểm truy cập là hoàn toàn tin cậy hay là điểm truy cập mặc nhiên đã được xác thực bởi trạm không dây.

3.1. Xác thực trong chuẩn 802.11 ban đầu

Đặc tả IEEE 802.11 ban đầu cung cấp hai phương pháp xác thực cho các trạm không dây là: Xác thực mở (Open Authentication) và Xác thực khóa chia sẻ (Shared Key Authentication).

Trong đó, phương pháp xác thực mở thực chất là một phương thức xác thực rỗng hay hoàn toàn không có xác thực. Mặc dù có vẻ vô nghĩa nhưng phương pháp xác thực mở vẫn được đưa vào trong đặc tả 802.11 bởi lý do là phương pháp xác thực phải cho phép trạm kết nối vào mạng một cách nhanh chóng. Ở phương pháp này, trạm không dây sẽ gắn địa chỉ MAC của mình vào trong thông điệp yêu cầu xác thực. Phía điểm truy cập, khi nhận được thông điệp này sẽ chấp nhận cho trạm được phép truy cập mạng, đồng thời gửi thông điệp thông báo xác thực thành công tới trạm.

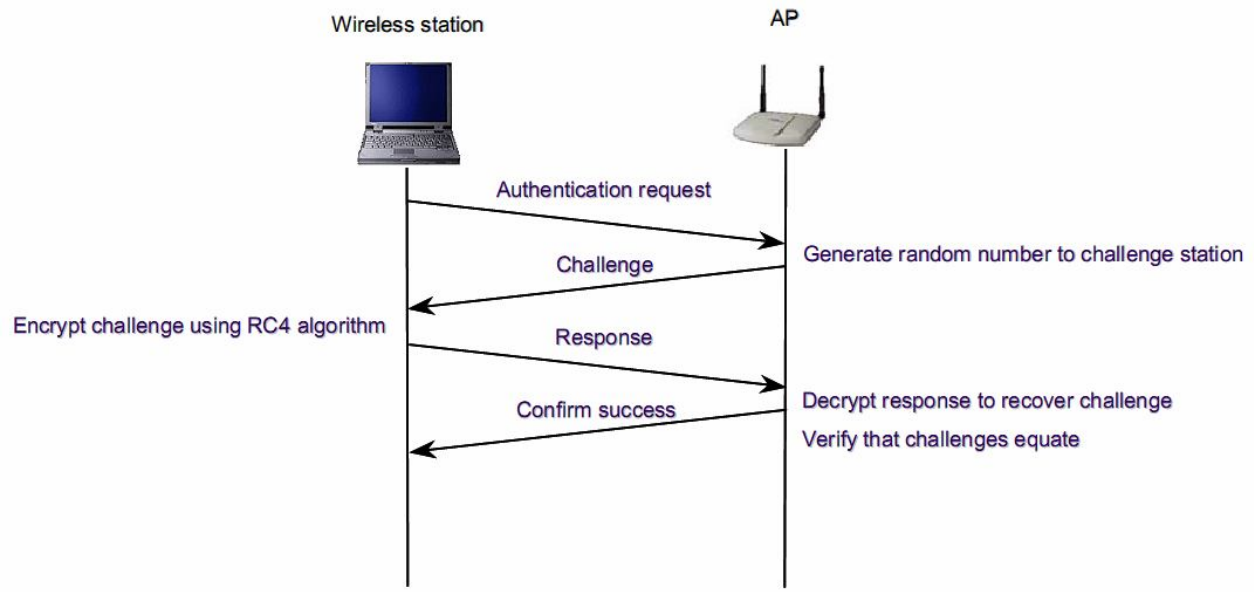


Hình 3-1. Xác thực mở

Khác với phương pháp xác thực mở, phương pháp xác thực khóa chia sẻ áp dụng phương pháp mã hóa WEP vào trong quá trình xác thực, trong đó yêu cầu cả

hai phía (điểm truy cập và trạm) đều phải hỗ trợ WEP và có cùng các khóa WEP chung. Khi đó, quá trình xác thực được diễn ra như sau:

- Trạm gửi thông điệp yêu cầu xác thực bằng phương pháp khóa chia sẻ tới điểm truy cập
- Điểm truy cập gửi lại thông điệp thánh thức với nội dung không mã hóa
- Trạm thực hiện mã hóa thông điệp thách thức bằng khóa WEP mà nó có và gửi lại cho điểm truy cập.
- Khi nhận được thông điệp trả lời, điểm truy cập thực hiện giải mã bằng khóa WEP của nó. Nếu như điểm truy cập (sau quá trình giải mã) thu lại được nội dung thông điệp thách thức nó đã gửi đi, nó sẽ gửi thông điệp báo thành công và cho phép trạm được truy cập vào mạng không dây.



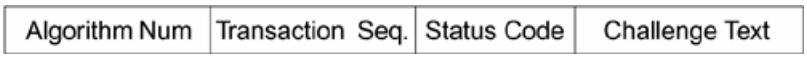
Hình 3-2. Xác thực khóa chia sẻ (Xác thực WEP)

Có thể thấy có nhiều loại thông điệp được sử dụng phục vụ cho quá trình xác thực trong đặc tả 802.11. Tuy nhiên các thông điệp này đều có chung một định dạng bao gồm 4 trường:

- Trường số hiệu thuật toán chỉ định loại xác thực được sử dụng với giá trị 0 dành cho xác thực mở còn 1 dành cho xác thực WEP.
- Trường thứ tự giao dịch xác định vị trị trong quá trình xác thực. Thông điệp đầu được đặt giá trị 1, thông điệp thứ 2 được đặt giá trị 2, còn thông điệp

dùng với WEP được đặt giá trị 3.

- Trường mã trạng thái được thiết lập trong thông điệp cuối cùng nhằm xác định sự thành công hay thất bại của quá trình xác thực.
- Trường thách thức (chỉ dùng cho xác thực WEP) lưu nội dung văn bản thách thức.



Hình 3-3. Cấu trúc thông điệp xác thực

Giống như giải pháp mã hóa WEP, xác thực trong đặc tả 802.11 cũng vấp phải những điểm yếu an ninh cần khắc phục:

Thứ nhất, phương pháp xác thực mở về bản chất không phải là phương pháp xác thực bởi ở phương pháp này điểm truy cập chấp nhận mọi trạm muốn truy cập.

Thứ hai, độ an toàn do phương pháp xác thực khóa chia sẻ mang lại thực chất không cao hơn phương pháp đầu là mấy. Mặc dù đã áp dụng kỹ thuật mã hóa vào trong quá trình, kẻ tấn công vẫn có thể tấn công vào phương pháp này. Bởi môi trường không dây là môi trường hoàn toàn mở, thêm vào đó, bản chất của mã hóa WEP là phép toán XOR (chương 2), nên kẻ tấn công chỉ sử dụng một công cụ nghe lén để lấy được thông điệp thách thức và thông điệp trả lời, thực hiện XOR chúng lại với nhau là thu được khóa WEP được chia sẻ giữa điểm truy cập và trạm. Từ khóa WEP thu được này, kẻ tấn công không những chỉ thực hiện đăng nhập vào mạng mà còn thể sử dụng khóa này để giải mã các thông tin được mã hóa sau đó.

3.2. Xác thực dựa trên địa chỉ MAC

Phương pháp xác thực dựa trên địa chỉ MAC tuy không được chỉ ra trong đặc tả 802.11 ban đầu nhưng được hỗ trợ bởi rất nhiều nhà sản xuất thiết bị phần cứng. Nguyên tắc chính của phương pháp này là điểm truy cập (bên xác thực) lưu trữ một danh sách các địa chỉ MAC được phép truy cập vào mạng. Mỗi khi nhận được một yêu cầu xác thực, nó thực hiện so sánh địa chỉ MAC thu được với danh sách: nếu như địa chỉ MAC thuộc vào danh sách được phép, trạm mới được phép kết nối vào mạng không dây. Phương pháp này được đưa ra nhằm tăng cường cho cả hai phương pháp xác thực cung cấp bởi đặc tả 802.11 ban đầu.

Về nguyên tắc, địa chỉ MAC được gán cho mỗi giao diện mạng trong quá trình sản xuất là duy nhất. Tuy nhiên, chuẩn 802 vẫn cho phép người sử dụng có thể thiết đặt địa chỉ MAC cục bộ để sử dụng thay vì địa chỉ MAC toàn cục đã được gắn cứng cho giao diện mạng. Nhờ vậy, sử dụng một công cụ nghe lén và phân tích gói tin, kẻ tấn công có thể xác định được địa chỉ MAC nào được phép truy cập mạng, sau đó chờ cho tới khi trạm ngưng kết nối khỏi mạng để giả mạo MAC và kết nối vào mạng không dây một cách hợp pháp.

3.3. Xác thực trong chuẩn 802.11i

Rõ ràng rằng, kiến trúc xác thực trong đặc tả 802.11 ban đầu không đủ để xác thực một trạm muốn tham gia vào mạng. Nguyên do là kiến trúc xác thực này thiếu những thành phần chính yếu tạo nên một kiến trúc xác thực hiệu quả bao gồm:

- Xác thực dựa trên người dùng và tập trung
- Sử dụng các khóa mã hóa động
- Quản lý khóa mã hóa
- Xác thực hai phía

Xác thực dựa trên người dùng đóng vai trò quan trọng trong an ninh mạng. Bởi xác thực dựa trên thiết bị không thể nào phát hiện và ngăn cản người dùng trái phép sử dụng các thiết bị đã được xác thực. Và việc quản lý tập trung dựa trên người dùng cho phép xác thực một cách hiệu quả, không phụ thuộc vào thiết bị mà người dùng đó sử dụng.

Thêm vào đó, nhu cầu về xác thực dựa trên người dùng lại nảy sinh một vấn đề: sử dụng khóa mã hóa dựa trên người dùng. Cách xác thực loại này một mặt phù hợp với mô hình quản lý và an ninh của mạng không dây, mặt khác làm giảm bớt gánh nặng của người quản trị trong việc quản lý khóa. Theo đó, với từng người dùng, khóa được sinh ra và hủy mỗi khi người sử dụng thực hiện xác thực và ngắt kết nối khỏi mạng.

