KỸ THUẬT RFID CHỦ ĐỘNG 125KHz VÀ ỨNG DỤNG XÁC THỰC TRONG KHÔNG GIAN HẸP

THE ACTIVE RFID 125KHz TECHNIQUE AND AUTHENTICATION IN MICRO LOCATION

Nguyễn Văn Xuân[1], Hoàng Tuấn Long[2], Nguyễn Thu Hồng[2], Nguyễn Gia Tuấn Anh[1]
[1] Trường đại học Công nghệ thông tin, Việt Nam.
[2] Trường Đại học Cảnh sát nhân dân, Việt Nam.

Ngày toà soạn nhận bài 27/3/2021, ngày phản biện đánh giá 18/4/2021, ngày chấp nhận đăng 4/6/2021.

TÓM TẮT

Trong bài báo này, tác giả trình bày về công nghệ RFID (Radio Frequency Identification Radio) chủ động ở dải tần số LF 125kHz và ứng dụng trong việc nhận dạng, xác thực ở khoảng cách hẹp từ 1-3m. Nội dung phần 1 giới thiệu căn bản về công nghệ RFID, sự giống và khác nhau về mặt kỹ thuật của RFID thụ động và chủ động, ưu nhược điểm của mỗi loại. Trong phần 2, bài toán nhận dạng và xác thực trong khoảng cách hẹp được đặt ra, cụ thể là ứng dụng nhận dạng chủ phương tiện khi ở gần xe, các giải pháp dùng RFID hiện tại đang có. Phần 3, tác giả xây dựng mô hình RFID chủ động để giải quyết bài toán trên. Tác giả cũng đề xuất kỹ thuật sử dụng OTP và mã hóa dữ liệu để chống giả mạo xác thực. Chi tiết phần cứng, mô hình thuật toán mã hóa OTP và dữ liệu được miêu tả trong phần 4. Phần 5 là kết quả thực nghiệm bao gồm dữ liệu khoảng cách nhận dạng thực tế 2,2m với RFID chủ động, ước tính thời gian sử dụng khoảng 3,5 năm nếu dùng pin coin CR2023 đối với hệ thống RFID chủ động dùng chíp nhận dạng AS3933. Kỹ thuật chống xác thực giả mạo mà bài báo đề xuất có thể áp dụng trên các thiết bị UWB (Ultra Wideband) mà đang trở thành xu thế trong ứng dụng nhận dạng thông minh hiện nay.

Từ khóa: *RFID chủ động; 125kHz; OTP; AS3933; UWB.*

ABSTRACT

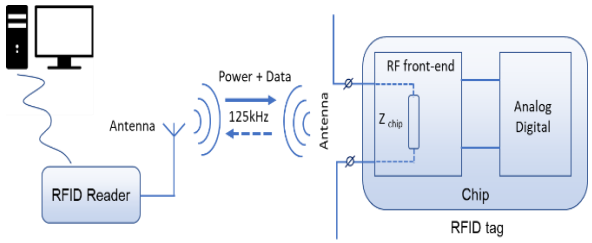
In this paper, we provide an overview of active RFID (Radio Frequency Identification) technique at low frequency band LF 125kHz for identification and authentication in micro location application. Section 1 describes about working principle of RFID technology, the advantages and disadvantages of both passive and active RFID techniques are also taken into account. Following sections, the problem of identification and authentication for vehicle's owner is considered. The current solutions for this problem are being used, nowadays. Section 3, we propose an active RFID system with OTP and data encryption scheme that encrypts OTP to protect data, avoid hacking and anti-counterfeit authentication. The detail of hardware architecture and software algorithm are described in section 4. In section 5, the experimental results emphasize the advantage of active RFID system in reading distance. It also provides an estimation of coin battery life-time about 3,5 years in a system with low power RF receiver chip AS3933. With benefits of proposed solution, it can be applied for UWB (Ultra Wideband) devices which going to be the main topic of real time location applications in very near future.