Vấn đề xác thực hai phía nảy sinh từ quan điểm: không chỉ người dùng có thể giả mạo mà mạng không dây cũng có thể giả mạo. Theo đó, không những điểm truy

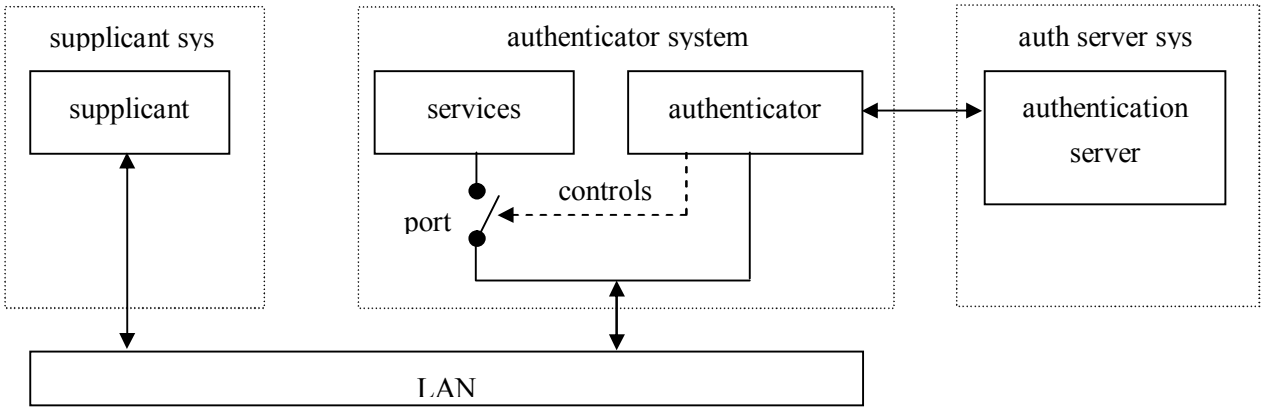
cập thực hiện xác thực trạm mà ngược lại trạm cũng thực hiện xác thực cả điểm truy cập để hai bên có thể chắc chắn rằng phía bên kia là hợp lệ.

Để giải quyết những vấn đề về xác thực trong đặc tả 802.11 ban đầu, chuẩn IEEE 802.11i đã kết hợp chuẩn 802.1X cùng khung xác thực EAP vào trong như một thành phần của RSN phục vụ cho quá trình xác thực.

3.3.1. Chuẩn 802.1X

IEEE 802.1X là giao thức điều khiển truy cập dựa trên cổng (port-based) với mục đích là cho phép thực hiện việc điều khiển truy cập tại nơi người dùng liên kết vào mạng. Mạng 802.1X điển hình bao gồm 3 thực thể tham gia vào quá trình xác thực:

- Người dùng (Supplicant) – thực thể muốn tham gia vào mạng
- Bộ xác thực (Authenticator) – thực thể thực hiện việc điều khiển truy cập
- Máy chủ xác thực (Authentication Server) – thực thể thực hiện quá trình xác thực người dùng.



Hình 3-4. 802.1X framework

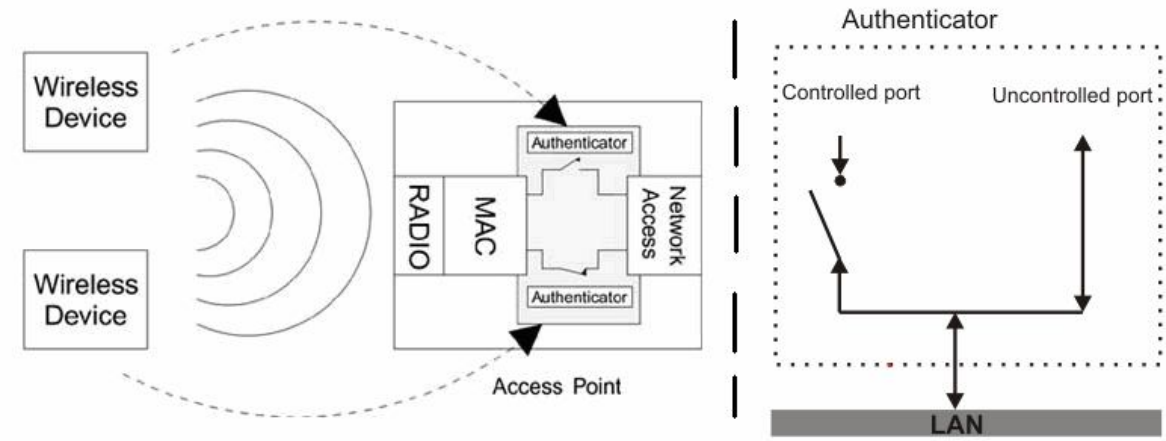
Cổng (port) là khái niệm dùng để chỉ nơi người dùng kết nối vào mạng. Khái niệm này được sử dụng bởi 802.1X ra đời trước 802.11 nhằm phục cho mạng không dây cục bộ (LAN). Theo đó, với mỗi người dùng sẽ có một cổng được quản lý bởi một bộ xác thực.

Về mặt hình thức, cách hoạt động của 802.1X tương đối đơn giản: Các cổng ban đầu ở trạng thái mở (open). Mỗi khi người dùng kết nối vào một cổng, bộ xác thực sẽ kiểm tra và chuyển cổng sang trạng thái đóng (nếu người dùng được phép

truy cập). Khi đó, người dùng mới có khả năng gửi gói tin xác thực tới máy chủ xác thực. Máy chủ xác thực tiếp đó sẽ thực hiện việc xác thực người dùng. Việc truyền thông giữa người dùng, bộ xác thực được thực hiện nhờ giao thức EAPOL (EAP over LAN) [27].

Giao thức EAPOL được định nghĩa trong chuẩn 802.1X nhằm định ra cách truyền thông các thông điệp EAP trên mạng LAN. Về thực chất, EAPOL định nghĩa cách đóng gói thông điệp EAP trong các khung tin tầng liên kết dữ liệu. Tuy vậy chuẩn 802.1X không định nghĩa cách thức chuyển các thông điệp EAP giữa bộ xác thực và máy chủ xác thực. Trong mạng LAN sử dụng giao thức TCP/IP, máy chủ xác thực RADIUS (dịch vụ người dùng quay số truy cập từ xa) được sử dụng rộng rãi và phổ biến. Để gửi/nhận các thông điệp xác thực tới máy chủ RADIUS, bộ xác thực sử dụng giao thức EAP-over-Radius [29].

Khi áp dụng 802.1X vào mạng không dây WLAN, điểm truy cập sẽ đóng vai trò bộ xác thực, tạo ra các cổng logic và quản lý trạng thái của các cổng này. Mỗi khi, có một trạm tham gia vào mạng, điểm truy cập sẽ gán cho nó hai cổng: cổng bị điều khiển và cổng không bị điều khiển. Quá trình xác thực sẽ được diễn ra thông qua cổng không bị điều khiển, các luồng thông tin khác sẽ được chuyển thông qua cổng bị điều khiển. Tuy nhiên, điểm truy cập sẽ chặn cổng này lại cho đến khi quá trình xác thực diễn ra thành công.



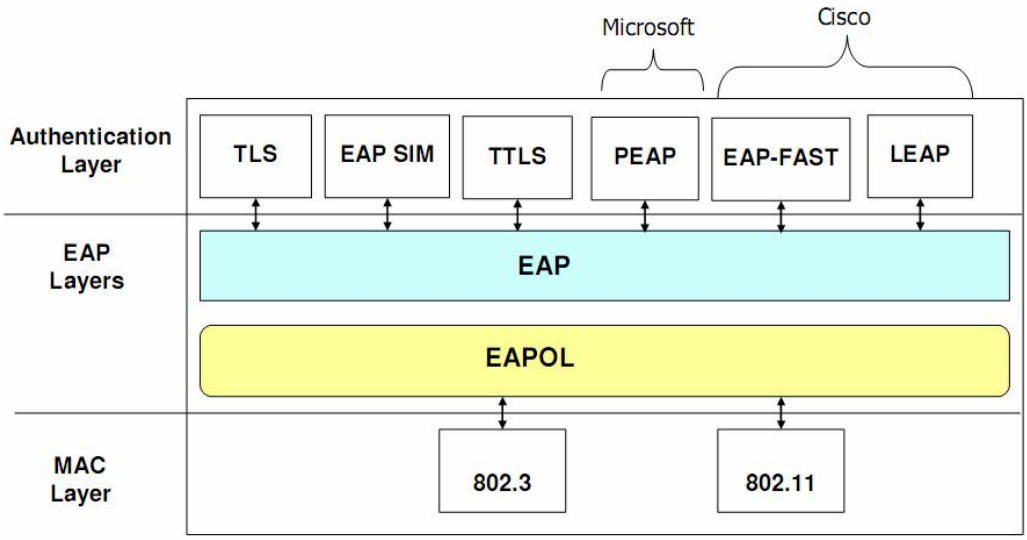
Hình 3-5. Cổng 802.1X logic trong điểm truy cập

Cần chú ý rằng, ở đây máy chủ xác thực không nhất thiết phải là một máy chủ riêng (chẳng hạn: máy chủ Radius,…) mà có thể là một tiến trình nhỏ trong điểm truy cập làm nhiệm vụ quản lý danh sách người dùng/mật khẩu phục vụ quá trình

xác thực.

3.3.2. Giao thức xác thực mở rộng (EAP)

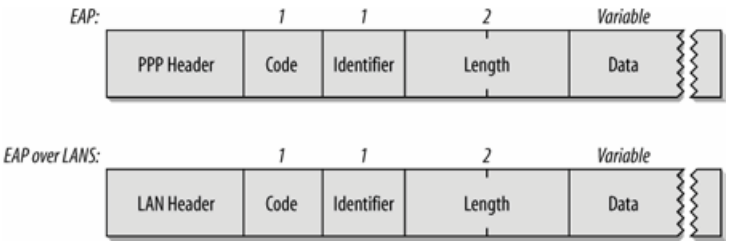
EAP được sử dụng trong quá trình xác thực của 802.11 RSN có sử dụng chuẩn điều khiển truy cập 802.1X. Về bản chất EAP không phải là một giao thức xác thực mà là một khung hoạt động cho phép áp dụng nhiều phương pháp trên đó [27]. Đặc tả EAP không quy định rõ cơ chế xác thực nào được sử dụng trên đó. Nói cách khác, EAP là một bộ bao gói cho phép hoạt động trên mọi kiểu tầng liên kết dữ liệu.



Hình 3-6. Kiến trúc EAP áp dụng cho LAN và WLAN

RSN không quy định sử dụng EAP với phương pháp xác thực nào cụ thể, tuy vậy, hiệp hội WiFi quy định sử dụng một vài phương pháp xác thực EAP (chẳng hạn EAP-TLS) các thiết bị hỗ trợ WPA/WPA2.

Hình vẽ bên dưới mô tả cấu trúc khung tin EAP hoạt động trên tầng liên kết dữ liệu của giao thức PPP và giao thức mạng LAN.



Hình 3-7. Cấu trúc khung tin EAP

Trong đó:

- Trường Code (mã) có độ dài 1 byte dùng để định nghĩa kiểu của gói tin EAP.