Keywords: *Active RFID; 125kHz; OTP; AS3933; UWB.*

1. GIỚI THIỆU

RFID (Radio Frequency Identification) là thiết bị nhận dạng sử dụng sóng vô tuyến để tự động nhận dạng, theo dõi, quản lý hàng hoá, con người, động vật và các ứng dụng khác.

Doi: https://doi.org/10.54644/jte.64.2021.93



Hình 1. *Minh hoạ mô hình hệ thống RFID*

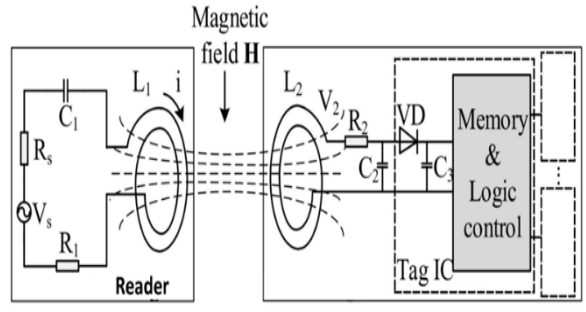
Hệ thống RFID bao gồm hai khối riêng biệt là Reader và Tag [1] ở hình 1, được kết nối thông qua sóng RF.

Dải tần LF (Low Frequency) 125kHz với đặc tính đâm xuyên tốt, nhưng không truyền được xa, thiết kế đơn giản, nó rất phù hợp ứng dụng nhận dạng và xác thực trong phạm vi hẹp. Trong bài báo này, tác giả sẽ xây dựng mô hình nhận dạng và xác thực chủ phương tiện sử dụng kỹ thuật RFID chủ động với khoảng cách nhận dạng từ 1-3m.

1.1 RFID thụ động

Một số Tag có thể tái tạo năng điện từ không gian trường điện từ biến thiên mà Reader tạo ra. Khi antenna của Reader ngừng phát sóng, năng lượng này biến mất, các phần tử trên Tag ngừng hoạt động hoàn toàn. Loại tag này do vậy được gọi là tag thụ động (passive Tag). Nó không thể tự khởi tạo một quá trình giao tiếp với Reader.

Antenna của tag cộng hưởng tại tần số 125kHz và khi Tag đặt trong vùng từ trường H, quá trình trao đổi dữ liệu được diễn ra giữa Reader và Tag [2] như minh họa ở hình 2 dưới đây.



Hình 2. *Tương tác điện cảm giữa Reader và tag thụ động*

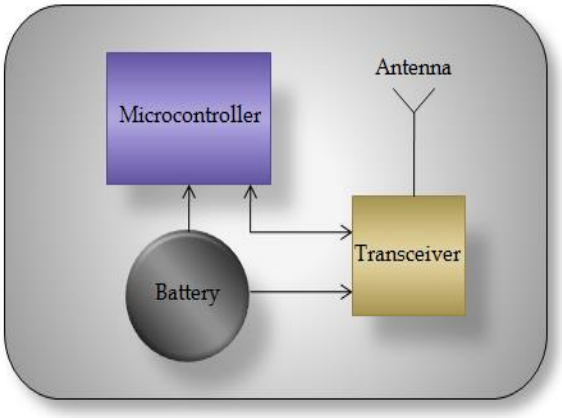
Antenna trên cả Reader và Tag [2] đều có chung tần số cộng hưởng theo công thức:

$$f_0 = \frac{1}{2\pi\sqrt{L_1C_1}} = \frac{1}{2\pi\sqrt{L_2C_2}} \quad (1)$$

Không cần nguồn pin là ưu điểm nổi bật của loại thẻ này, tuy nhiên mã ID thường dễ dàng có thể đọc và giả mạo bằng cách phát chuỗi từ trường giả giống như đáp ứng ID của tag.

1.2 RFID chủ động

Khác với thẻ RFID thụ động, tag chủ động (active tag) có thể khởi tạo một quá trình trao đổi dữ liệu với Reader bất cứ khi nào. Khoảng các giao tiếp cũng xa hơn. Để có được điều này, tag chủ động được trang bị thêm mạch phát RF và nguồn điện riêng [3] theo hình 3 dưới đây.