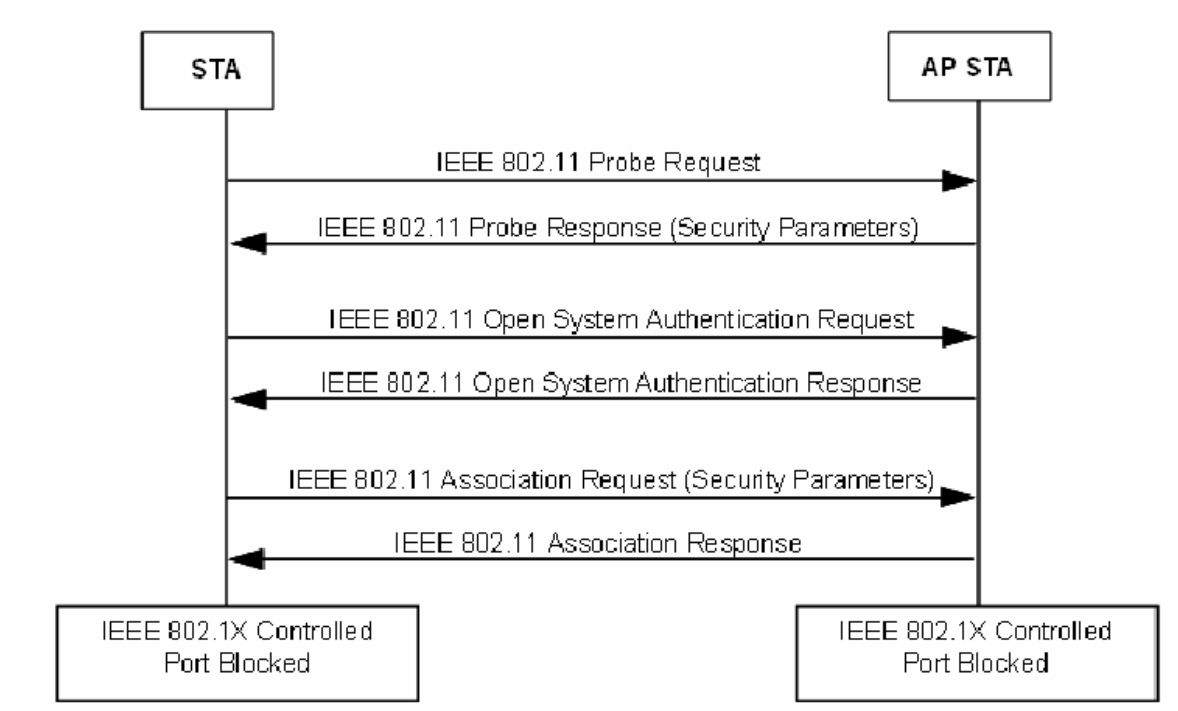
- Trường Identifier (số định danh) có độ dài 1 byte dùng để lưu giá trị nguyên không dấu sử dụng để đồng bộ giữa hai thông điệp yêu cầu và trả lời.
- Trường Length (độ dài) có kích thước 2 byte chứa kích thước của toàn bộ gói tin ngoài trừ phần mào đầu (header).
- Trường Data (dữ liệu) có độ dài biến thiên lưu thông tin phục vụ quá trình xác thực.

3.3.2. Xác thực trong WLAN dựa trên 802.1X

Như trên đã trình bày, chuẩn 802.11i dựa trên để quản lý luồng thông tin giữa hệ thống phân phối và trạm không dây thông qua mô hình cổng bị điều khiển/không bị điều khiển của 802.1X. Quá trình xác thực này kết hợp với quá trình bắt tay 4-bước và bắt tay nhóm (đã trình bày ở trên) để thực hiện việc thiết lập và đồng bộ các khóa mã hóa.

Để quá trình xác thực thông qua 802.1X có thể diễn ra, các trạm cần thiết lập liên kết với điểm truy cập. Quá trình này diễn ra như sau:

- Các trạm thực thực hiện dò tìm các thông số an ninh của điểm truy cập thông qua việc dò tìm bị động (dựa trên các khung tin Dẫn đường) hoặc dò tìm chủ động (thông qua các khung tin Dò tìm).
- Tiếp đó, các trạm thực hiện việc xác thực với điểm truy cập dựa trên cơ chế xác thực mở.
- Cuối cùng, các trạm thực hiện việc liên kết với điểm truy cập thông qua việc trao đổi các gói tin liên kết (Association frame).



Hình 3-8. Quá trình thiết lập liên kết

Sau quá trình thiết lập liên kết, khi xác định được mạng yêu cầu xác thực dựa trên 802.1X và EAP, điểm truy cập sẽ gửi thông điệp EAP-Request hoặc trạm sẽ gửi thông điệp EAP-Start để bắt đầu quá trình xác thực bằng EAP.

Với giả thiết máy chủ RADIUS được sử dụng làm máy chủ xác thực, quá trình xác thực trong WLAN dựa trên 802.1X diễn ra như sau:

1. Trạm gửi gói tin EAPOL-Start tới điểm truy cập. (Bước này là tùy chọn)

2. Điểm truy cập gửi khung tin EAP-Request/Identity thông báo với trạm rằng cần phải xác thực 802.1X.

3. Trạm trả lời với khung tin EAP-Response/Identity. Khung tin này sẽ được chuyển tiếp tới máy chủ Radius với vai trò khung tin Radius-Access-Request.

4. Máy chủ Radius gửi gói tin EAP-Request xác định phương pháp xác thực. Gói tin này được bao gói trong khung tin Radius-Access-Challenge gửi tới điểm truy cập. Điểm truy cập sẽ chuyển tiếp khung tin EAP-Request tới trạm. Khung tin EAP-Request thông thường được gọi là EAP-Request/Method trong đó Method là phương pháp EAP được sử dụng (chẳng hạn PEAP, EAP-TLS).

5. Trạm nhận thông tin trả lời từ người dùng (ví dụ: tên/mật khẩu) và trả lời bằng khung tin EAP-Response. Khung tin này sẽ được điểm truy cập chuyển

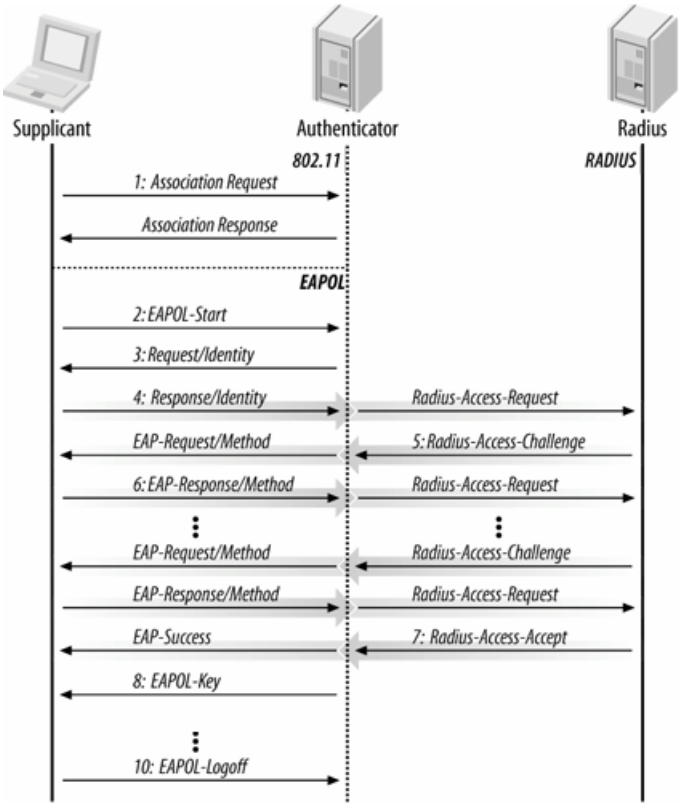
thành gói tin Radius-Access-Request với nội dung thách thức được kèm trong thân gói tin.

Bước 4 và 5 có thể phải lặp đi lặp lại nhiều lần để hoàn tất quá trình xác thực. Khóa cặp chính cũng được chuyển tới điểm truy cập và trạm trong quá trình này.

6. Máy chủ RADIUS gửi gói tin RADIUS-Access-Accept thông báo xác thực thành công. Điểm truy cập sẽ chuyển tiếp gói tin này thành gói tin EAP-Success chuyển tới trạm đồng thời chuyển trạng thái của cổng sang đã xác thực.

7. Ngay sau khi nhận được gói tin Radius-Access-Accept, điểm truy cập thực và trạm thực hiện quá trình bắt tay 4-bước để sinh cây phân cấp khóa thông qua các thông điệp EAPOL-Key. (Bước này không xảy ra khi áp dụng 802.1X cho WEP).

8. Khi muốn ngắt kết nối khỏi mạng, trạm gửi gói tin EAPOL-Logoff tới điểm truy cập. Cổng logic tương ứng sẽ được chuyển sang trạng thái chưa xác thực.



Hình 3-9. Quá trình xác thực dựa trên 802.1X

3.3.3. Xác thực trong chế độ khóa chia sẻ trước

Bên cạnh việc sinh và phân phối khóa dựa trên 802.1X, kiến trúc RSN trong 802.11i định nghĩa một phương pháp khác gọi là khóa chia sẻ trước (PSK). Ở chế độ này, khóa cặp chính thay vì được sinh và phân phối bởi máy chủ xác thực, nó được cấu hình sẵn ở cả hai phía.

Trong chế độ này, sau khi quá trình thiết lập liên kết diễn ra, cả trạm và điểm truy cập sẽ tiến hành quá trình sinh và đồng bộ khóa dựa trên các thông điệp EAP-Key và khóa cặp chính (được sinh từ PSK) (hình 2-14). Sau đó, cả hai phía sẽ tiến hành truyền thông an toàn sử dụng cây phân cấp khóa đã được sinh.

3.4. Tổng kết

Chương này đã trình bày và giới thiệu các phương pháp xác thực được áp dụng trong mạng WLAN. Trong đó xác thực thông qua 802.1X cho phép thực hiện việc xác thực dựa trên người dùng, điều không có được ở các phương pháp trước đó trong chuẩn 802.11. Việc xác thực dựa trên người dùng là phương pháp xác thực được sử dụng phổ biến hiện nay bởi xác thực dựa trên thiết bị là có điểm yếu là thiết bị có những thông số cố định gắn liền rất dễ cho kẻ tấn công giả mạo.

Bên cạnh đó, cơ chế xác thực dựa trên 802.1X đã cung cấp một cách thức phân phối khóa bí mật tới điểm truy cập và trạm không dây một cách an toàn, giải quyết được vấn đề cấu hình tĩnh khóa như trong cơ chế WEP. Thêm vào đó, khóa được sinh ra bởi máy chủ xác thực là động với từng người dùng cụ thể sau khi đã được xác thực nên cho dù kẻ tấn công có thể tấn công được vào khóa của một người dùng thì cũng khó có thể tấn công vào dữ liệu gửi của người dùng khác.

Tuy vậy, chuẩn 802.11i lại không chỉ rõ trong đặc tả của mình là phương pháp xác thực EAP nào sẽ được dùng để phục vụ cho quá trình xác thực. Điều đó dẫn tới là các nhà sản xuất thiết bị có thể áp dụng các phương pháp xác thực khác nhau, và nếu như không xem xét cẩn thận trong quá trình xây dựng sẽ có thể dẫn tới những rủi ro an ninh từ quá trình xác thực này.

Bên cạnh đó, giải pháp xác thực dựa trên 802.1X cũng bị yếu điểm khi gặp kiểu tấn công từ chối dịch vụ (DoS). Nguyên nhân là do các đặc tả an ninh cho

mạng WLAN 802.11 đã bỏ qua việc đảm bảo tính sẵn sàng cho mạng.

Do vậy, mục đích và nội dung của chương cuối cùng là đi xem xét những vấn đề an ninh trong mạng WLAN 802.11 liên quan đến kiểu tấn công DoS, phân tích và so sánh các giải pháp xác thực EAP đang được sử dụng phổ biến để từ đó có cơ sở xây dựng một mô hình mạng WLAN an toàn có khả năng giảm thiểu rủi ro từ kiểu tấn công DoS cũng như đảm bảo được an toàn dữ liệu truyền thông.

CHƯƠNG 4. HỆ THỐNG WLAN AN TOÀN

Trong chương 2 và 3, chúng ta đã tìm hiểu và phân tích các giải pháp an ninh dành cho 802.11, đặc biệt là chuẩn an ninh mới 802.11i trên các khía cạnh: toàn vẹn dữ liệu, tính bí mật và xác thực. Đó cũng chính là ba tiêu chí được tổ chức IEEE đặt ra khi xây dựng giải pháp an ninh cho mạng WLAN.

Tuy nhiên, trong an toàn dữ liệu nói chung, còn một tính chất cũng quan trọng không kém là tính sẵn sàng (availability). Tính sẵn sàng dùng để chỉ mức độ sẵn sàng đáp ứng dịch vụ của mạng cũng như các trạm tham gia vào mạng. Liên kết mạng phải được duy trì cho đến khi một trong các bên tham gia (hợp lệ) thực hiện yêu cầu ngắt kết nối. Về tính chất này, các chuẩn an ninh cho 802.11 khi được đặc tả đều không đề cập tới.

Thêm vào đó, chuẩn 802.11i trong quá trình triển khai vẫn tồn tại những rủi ro an ninh tiềm ẩn như lỗ hổng tấn công quay lui dịch vụ. Việc không định rõ cơ chế xác thực EAP nào được sử dụng cũng dẫn tới nhiều vấn đề: thứ nhất là sự không đồng bộ giữa các nhà sản xuất thiết bị, thứ hai là nếu áp dụng cơ chế xác thực EAP yếu sẽ khiến cho những cố gắng an ninh sau bước xác thực sẽ bị đổ vỡ. Một ví dụ điển hình cho vấn đề này là nếu khóa bí mật bị lộ trong quá trình xác thực, quá trình mã hóa về sau sẽ không còn ý nghĩa nữa.

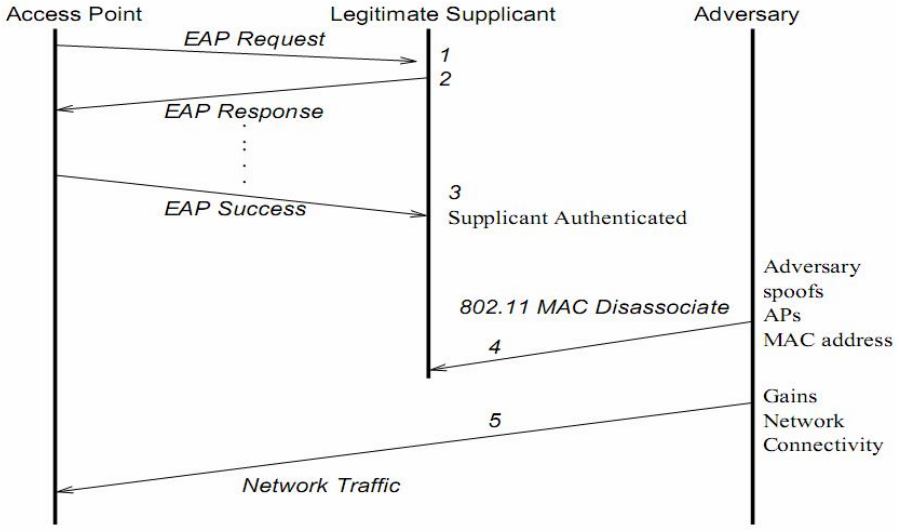
4.1. Tính sẵn sàng của 802.11i

Các nghiên cứu [14], [31], [32] đã chỉ ra rằng mạng WLAN 802.11 không đủ sức chống chọi lại với kiểu tấn công từ chối dịch vụ. Theo đó, kiểu tấn công này có thể được thực hiện một cách dễ dàng và rất khó để phát hiện với đặc tả 802.11 hiện tại.

4.1.1. Các kiểu tấn công DoS điển hình

Trong ba loại khung tin được sử dụng (khung tin quản lý, khung tin điều khiển và khung tin dữ liệu), chỉ có khung tin dữ liệu là được bảo vệ trong mạng 802.11. Từ tính chất đó kẻ tấn công có thể dễ dàng giả mạo hai kiểu khung tin này để thực hiện tấn công vào mạng.

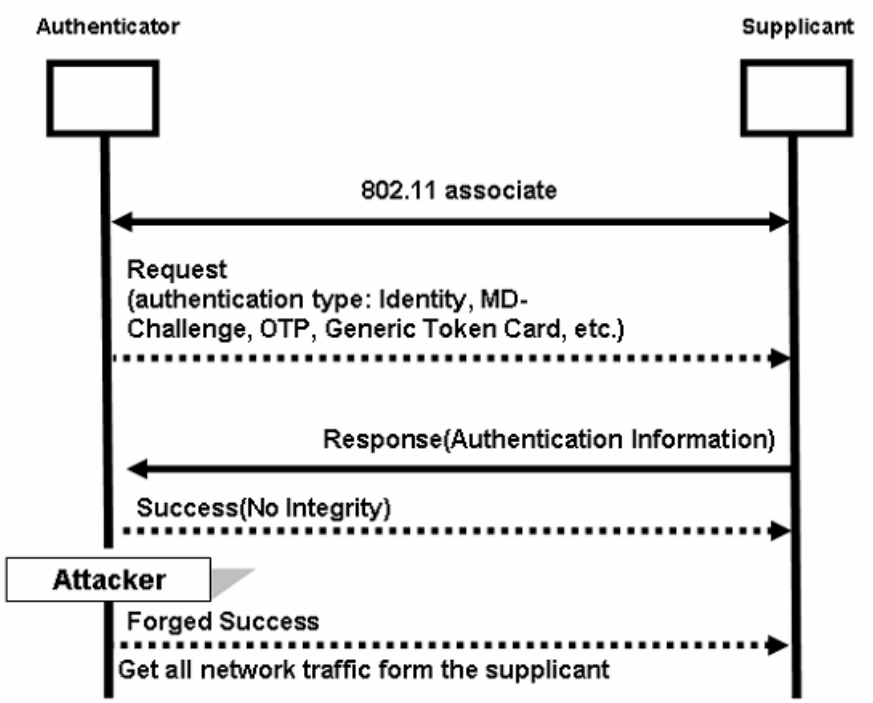
Điển hình trong các kiểu tấn công loại này là việc kẻ tấn công thực hiện giả mạo và liên tục gửi các khung tin ngắt liên kết (Disassociation) và khung tin ngừng xác thực (Deauthentication). Kiểu tấn công này còn có tên gọi là kiểu tấn công "cướp phiên" (session high-jacking) [31]. Như mô tả trong hình 4-1, kẻ tấn công giả mạo địa chỉ của điểm truy cập để gửi thông điệp ngắt liên kết (Disassociate) tới trạm thông báo liên kết đã bị hủy. Bằng cách tấn công kiểu này, kẻ tấn công thực hiện được hai mục đích: thứ nhất là làm gián đoạn hoặc hủy dịch vụ của người dùng, thứ hai là kế đó, kẻ tấn công có thể tiếp tục truyền thông với máy chủ bằng cách giả mạo địa chỉ MAC của trạm. Tất nhiên, để có thể truyền thông tiếp được trong mạng được bảo vệ bằng phương pháp mã hóa, kẻ tấn công còn phải biết được khóa được sử dụng để mã hóa. Kỹ thuật tấn công này cũng được sử dụng để tấn công lại các hệ thống có hỗ trợ xác thực hai chiều.



Hình 4-1. Tấn công bằng cách giả mạo gói tin ngắt liên kết

Bên cạnh đó, việc sử dụng một số thông điệp EAP không mã hóa giao thức xác thực 802.1X cũng cho phép một vài kiểu tấn công DoS được thực hiện. Cụ thể là kẻ tấn công có thể giả mạo thông điệp EAPOL-Start và gửi liên tục khiến cho việc xác thực 802.1X không thể thành công, giả mạo các thông điệp EAPOL-Failure và EAPOL-Logoff để ngắt kết nối từ trạm. Ngoài ra, kẻ tấn công còn có thể thực hiện giả mạo điểm truy cập thông qua việc giả mạo thông điệp EAP-Success. Hình 4.2 mô tả một ví dụ về việc giả mạo thông điệp EAP-Success. Nguyên nhân là do thông điệp này không được đảm bảo tính toàn vẹn. Do đó, kẻ tấn công thực hiện

sửa đổi thông điệp EAP-Success lấy được trong pha xác thực của một người dùng khác, rồi gửi thông điệp này tới người dùng hiện tại để đóng giả là một bộ xác thực hợp pháp. Từ đó, kẻ tấn công có thể nhận diện và can thiệp vào mọi dữ liệu được gửi đi từ người dùng.