Hình 3. *Minh họa sơ đồ khối của Tag RFID chủ động*

RFID chủ động có thể loại bỏ thao tác quẹt thẻ như ở thẻ thụ động, cho phép hệ thống tự động xác thực. Dữ liệu được bảo mật thông qua hai kênh truyền ở tần số LF (Low Frequency) 125kHz và UHF (Ultra High Frequency) 433MHz [2]. Tính chủ động của thẻ tag thể hiện nhờ trang bị mạch phát, nó gửi yêu cầu xác thực tới Reader thông qua link UHF, Reader sẽ kích hoạt quá trình xác thực thông qua link LF (Hình 4).

2. NHẬN DẠNG VÀ XÁC THỰC TRONG KHOẢNG CÁCH HẸP

2.1 Nhận dạng chủ phương tiện với thẻ RFID thụ động

Nhận dạng là ứng dụng cốt lõi của thẻ RFID. Thẻ tag chứa nhiều byte ID mang tính

duy nhất nên có thể dùng nó như chìa khóa điện tử để bảo vệ phương tiện, khắc phục trường hợp xe bị bẻ ổ khóa. Đây là ứng dụng rất phổ biến ở Việt Nam. Tuy nhiên nó chứa 2 nhược điểm lớn. Thứ nhất là khoảng cách đọc ngắn, chỉ khoảng 10-20cm, chủ xe phải đặt thẻ này lại gần khu vực antenna của Reader để nhận dạng. Thứ hai là ID của thẻ là các mã cố định, hacker dễ dàng "bẻ khóa" bằng kỹ thuật replay attack, trong đó chuỗi bit của mã thẻ được copy và phát lại y hệt mà không cần quan tâm dữ liệu cụ thể của chuỗi bít đó là gì.

2.2 Nhận dạng với sóng RF (433MHz)

Điển hình là ứng dụng Remote control để tìm xe, mở cửa cuốn… Bộ nhận sóng trên cửa cuốn nhận tín hiệu RF ở tần số 433MHz từ Remote để kiểm tra xem có đúng là chủ nhà không, nếu đúng sẽ thực hiện lệnh mở cửa. Với ưu điểm khoảng cách phát xa khoảng 30m, nhưng nếu Remote chỉ phát mỗi ID của nó tới bộ nhận, thì hacker dễ dàng thu lại được ID này và vẫn dùng kỹ thuật Replay attack để giả mạo chủ nhà. Giải pháp là chống hack trong trường hợp này là sử dụng Rolling code hay còn gọi là hopping code. Trong đó mã ID của Remote cố định được gửi đi kèm 1 mã động, mã này có quy luật riêng, tăng hoặc giảm sau mỗi lần phát. Mã xã thực có dạng:

$$\text{Auth\_key}(i) = \text{ID} + \text{E}(i) \quad (2)$$

Trong đó khóa Auth_key(i) là mã xác thực lần phát thứ i. Phía thu chỉ chấp nhận các Auth_key(i) theo thứ tự nào đó, ví dụ thứ tự tăng dần. Kỹ thuật Replay attack sẽ phát lại Auth_key(i) ở lần thứ (i + 1), và tất nhiên bộ thu sẽ loại khóa này vì nó đang đợi Auth_key(i+1).

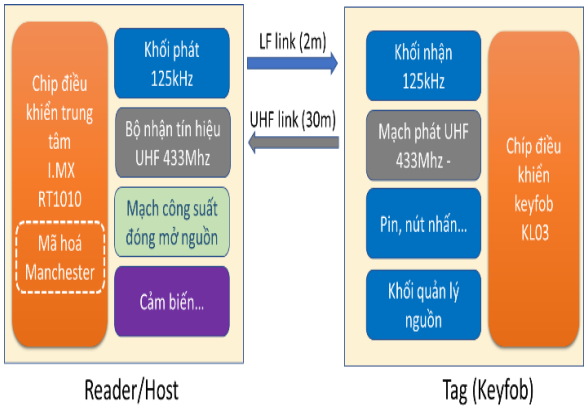
Mức độ bảo mật của hệ thống phục thuộc vào độ bảo mật của hàm mã hóa E(i). Tuy nhiên, đây là hàm tĩnh chỉ chứa tham số i, hacker dễ dàng xây dựng lại hàm E bằng các quan sát quy luật giá trị Auth_key với nhiều giá trị i khác nhau. Hoặc đơn giản hơn, hacker có thể xây dựng bảng dò dạng lookup table mà không cần xây dựng lại hàm mã hóa E.

2.3 Nhận dạng với RFID dải tần UHF (860-915MHz).

Các hệ thống thu phí không dừng, quản lý hàng trong kho bãi là minh chứng hiệu quả nhất tính ưu việt về khoảng cách của RFID ở dài tần UHF (860-915MHz). Ở dài tần tần này, khoảng cách đọc lên tới 10-15m trong khi tag vẫn là tag thụ động, không cần dùng pin. Tuy nhiên, đây không phải giải pháp thích hợp cho ứng dụng nhận dạng chủ phương tiện vì 3 lý do: Kích thước antenna đọc rất lớn khó lắp đặt trên xe, chi phí đầu đọc đắt đỏ, đầu đọc tiêu thụ năng lượng lớn sẽ nhanh chóng làm hệ thống acquy trên xe cạn kiệt.

3. RFID CHỦ ĐỘNG 125kHz TRONG ỨNG DỤNG XÁC THỰC Ở KHOẢNG CÁCH HẸP

Mô hình của một hệ thống RFID chủ động [4] gồm các thành phần cơ bản như hình 4, trong đó Tag chứa nguồn điện riêng và được trang bị kênh phát tín hiệu riêng tới Reader.

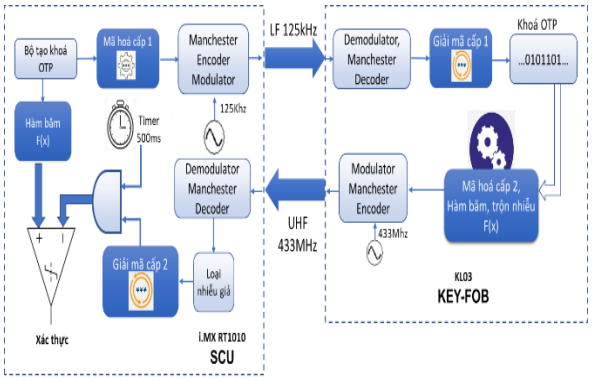


Hình 4. *Sơ đồ khối của RFID chủ động*

Mô hình này phù hợp với ứng dụng xác thực chủ phương tiện, vì khoảng cách giao tiếp của link LF chỉ khoảng 2m, tức chỉ xác thực nếu chủ xe mang Remote trong bán kính 2m gần xe, khi đó xe mới có thể khởi động được. Kích thước antenna nhỏ gọn, năng lượng tiêu thụ thấp là đặc điểm nổi bật, khắc phục các điểm yếu của RFID băng tần UHF (860-915MHz).

Do được trang bị kênh truyền song công, khóa xác thực *Auth_key* là một chuỗi giả

ngẫu nhiên được mã hóa và truyền tới Remote từ SCU, khi Remote nhận được sẽ giải mã hóa và phát lại (qua link UHF 433MHz) mã Hash(*Auth_key*) là hàm hash 1 chiều.



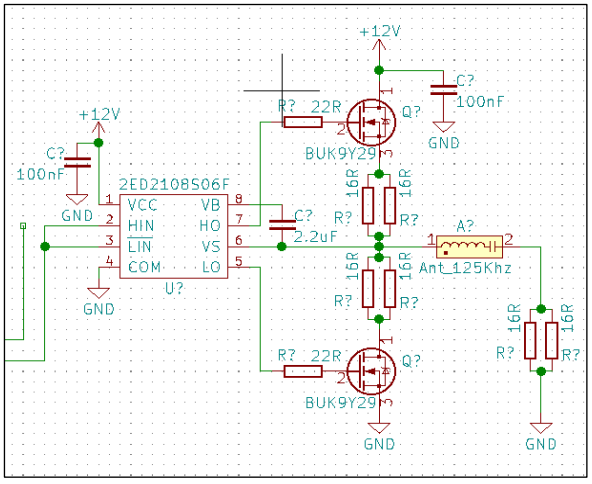
***Hình 5**. Mô hình dùng OTP để chống kỹ thuật hack Replay attack.*