Hình 4-2. Giả mạo thông điệp EAP-Success

Kẻ tấn công cũng có thể thực hiện kiểu tấn công làm suy kiệt tài nguyên của máy chủ xác thực. Cụ thể là, máy chủ xác thực phân bổ tài nguyên để xác thực người dùng trong khi không có một cơ chế nào kiểm tra tính hợp pháp của người dùng. Khi đó, người dùng hợp lệ có thể không truy cập được vào hệ thống bởi máy chủ xác thực đang dành hết tài nguyên để phục vụ xác thực kẻ tấn công. Đặc biệt là với phương pháp xác thực sử dụng khóa công cộng như EAP-TLS hoặc EAP-TTLS đòi hỏi nhiều năng lực tính toán và tài nguyên, kiểu tấn công này là khá hiệu quả.

4.1.2. Tấn công vào cơ chế phản ứng MIC

Thuật toán Michael được TKIP sử dụng làm phương pháp đảm bảo tính toàn vẹn cho các khung tin gửi đi. Với mức độ an ninh 20 bit, TKIP áp dụng thêm cơ chế phản ứng MIC nhằm chống lại các trường hợp giả mạo mã MIC. Như trong chương 2 đã trình bày, khi cơ chế này được áp dụng, kẻ tấn công phải mất khoảng thời gian là 6 tháng mới có thể tạo ra được một khung tin có mã MIC giả mạo là hợp lệ. Tuy

nhiên, cơ chế này lại khiến cho TKIP không đảm bảo được tính sẵn sàng của dữ liệu. Trong [14], hai tác giả đã chỉ ra rằng cơ chế phản ứng khi mã MIC sai áp dụng trong thuật toán TKIP cũng gặp phải những rủi ro khi đối mặt với kiểu tấn công DoS. Theo các tác giả, bằng việc sử dụng các phần cứng (các ăng ten chuyên dụng), kẻ tấn công có thể lấy được gói tin trước khi nó được truyền tới đích. Khi đó, bằng việc giữ nguyên trường TSC và thay đổi một vài bit trong gói tin sao cho hai giá trị FCS và ICV vẫn thỏa mãn (dựa vào lỗ hổng của thuật toán CRC), kẻ tấn công thu được một gói tin mới với TSC, FCS và ICV thỏa mãn điều kiện của TKIP nhưng mã MIC đã bị sửa đổi. Cách làm của cơ chế phản ứng MIC là sau hai lần gặp mã MIC sai sẽ tạm thời ngắt liên lạc giữa trạm và điểm truy cập trong 60 giây. Bằng cách gửi 2 lần gói tin đã sửa đổi , kẻ tấn công hoàn toàn có thể làm ngừng liên kết của trạm.

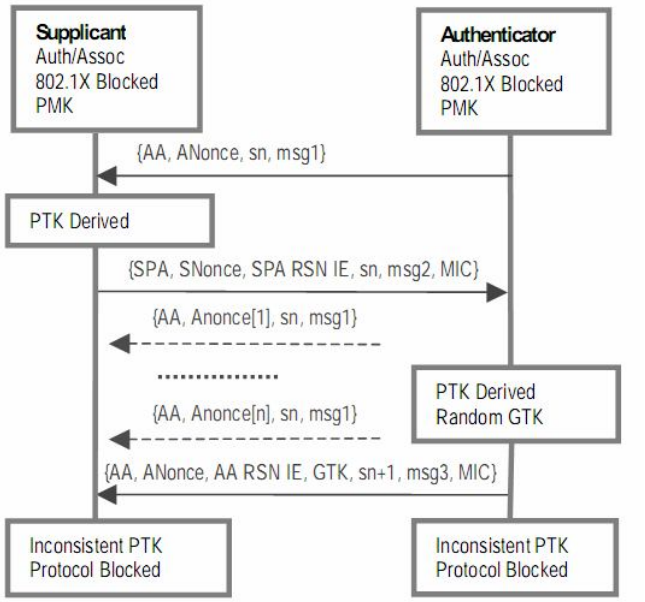
Tuy nhiên, cách làm này đòi hỏi kẻ tấn công phải đầu tư nhiều chi phí và công sức. Ngoài ra, khi áp dụng CCMP thay thế cho TKIP thì cách tấn công kiểu này là không thể thực hiện được.

4.1.3. Tấn công vào quá trình bắt tay 4-bước

Quá trình bắt tay 4-bước là một thành phần quan trọng trong quá trình thiết lập kênh truyền thông an toàn giữa điểm truy cập và trạm không dây. Mục đích của quá trình này là để xác nhận sự sở hữu khóa PMK cũng như việc hoàn tất quá trình sinh khóa ở cả điểm truy cập và trạm.

Tuy nhiên, với 4 thông điệp được trao đổi trong quá trình, chỉ có 3 thông điệp sau là được bảo vệ bởi các khóa sinh ra trong cây phân cấp khóa. Thông điệp đầu được điểm truy cập gửi tới trạm nhằm cung cấp giá trị ngẫu nhiên (nonce) thứ nhất phục vụ cho quá trình sinh khóa. Trạm mặc nhiên chấp nhận mọi thông điệp dạng này để có thể chắc chắn rằng quá trình bắt tay vẫn thành công trong trường hợp mất gói tin hoặc truyền lại. Điều này cho phép kẻ tấn công thực hiện giả mạo thông điệp 1 với giá trị nonce thay đổi khiến cho quá trình bắt tay 4-bước thất bại. Để đối phó với trường hợp thông điệp 1 bị giả mạo, phía trạm cho phép lưu tất cả giá trị nonce nó nhận được và sinh ra các PTK tương ứng. Tuy nhiên, khi gửi đi hàng loạt gói tin giả mạo này, kẻ tấn công một lần nữa có thể khiến cho phía trạm cạn kiệt tài nguyên

(CPU và RAM). Kiểu tấn công này khá nghiêm trọng bởi nó tương dối dễ dàng cho kẻ tấn công và một khi thành công, nó khiến cho mọi nỗ lực đảm bảo an ninh trong bước xác thực phía trước mất đi ý nghĩa.



Hình 4-3. Tấn công vào quá trình bắt tay 4-bước

4.2. Hệ thống WLAN an toàn

Dựa vào những nghiên cứu và phân tích có được về mức độ an ninh mạng WLAN 802.11 nói chung và của chuẩn an ninh 802.11i nói riêng, ở đây tôi đề xuất một mô hình hệ thống WLAN an toàn với những cải tiến nhằm nâng cao mức độ an ninh của môi trường mạng cũng như cho phép xây dựng một hệ thống dựa trên chuẩn 802.11i sẵn có với những sửa đổi là ít nhất. Như đã trình bày, đảm bảo an ninh cho mạng WLAN 802.11 chính là đảm bảo bốn tiêu chí: tính bí mật, tính toàn vẹn, tính xác thực và tính sẵn sàng cho mạng này. Do vậy, hệ thống WLAN an toàn được đề xuất cũng nhằm đảm bảo bốn tiêu chí này.

Thứ nhất, về mặt mã hóa và đảm bảo tính toàn vẹn dữ liệu cho mạng, với giao thức CCMP, các phân tích và nghiên cứu cho đến nay đều chỉ ra rằng việc mã hóa và đảm bảo tính toàn vẹn trong 802.11i sử dụng khóa có độ dài 128 bit là hiệu quả, khó có thể tấn công vào được. Tính đến nay, chưa có rủi ro an ninh nào liên quan đến CCMP được công bố. Với lý do đó, hệ thống WLAN an toàn sẽ sử dụng CCMP như là phương pháp duy nhất để mã hóa và đảm bảo tính toàn vẹn cho dữ liệu mạng.

Thêm vào đó, kiểu tấn công quay lui dịch vụ lợi dụng việc hai khung tin dẫn đường và dò tìm là không được bảo vệ trong mạng WLAN. Việc mã hóa hay kiểm tra tính toàn vẹn của các khung tin này là rất khó bởi tại thời điểm này, giữa điểm truy cập và trạm chưa có khóa chia sẻ nào để áp dụng. Nếu áp dụng giải pháp khóa chia sẻ trước ở trường hợp này sẽ dẫn tới việc khó khăn trong quản lý khóa cũng như đảm bảo tính bí mật của khóa. Do đó, việc sử dụng duy nhất CCMP cũng để nhằm chống lại kiểu tấn công này bởi điểm truy cập chỉ chấp nhận một giải pháp mã hóa và toàn vẹn dữ liệu duy nhất là CCMP.

Thứ hai, việc áp dụng chuẩn 802.1X kết hợp EAP trong 802.11i vào quá trình xác thực giúp cho việc xác thực và phân phối khóa trở nên an toàn và hiệu quả. Tuy vậy 802.11i lại không đặc tả phương pháp xác thực EAP cụ thể được dùng mặc dù có rất nhiều phương pháp xác thực có thể sử dụng với EAP. Do đó hệ thống WLAN đề xuất sử dụng phương pháp xác thực EAP-TLS kết hợp với máy chủ xác thực RADIUS.

Cụ thể thì EAP-TLS là một chuẩn xác thực EAP mở được định nghĩa trong văn bản RFC 2716. Chuẩn xác thực này sử dụng giao thức TLS hay còn gọi là SSL (Secure Socket Layer). TLS sử dụng cơ sở hạ tầng khóa công khai (PKI) để đảm bảo để đảm bảo an toàn cho dữ liệu truyền thông. PKI được xem là an toàn và có nhiều ứng dụng bao quanh như chứng chỉ số, SSL, SSH, mạng riêng ảo dựa trên SSL,… Cho đến nay, EAP-TLS vẫn được xem là một trong những giải pháp xác thực an toàn nhất và được hỗ trợ bởi mọi nhà sản xuất phần cứng và phần mềm. Còn máy chủ xác thực RADIUS sử dụng giao thức RADIUS phục vụ cho quá trình xác thực hiện được xem là hiệu quả và phổ dụng với các mạng hữu tuyến lẫn không dây.