Reader thực hiện hàm Hash() cho khóa *Auth_key* của nó, so sánh kết quả với chuỗi bit nhận được từ Remote, nếu đúng, thì xác nhận xác thực. Để chống kỹ thuật hack brute-force attack, toàn bộ quá trình này được kiểm soát bởi bộ Timer với timeout là 500ms, sau thời gian này, nếu hacker gửi lại đúng chuỗi bits, thì vẫn bị coi là không hợp lệ.

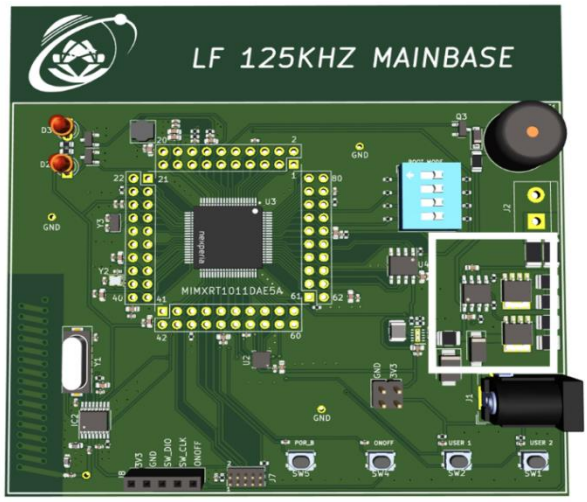
4. THIẾT KẾ HỆ THỐNG

4.1 Phần cứng

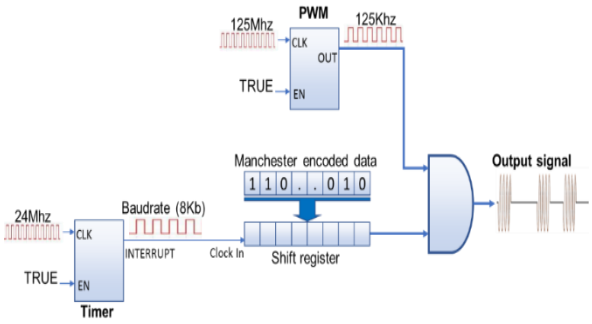
Reader điều chế AM, sóng mang 125kHz để truyền tín hiệu tới Keyfob. Mạch phát tín hiệu 125kHz theo nguyên lý bán cầu H như hình 6 và được thiết kế trên board mạch theo hình 7.



***Hình 6**. Mạch phát 125kHz nửa cầu H*

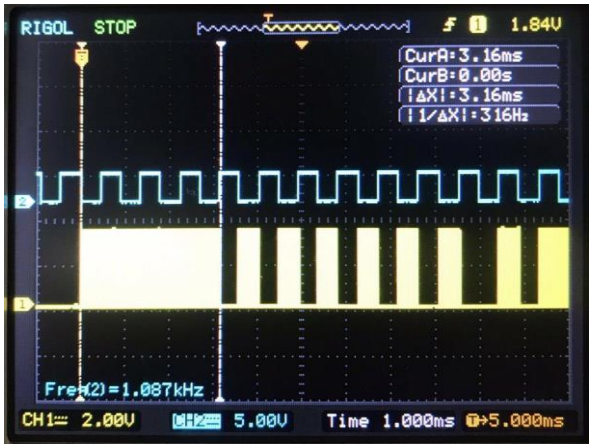


***Hình 7**. Vị trí khối phát 125kHz trên board mạch Reader*



***Hình 8**. Điều chế AM thực thi trên khối phát.*

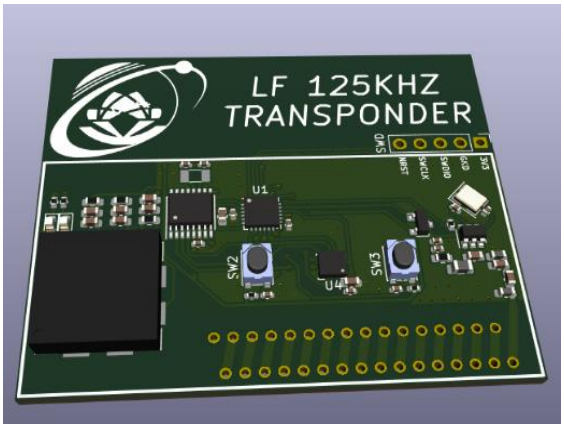
Việc điều chế AM có thể thực hiện theo hình 8 sử dụng các module phần cứng của chip MCU. Hình 9 là dạng sóng đã điều chế AM quan sát tại đầu ra antenna.



***Hình 9.** Dạng sóng điều chế AM (OOK) quan sát trên máy Oscilloscope.*

Hình 10 là mô hình 3D của Remote (hay còn gọi là Keyfob), sử dụng IC AS3933 [5] nhận tín hiệu LF có độ nhạy cao, được điều

khiển bởi MCU ARM Cortex M0+ MKL03. Antenna nhận tín hiệu 3D cho phép Remote nhận tín hiệu tin cậy ở mọi hướng. Ngoài ra còn có IC MICRF113 của hãng Microchip phát tín hiệu AM ở tần số UHF 433Mhz. Cả hệ thống được cấp năng lượng từ pin CR2032.



***Hình 10**. Remote 125kHz transponder*

4.2 Phần mềm

Trong nội dung phần này, tác giả trình bày chi tiết quá trình xác thực ở phương diện phần mềm với thuật toán mã hóa mã OTP.

Để chống việc tạo mã xác thực giả, tác giả đã xây dựng kỹ thuật mã hoá mã OTP (One Time Password), sử dụng trong giao thức xác thực theo mô hình ở hình 5. Mã OTP là một mã 32 bits ngẫu nhiên, được lấy từ giá bộ đếm 32bits. Mã OTP được gửi từ Reader tới Tag sau khi thực hiện hàm mã hoá cấp 1, có thời gian xác thực hợp lệ trong khoảng tauth = 500ms được kiểm soát bởi bộ định thời Timer.

Mã hóa cấp 1 thực hiện trên kênh truyền LF, cho tín hiệu gửi từ Reader (SCU) tới Keyfob. Nó dựa trên thuật toán khoá đối xứng (symmetric-key algorithms), trong đó việc mã hoá và giải mã dùng chung một khoá (hay còn gọi là salt-key hoặc encryption key). Gọi k là khoá, E(x, msg) là hàm mã hoá sử dụng khoá k cho thông điệp msg, C là thông điệp đã mã hoá, ta có

$$C = E(k, msg) \quad (3)$$

Khi đó tồn tại ánh xạ ngược E^{-1} là hàm giải mã hoá, cho phép khôi phục lại dữ liệu gốc

$$msg = E^{-1}(k, C) \quad (4)$$

Khoá k: là byte ngẫu nhiên được lấy từ 8 bit nhỏ nhất của bộ đếm 32 bits

Hàm mã hoá E(k, msg) thực hiện theo các bước sau (được minh họa ở hình 11).

- Bước 1: Chia chuỗi msg thành n byte riêng lẻ (với n = xbyte là kích thước của msg). Đánh số thứ tự từ 0 đến (n -1) và xếp lần lượt theo thứ tự tăng dần. Gọi mảng này là LF_Encrypteddata.
- Bước 2: Đảo trạng thái tất cả các bit của byte đầu tiên nếu bit cuối cùng LSB của k là 0.
- Bước 3: Xây dựng mảng temp_arr gồm 8 phần tử bằng cách ghép các bit của mảng LF_Encrypteddata theo chiều dọc.
- Bước 4: Xoay vòng xuống (quay trái) *i* vị trí của phần từ temp_arr[*i*] nếu bit thứ *i* của k là 1.
- Bước 5: Khôi phục mảng LF_Encrypteddata sau khi xoay các bit ở bước trên.
- Bước 6: Đảo tất cả các bit của byte cuối trong mảng LF_Encrypteddata nếu bit cuối cùng LSB của k là 1.
- Bước 7: Mã hóa k bằng cách kiểm tra MSB và LSB của k, nếu giống nhau thì đảo các bit từ *k1-k6*, nếu khác nhau thì đổi vị trí *k123* cho *k456*.