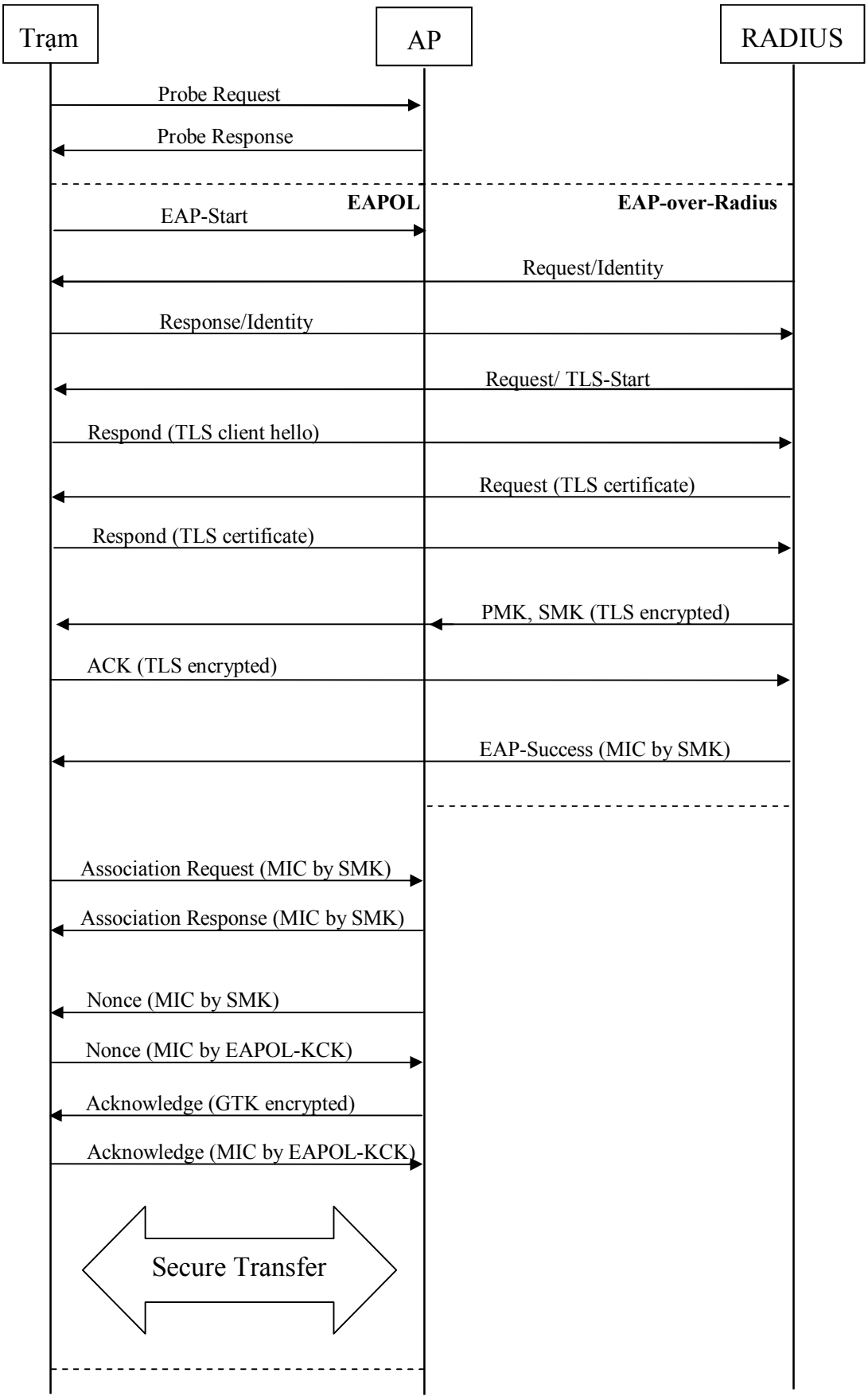
Thứ ba, hệ thống WLAN an toàn đề xuất những sửa đổi cần thiết để giảm thiểu những rủi ro liên quan đến kiểu tấn công DoS - được xem là khá dễ dàng để tấn công vào mạng 802.11. Tuy nhiên, có nhiều dạng tấn công DoS có thể thực hiện được từ tầng vật lý cho đến tầng ứng dụng nên ở đây chỉ cố gắng đạt được khả năng phòng chống DoS ở tầng liên kết dữ liệu.

- Trước hết, để loại bỏ được kiểu tấn công tràn ngập gói tin hủy liên kết hay

hủy xác thực, giải pháp được đưa ra là thay đổi mô hình hoạt động của 802.11i trong đó bước xác thực 802.11X được đưa lên trước bước liên kết – khởi nguồn từ nghiên cứu [33], đồng thời loại bỏ bước xác thực mở trong mô hình hoạt động của 802.11i. Cách làm này cũng không làm thay đổi nhiều mô hình của quá trình kết nối trong mạng WLAN 802.11, theo đó các trạm cần được xác thực trước khi có thể liên kết với điểm truy cập. Sau khi thực hiện xác thực nhờ 802.1X kết hợp EAP-TLS, bên cạnh khóa bí mật được gửi tới điểm truy cập và trạm, máy chủ xác thực sẽ thực hiện tạo thêm một khóa nữa nhằm đảm bảo tính toàn vẹn cho các thông điệp liên kết. Khóa này – được gọi là SMK- cũng được bảo vệ bởi EAP-TLS. Sau cùng, các thông điệp liên kết được đảm bảo toàn vẹn bởi khóa này sử dụng hàm băm HMAC-SHA-1 giống như trong quá trình bắt tay bốn bước.

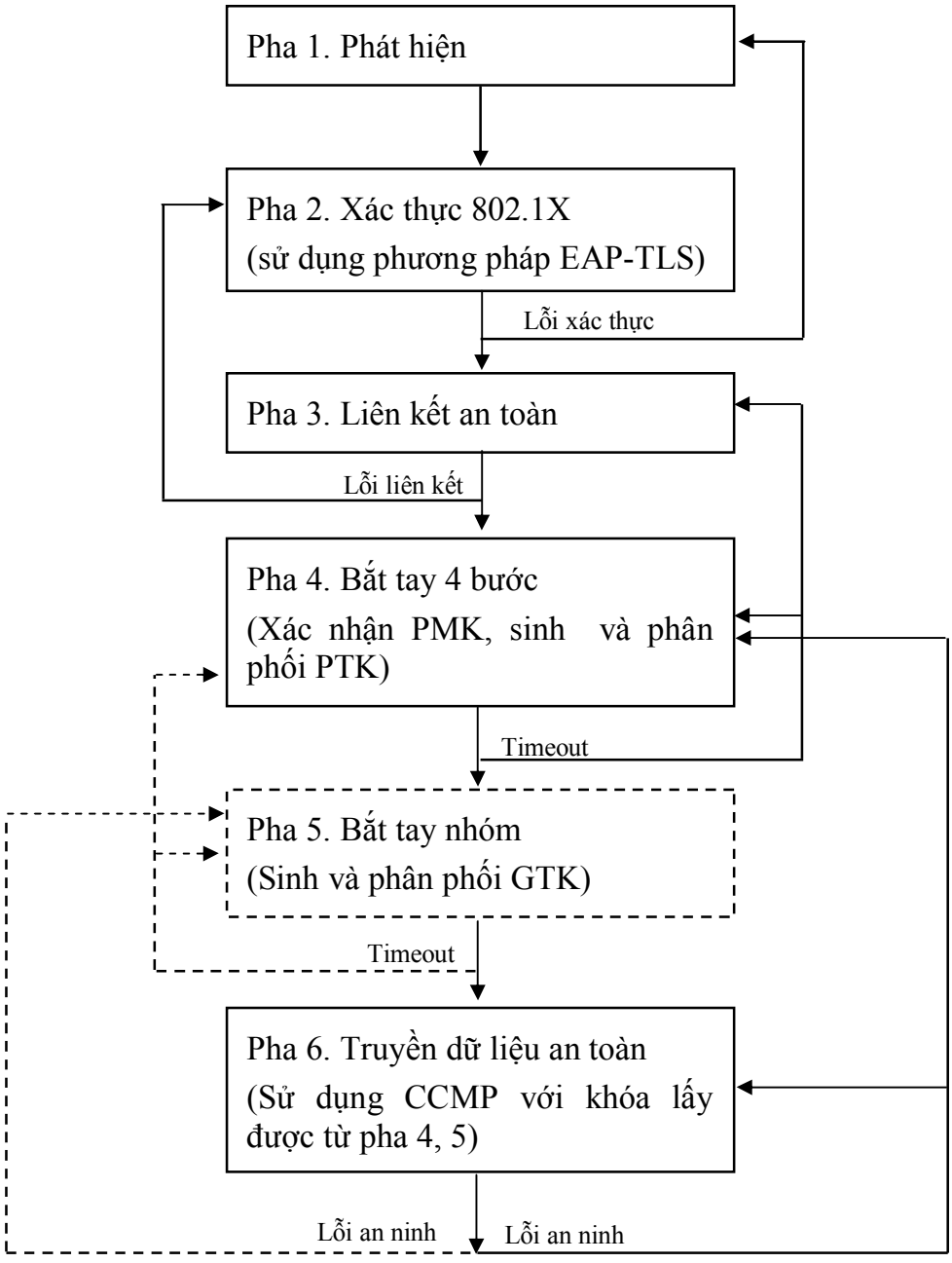
- Tiếp đó, để chống lại khả năng giả mạo các thông điệp 1 trong quá trình bắt tay bốn bước, khóa trên cũng được dùng để đảm bảo toàn vẹn cho thông điệp này sử dụng hàm băm HMAC-SHA-1. Phía trạm khi kiểm tra giá trị toàn vẹn của thông điệp này, nếu phát hiện sai sẽ bỏ qua. Nhờ đó, loại bỏ được kiểu tấn công DoS vào quá trình bắt tay này.
- Cuối cùng, để chống lại kiểu tấn công bằng việc giả mạo các thông điệp EAPOL-Success, EAPOL-Failure và EAPOL-Logoff, hệ thống WLAN an toàn cũng thực hiện việc kiểm tra toàn vẹn các thông điệp này nhờ khóa sinh ra ở bước xác thực kết hợp với hàm băm HMAC-SHA-1. Việc sử dụng lại khóa này nhằm giảm bớt việc sinh cũng như quản lý khóa ở điểm truy cập và trạm.

Với những sửa đổi và đề xuất đó, mô hình hoạt động của hệ thống WLAN 802.11 an toàn được mô tả bởi quá trình gửi/nhận các thông điệp như sau:



Hình 4-4. Mô hình hoạt động của hệ thống WLAN an toàn

Ngoài ra, để nâng cao hiệu suất và giảm bớt thời gian thực thi của quá trình trong trường hợp xảy ra lỗi, hệ thống WLAN an toàn áp dụng mô hình khôi phục lỗi được đưa ra trong [14]. Theo đó, tại mỗi bước trong quá trình nếu có xảy ra lỗi, hệ thống sẽ quay lại bước gần nhất trước đó (với giả định rằng đã thành công).



Hình 4-5. Mô hình hệ thống WLAN an toàn
(trong mô hình, pha 5 là tùy chọn)

KẾT LUẬN

An toàn dữ liệu máy tính luôn là vấn đề nóng hổi đặc biệt là vấn đề an toàn dữ liệu mạng khi mà mạng máy tính đang ở trong giai đoạn phát triển mạnh mẽ. Mạng WLAN 802.11 sử dụng môi trường truyền dẫn không dây điện từ với những đặc điểm riêng của nó cần có những giải pháp an ninh riêng bên cạnh các giải pháp an ninh truyền thống cho mạng hữu tuyến. Việc tập trung nghiên cứu, đánh giá mức độ an ninh của mạng này không chỉ có ý nghĩa đối với riêng lĩnh vực quân sự, kỹ thuật mà còn đối với tất cả các lĩnh vực đang áp dụng nó.