Mảng LF_Encrypteddata			Mảng temp_arr							
			arr[7]		arr[5]	...			arr[1]	arr[0]
MESSAGE	BIN	HEX	0xA	0x21	0x3	0x3	0x28	0xC	0x3	0x9
OTP0	0x73	01110011	0	1	1	1	0	0	1	1
OTP1	0xB2	10110010	1	0	1	1	0	0	1	0
OTP2	0x04	00000100	0	0	0	0		1	0	0
OTP3	0x8D	10001101	1	0	0	0	1	1	0	1
cmd	0x00	00000000	0	0	0	0	0	0	0	0
Checksum	0x48	01001000	0	1	0	0	1		0	
Salt (k)	0x49	01001001	1	0	0	1	1	1	1	1

***Hình 11.** Minh họa các bước mã hóa OTP*

Tập sinh V của E*(k, msg)* sẽ bao gồm 2^{8*n} vector.

Giả sử hacker phát sóng UHF và sử dụng kỹ thuật brute-force attack để dò mã xác thực

32 bits. Đối với hệ thống không dùng mã OTP, gọi ρ_i là xác suất mã thử thứ i (i = 1÷ 2^{32}) trùng với mã xác thực, dễ thấy $\rho_i = \frac{1}{2^{32}}$. Nếu tốc độ bit trên kênh UHF là 4kbps, thời gian trung bình để hacker dò được mã:

$$\bar{t}_h = \frac{32}{4kbps}\sum(i\rho_i) = \frac{32}{4kbps}.\frac{2^{32}+1}{2} \; ; \; 199 \quad (5)$$

ngày và thời gian tối đa để chắc chắn dò được mã là:

$$t_h = \frac{32*2^{32}}{4kbps} = 34359738 \text{ (s)} = 397 \text{ ngày,}$$ mã sau khi dò được sẽ được sử dụng để truy cập tiếp các lần sau.

Với giải pháp mã OTP ngẫu nhiên mà tác giả đề xuất, cứ 500ms một phiên xác thực kết thúc. Phương pháp brute-force attack không còn ý nghĩa vì chỉ thử được khoảng $n = \frac{500ms*4kbps}{32} = 62$ mã trong thời gian này. Do vậy không có thời gian hữu hạn để chắc chắn mã OTP được dò ra.

Cần phải lưu ý rằng, khóa OTP nếu dò được cũng không có nhiều ý nghĩa gì vì nó không dùng lại được để cho các lần xác thực sau.

5. KẾT QUẢ THỰC NGHIỆM

Bảng 1 tổng hợp một số kết quả thực nghiệm khi so sánh tính năng giữa Tag RFID thụ động và chủ động.

Thực nghiệm đo khoảng cách nhận dạng và tần số sóng mang được tác giả thực hiện với cả RFID chủ động và thụ động theo thiết lập ở bảng 2.

Kết quả: Khoảng cách nhận dạng RFID chủ động xa khoảng 2,2m do dùng chíp AS3933 có độ nhạy thu cao và mạch phát có công suất lớn hơn RFID thụ động. Với cả hai loại, thì khoảng cách đọc tại tần số cộng hưởng 125kHz là xa nhất. Khoảng cách này giảm đi nhanh chóng khi tần số thay đổi lệch khỏi tần số cộng hưởng.