Do vậy, luận văn trước hết thực hiện việc tìm hiểu, phân tích các giải pháp an ninh cũng như các rủi ro từ mạng 802.11 dựa trên các tiêu chí đảm bảo: tính an toàn, tính xác thực, tính toàn vẹn. Qua đó có thể thấy, chuẩn an ninh 802.11i với mục tiêu cung cấp một giải pháp an ninh mới cho mạng 802.11 đủ khả năng để mang lại khả năng mã hóa và đảm bảo tính toàn vẹn hiệu quả khi sử dụng CCMP.

Kiến trúc mạng an toàn ổn định RSN trong 802.11i cung cấp khả năng xác thực hai chiều, sinh khóa động cũng như phân phối khóa tương đối hiệu quả. Tuy vậy, khả năng hỗ trợ các thiết bị phần cứng cũ đã khiến cho 802.11i có những rủi ro khi triển khai trong thực tế. Đối với chế độ xác thực khóa chia sẻ trước, nếu không được thiết lập đúng mức, rủi ro an ninh xảy ra cho mạng là tương đối cao. Ngoài ra, mạng hỗn hợp cho phép kẻ tấn công thực hiện kiểu tấn công quay lui mức độ an ninh nếu không được nghiên cứu và triển khai hợp lý. Việc không chỉ định một phương pháp xác thực EAP cụ thể nào dẫn tới sự mất đồng bộ giữa các nhà sản xuất thiết bị, và càng nguy hiểm hơn nếu phương pháp xác thực EAP được áp dụng là không an toàn bởi khóa mã hóa chính được cung cấp trong quá trình này.

Nhu cầu về mạng tăng cao khiến cho tính sẵn sàng trở thành một thuộc tính an ninh quan trọng cho mạng 802.11. Việc bỏ tiêu chí này trong các đặc tả 802.11 (đặc biệt là đặc tả 802.11i) khiến cho mạng trở nên mất an toàn trước các kiểu tấn công từ chối dịch vụ (DoS). Trong đó, các kiểu tấn công dựa trên các khung tin quản lý, khung tin liên kết và khung tin EAP là tương đối dễ dàng thực hiện bởi các khung tin này được truyền đi không bảo vệ. Điển hình là các kiểu tấn công ngắt liên kết,

tấn công vào quá trình bắt tay 4-bước. Cách giải quyết tốt cho các vấn đề này là thực hiện việc kiểm tra toàn vẹn các thông điệp đó sử dụng một khóa riêng được chia sẻ giữa hai bên (điểm truy cập và trạm không dây). Kiểu tấn công DoS dựa trên cơ chế phản ứng khi mã MIC sai cũng tương đối dễ dàng cho kẻ tấn công. Tuy vậy, kiểu tấn công này hoàn toàn có thể bị loại bỏ nhờ áp dụng CCMP vào quá trình mã hóa và kiểm tra tính toàn vẹn của dữ liệu.

Từ những kết quả nghiên cứu đó, luận văn đề xuất một mô hình lý thuyết mạng không dây WLAN an toàn với những yêu cầu cùng một số sửa đổi nhỏ trong chuẩn 802.11i với mục đích nâng cao khả năng an toàn và đặc biệt là giảm thiểu những rủi ro an ninh khi đối mặt với kiểu tấn công từ chối dịch vụ.

Mặc dù cung cấp một cái nhìn toàn diện và tổng quát về an ninh cho mạng 802.11, tuy vậy do hạn chế về mặt thời gian, điều kiện thiết bị, cộng với trình độ có hạn, luận văn chưa tiến hành được về mặt thực nghiệm mô hình lý thuyết đã đề xuất. Do đó chưa có được nhưng đánh giá bước đầu về hiệu năng của những cải tiến trong mô hình này.

Do đó, trong tương lai, bên cạnh việc tiến hành thực nghiệm mô hình lý thuyết đã đề xuất, việc tiếp tục nghiên cứu phương pháp mã hóa hiệu quả thay thế cho phương pháp EAP-TLS để giảm thiểu thời gian thực thi, cùng việc nghiên cứu giải pháp đối phó với các kiểu tấn công DoS chưa được đề cập tới cũng gợi mở nhiều triển vọng.

TÀI LIỆU THAM KHẢO

[1] Matthew Gast. "802.11- Wireless Networks The Definitive Guide", 2nd edition. O'Reilly 4/2005.

[2] Tom Karygiannis, Les Owens. "Wireless Network Security: 802.11, Bluetooth and Handheld Devices", Special Publication 800-48. National Institute of Standards and Technology 11/2002, pp. 17-63.

[3] Pejman Roshan, Jonathan Leary. "802.11 Wireless LAN Fundamentals". Cisco Press 12/2003.

[4] Phan Hương. "Công nghệ OFDM trong truyền dẫn vô tuyến băng rộng điểm - đa điểm tốc độ cao". 3/2006.
[http://www.tapchibcvt.gov.vn/News/PrintView.aspx?ID=16379].

[5] Mark Davis. "The 802.11 Family of WLAN Standards – Untangling the Alphabet Soup". School of Electronics and Communications Engineering, 2004.

[6] Williams Stalling. "IEEE 802.11: Wireless LANs from a to n". IEEE Computer Society 2004.

[7] Jon Edney, William A. Arbaugh. "Real 802.11 Security: Wi-Fi Protected Access and 802.11i". Addison Wesley 6/2003.

[8] Sheila Frankel, Bernard Eydt, Les Owens, Karen Scarfone. "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i", Special Publication 800-97. National Institute of Standards and Technology 2/2007.

[9] Jesse Walker. "Unsafe at any key size: An analysis of the WEP encapsulation". Submission to the IEEE 802.11 Standards Committee, 10/2000.

[10] Fluhrer, S., I. Mantin, and A. Shamir. "Weaknesses in the key scheduling algorithm of RC4". Eighth Annual Workshop on Selected Areas in Cryptography, 2001.

[11] Cyrus Peikari, Seth Fogie. "Maximum Wireless Security". Sams Publishing 12/2002.

[12] Borisov, N, I. Goldberg, and D. Wagner. "Intercepting mobile communications: the insecurity of 802.11". In Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking 2001, pp. 180–188.

[13] Tom Denis. "Analysis of TKIP Temporal Key Integrity Protocol". 5/2003.
[http://libtomcrypt.com/files/tkip.pdf]

[14] Changhua He, John C Mitchell. "Security Analysis and Improvements for IEEE 802.11i". Network and Distributed System Security Symposium Conference Proceedings, 1/2005.

[15] Ross Hytnen, Mario Garcia. "An analysis of Wireless Security". Consortium for Computing Sciences in Colleges, 4/2006.

[16] Jennifer Seberry. "Security Analysis of Michael the IEEE 802.11i Message Integrity Code". University of Wollongong - New South Wales, Australia, 2005.

[17] Daemen, J., and V. Rijmen. "Smart Card Research and Applications, The Block Cipher Rijndael". Springer-Verlag 2000, pp. 288–296.

[18] Daemen, J., and V. Rijmen. "Rijndael, the advanced encryption standard". Dr. Dobb's Journal 26(3), 2001, .pp 137–139.

[19] Bellare, M. J. Kilian, and P. Rogaway. "The security of the cipher block chaining message authentication code". Journal of Computer and System Sciences 61(3), 2000, pp. 362–399.

[20] N. Ferguson. "Michael: an improved MIC for 802.11 WEP". IEEE 802.11 02-020r0, 1/2002.
[http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/2-020.zip]

[21] "Cyclic redundancy check".
[http://en.wikipedia.org/wiki/Cyclic_redundancy_check]

[22] J. S. Park, D. Dicoi. "WLAN Security: current and future". IEEE Internet Computing, Volume 7, No 5, 10/2003, pp.60-65.

[23] V. Moen, H. Raddum, K. J. Hole. "Weakness in the Temporal Key Hash of WPA". ACM SIGMOBILE Mobile Computing and Communication Review, Volume 8, Issue 2, 4/2004. pp. 76-83.

[24] Glenn Fleishman. "Weakness in Passphrase Choice in WPA Interface". 11/2003 [http://wifinews.com/archives/002452.html]

[25] Nancy Cam-Winget, Russ Housley, David Wagner, and Jesse Walker. "Security Flaws in 802.11 Data Link Protocols". Communications of the ACM Vol. 46, No. 5, 5/2003.

[26] J. D. Morrison. "IEEE 802.11 Wireless Loca Area Network Security through Location Authentication". Thesis of Master of Science, NAVAL Postgraduate School, California, United States. 9/2002.

[27] RFC 3748. "Extensible Authentication Protocol (EAP)". 6/2004.
[http://www.ietf.org/rfc/rfc3748.txt]

[28] "802.1X - Port Based Network Access Control". IEEE Std 802.1D-1998.

[29] RFC 2869. “RADIUS Extensions”. 2000. [http://www.ietf.org/rfc/rfc2869.txt]

[30] RFC 2898. “PKCS #5: Password-Based Cryptography Specification Version 2.0”. 9/2000. [http://www.ietf.org/rfc/rfc2898.txt]

[31] Arunesh Mishra, William A. Arbaugh. “An Initial Security Analysis of the IEEE 802.1X Standard”. Universiy of Maryland, 2/2002.

[32] Seong-Pyo Hong, Joon Lee. “Supporting Secure Authentication and Privacy in Wireless Computing”. International Conference on Hybrid Information Technology, 2006.

[33] D. B. Faria, D. R. Cherition. “DoS and authentication in wireless public access network”. Proceedings of the First ACM Workshop on Wireless Security, 2002.

[34] IEEE Standards. “802.11i”. 7/2004.

[35] Bruce Schneier. “Cryptanalysis of SHA-1”. 2/2005. [http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html]

[36] RFC 3394. “Advanced Encryption Standard (AES) Key Wrap Algorithm”. 9/2002 [http://www.ietf.org/rfc/rfc3394.txt]

[37] A. A. Vladimirov, K. V. Gavrilenko, A. A. Mikhailovsky. "Wi-Foo: The Secrets of Wireless Hacking". Addison Wesley, 6/2004.

PHỤ LỤC 1 - Danh sách các đặc tả IEEE 802.11 [1]

Đặc tả	Chú giải
802.11	Chuẩn đầu tiên (1997).
802.11a	Chuẩn thứ 2 cho tầng vật lý (1999)
802.11b	Chuẩn thứ 3 cho tầng vật lý (1999)
802.11d	Mở rộng công nghệ trải phổ nhảy tần để có thể hoạt động trên liên miền tần số được quy định khác nhau ở các quốc gia.
(802.11e)	Cung cấp mở rộng QoS cho tầng MAC.
802.11F	Giao thức liên điểm truy cập cho phép cải thiện hoạt động của các điểm truy cập được roaming
802.11g	Chuẩn thứ 4 cho tầng vật lý (2003).
802.11h	Chuẩn mở rộng cho phép 802.11a tương thích với các quy định của Châu Âu.
802.11i	Nâng cao mức độ an ninh tại tầng liên kết dữ liệu
802.11j	Chuẩn mở rộng cho phép 802.11a tương thích với các quy định của Nhật.
(802.11k)	Nâng cao khả năng liên lạc giữa các trạm và mạng.
(802.11n)	Mục đích tạo ra thông lượng mạng đạt tới 100Mbps.
(802.11p)	Dành cho mục đích sử dụng trên xe hơi.
(802.11r)	Mở rộng nhằm cải thiện hiệu năng roaming
(802.11s)	Mở rộng 802.11 nhằm sử dụng trong công nghệ mesh networking.
(802.11u)	Thay đổi 802.11 nhằm hỗ trợ khả năng liên mạng với các công nghệ mạng khác.

PHỤ LỤC 2 - Thuật toán sinh khóa trong TKIP [7] [13]

Giống như WEP, cả hai pha trong giao thức TKIP sử dụng một bảng hoán vị gọi là bảng S. Do TKIP sử dụng các giá trị 16 bit trong quá trình tính toán, nên về lý thuyết, bảng hoán vị này có độ dài 2^{16} = 65536 từ (tương đương với 128KB). Tuy nhiên, thực tế, TKIP sử dụng một bảng gồm 512 phần tử, mỗi phần tử 1 byte. Thực chất bảng này được tách thành 2 phần (có thể gọi là 2 bảng), mỗi phần 256 phần tử gọi là TSU (TKIP_Sbox_Upper) và TSL (TKIP_Sbox_Lower). Các giá trị của bảng hoán vị S là xác định trước và được đặc tả trong chuẩn 802.11i [13]. Để lấy được hoán vị cho một từ 16bit X, TKIP sử dụng byte cao của X làm chỉ mục để xác định giá trị trong bảng TSU, còn byte thấp của X được sử dụng để xác định giá trị trong bảng TSL. Hai giá trị 16bit này sau đó được kết hợp lại bởi phép toán XOR để cho ra hoán vị 16bit cuối cùng.

Theo đó, i = S[j] có nghĩa i là hoán vị của j.

Pha 1.

Mặc dù pha này sử dụng toàn bộ 128 bit của khóa phiên theo thời gian, kết quả đầu ra chỉ là một mảng 80 bit gồm 5 từ 16-bit gọi là $P1K_0$, $P1K_1$, $P1K_2$, $P1K_3$, and $P1K_4$. Với cách ký hiệu:

- TSC_1 – là 16 bit giữa của TSC (bit 16–31)
- TSC_2 – là 16 bit cao của TSC (bit 32–47)
- TA_n là byte thứ n của địa chỉ MAC được sử dụng cho quá trình tính toán. Theo đó, TA_0 là byte thấp nhất còn TA_5 là byte cao nhất.
- TK_n là byte thứ n của khóa phiên theo thời gian. Theo đó, TK_0 là byte thấp nhất còn TK_{15} là byte cao nhất)
- Biểu thức x ∩ y đại điện cho phép toán kết hợp 2 byte (X, Y) thành một từ 16 bit:
- x ∩ y = 256*x + y
- S[ ] đại diện cho kết quả hoán vị lấy được từ bảng S.

thì quá trình tính toán ở pha 1 diễn ra như sau:

```
Bước 1:
  P1K0 = TSC1
  P1K1 = TSC2
  P1K2 = TA1 ∩ TA0
  P1K3 = TA3 ∩ TA2
  P1K4 = TA5 ∩ TA4

Bước 2:
  FOR i = 0 to 3
  BEGIN
     P1K0 = P1K0 + S[ P1K4 ∩ (TK1  ∩ TK0 ) ]
     P1K1 = P1K1 + S[ P1K0 ∩ (TK5  ∩ TK4 ) ]
     P1K2 = P1K2 + S[ P1K1 ∩ (TK9  ∩ TK8 ) ]
     P1K3 = P1K3 + S[ P1K2 ∩ (TK13 ∩ TK12) ]
     P1K4 = P1K4 + S[ P1K3 ∩ (TK1  ∩ TK0 ) ] + i
     P1K0 = P1K0 + S[ P1K4 ∩ (TK3  ∩ TK2 ) ]
     P1K1 = P1K1 + S[ P1K0 ∩ (TK7  ∩ TK6 ) ]
     P1K2 = P1K2 + S[ P1K1 ∩ (TK11 ∩ TK10) ]
     P1K3 = P1K3 + S[ P1K2 ∩ (TK15 ∩ TK14) ]
     P1K4 = P1K4 + S[ P1K3 ∩ (TK3  ∩ TK2 ) ] + 2*i + 1
  END
```

Pha 2.

Thoạt nhìn, pha 2 nhìn có vẻ phức tạp hơn pha 1. Tuy vậy, trong pha này, mặc dù có nhiều bước tính toán hơn nhưng vòng lặp không được sử dụng để tăng tốc độ tính toán. Kết quả trả ra sau 2 bước tính toán ban đầu là mảng gồm 6 từ 16-bit được đặt tên PPK_0, PPK_1, PPK_2, PPK_3, PPK_4 và PPK_5 được sử dụng cho bước cuối cùng nhằm xác định giá trị cho khóa RC4.

Với cách ký hiệu như pha 1, cộng thêm:

- P1Kn là từ 16-bit thứ n trả về từ pha 1
- Toán tử >>> đại diện cho phép toán dịch chuyển xoay vòng 16-bit sang phải 1 vị trí.
- Toán tử >> đại diện cho phép dịch bit đơn thuần.

Thì pha 2 được thực hiện qua ba bước tính toán chính:

```
Bước 1:
     PPK0 = P1K0
     PPK1 = P1K1
     PPK2 = P1K2
     PPK3 = P1K3
     PPK4 = P1K4
     PPK5 = P1K5 + TSC0

Bước 2:
     PPK0 = PPK0 + S[ PPK5 ⊕ (TK1  ∩ TK0 ) ]
     PPK1 = PPK1 + S[ PPK0 ⊕ (TK3  ∩ TK2 ) ]
     PPK2 = PPK2 + S[ PPK1 ⊕ (TK5  ∩ TK4 ) ]
```

$PPK_3 = PPK_3 + S[\ PPK_2 \oplus (TK_7 \cap TK_6)\ ]$
$PPK_4 = PPK_4 + S[\ PPK_3 \oplus (TK_9 \cap TK_8)\ ]$
$PPK_5 = PPK_5 + S[\ PPK_4 \oplus (TK_{11} \cap TK_{10})\ ]$
$PPK_0 = PPK_0 + >>>(PPK_5 \oplus (TK_{13} \cap TK_{12}))$
$PPK_1 = PPK_1 + >>>(PPK_0 \oplus (TK_{15} \cap TK_{14}))$
$PPK_2 = PPK_2 + >>>(PPK_1)$
$PPK_3 = PPK_3 + >>>(PPK_2)$
$PPK_4 = PPK_4 + >>>(PPK_3)$
$PPK_5 = PPK_5 + >>>(PPK_4)$

Bước 3:

$RC4Key_0 = UpperByte(TSC_0)$
$RC4Key_1 = (\ UpperByte\ (TSC_0)\ |\ 0x20\ )\ \&\ 0x7F$
$RC4Key_2 = LowerByte(TSC_0)$
$RC4Key_3 = LowerByte\ ((PPK_5 \oplus ((TK_1 \cap TK_0) >> 1)$
$RC4Key_4 = LowerByte\ (PPK_0)$
$RC4Key_5 = UpperByte\ (PPK_0)$
$RC4Key_6 = LowerByte\ (PPK_1)$
$RC4Key_7 = UpperByte\ (PPK_1)$
$RC4Key_8 = LowerByte\ (PPK_2)$
$RC4Key_9 = UpperByte\ (PPK_2)$
$RC4Key_{10} = LowerByte\ (PPK_3)$
$RC4Key_{11} = UpperByte\ (PPK_3)$
$RC4Key_{12} = LowerByte\ (PPK_4)$
$RC4Key_{13} = UpperByte\ (PPK_4)$
$RC4Key_{14} = LowerByte\ (PPK_5)$
$RC4Key_{15} = UpperByte\ (PPK_5)$

Như vậy kết quả trả về sau pha 2 là một mảng gồm 16 byte tạo thành khóa RC4 sử dụng cho việc mã hóa.

PHỤ LỤC 3 - PRF [34]

Hàm sinh số giả ngẫu nhiên (PRF) được đặc tả 802.11i xây dựng nhằm đưa ra một cách thức sinh cây phân phối khóa phục vụ cho việc mã hóa và đảm bảo tính toàn vẹn của dữ liệu. Hàm PRF có khả năng cho ra các khóa có độ dài 128, 192, 256, 384 và 512 bit. Hàm này sử dụng hàm băm HMAC-SHA-1 làm lõi cho quá trình tính toán.

Cách thức hoạt động của PRF được mô tả qua các biểu thức sau:

```
H-SHA-1(K, A, B, X) ← HMAC-SHA-1(K, A || Y || B || X)
PRF(K, A, B, Len)
{
  for i  ← 0 to (Len+159)/160 do
  R ← R || H-SHA-1(K, A, B, i)
  return L(R, 0, Len)
}

PRF-128(K, A, B) = PRF(K, A, B, 128)
PRF-192(K, A, B) = PRF(K, A, B, 192)
PRF-256(K, A, B) = PRF(K, A, B, 256)
PRF-384(K, A, B) = PRF(K, A, B, 384)
PRF-512(K, A, B) = PRF(K, A, B, 512)
```

Trong đó,

- K là khóa bí mật được sử dụng để tạo ra các khóa ngẫu nhiên
- A là nhãn mô tả mục đích của hàm
- X là 1 byte chứa tham số cho hàm
- Y là 1 byte chứa các bit 0
- || là phép toán nối xâu

Cụ thể là:

- PTK ← PRF-X(PMK, “Pairwise key expansion”, Min(AA,SPA) || Max(AA,SPA) || Min(ANonce,SNonce) || Max(ANonce,SNonce))

- GTK ← PRF-X(GMK, “Group key expansion”, AA || GNonce)

Với: AA – địa chỉ MAC của điểm truy cập, SPA – địa chỉ MAC của trạm, Nonce là các giá trị ngẫu nhiên được sinh bởi điểm truy cập (A, G) hoặc trạm (S).

MỤC LỤC