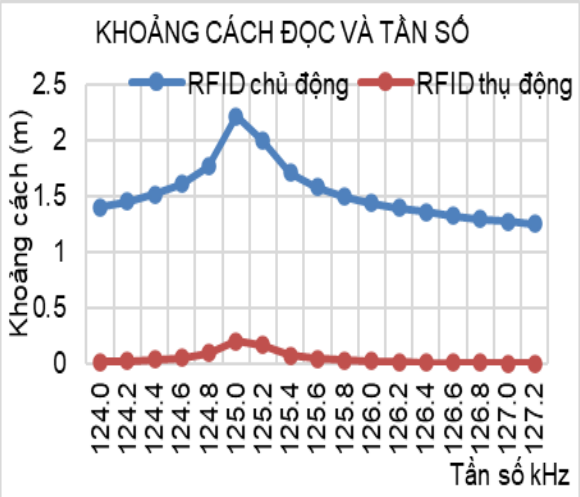
Bảng 1. *So sánh RFID thụ động và chủ động*

Đặc điểm	**RFID thụ động[1]**	**RFID chủ động[2]**
Băng tần sóng mang	125kHz	125Khz
Độ nhạy thu	3V	80µV
Khoảng cách giao tiếp	10 cm	2,2 m
Mã hoá kênh truyền	Manchester	Mancheste r/Bitpha…
Data rate	~1Kbps	~4Kbps
Ghi dữ liệu người dùng		✓
Mã hoá ID/Data	Không	Có, tuỳ chọn
Mức độ bảo mật	Rất thấp	Tốt
Khả năng nhận dạng ID	Có	Có
Khả năng chống xác thực giả mạo.	Không	Có
Khởi tạo xác thực	Không	Có
Điện năng tiêu thụ	0 µA	7,54 µA
Kích thước	Nhỏ gọn	Trung bình
Tổng quan	Không cần pin, khoảng cách đọc gần, dễ bị hack.	Cần pin, khoảng cách xa, bảo mật rất tốt, khó hack.

[1] Passive tag EM4100
[2] Đo với chip LF reciever AS3933

Bảng 2. *Thiết lập đo khoảng cách nhận dạng*

		RFID thụ động	RFID chủ động
PHẦN CỨNG	READER	RFIDREAD-4100	MCU: MIMXRT1010 Halfbridge Driver: 2ED2108S06F, BSC0906NS LF antenna: AS705A
	TAG	EM4100	AS3933DEV-SYSTEM FRDM-KL03Z
Phần mềm			MCUXpresso
Dữ liệu			Giả lập 32 bits ID ngẫu nhiên trên Tag
Thiết bị		AFG21112	Oscilloscope DC supply: E3644A



Hình 12. *Khoảng cách nhận dạng và tần số*

Để đánh giá độ khả thi về mặt năng lượng khi dùng tag chủ động với chip AS3933, tác giả đo mức tiêu thụ năng lượng và chu kỳ Sleep, Wakeup của Keyfob.

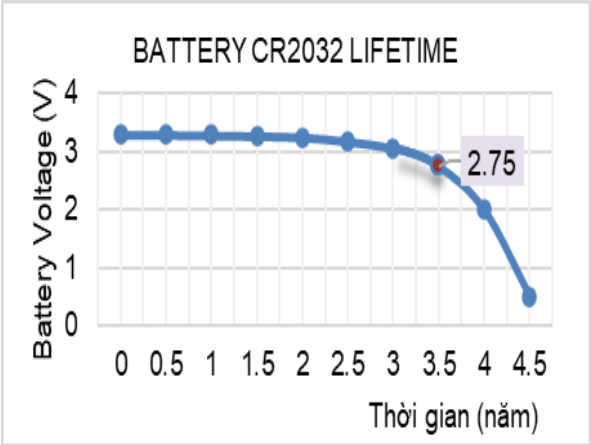
Bảng 3. *Dòng tiêu thụ của Keyfob*

Trạng thái keyfob	Thời gian (ms)	Dòng tiêu thụ (µA)
Sleep	950	3.2
Wakeup	50	90

Dễ tính được dòng tiêu thu trung bình của Keyfob:

$$I = \frac{950*3.2+50*90}{1000} = 7.540\mu A \qquad (6)$$

Với điện lượng 225mAh, pin CR2032 có thể ước tính được thời gian sử dụng theo biểu đồ sau:



Hình 13. *Biểu đồ tuổi thọ pin CR2032 dùng cho tag chủ động*[3]

Ở hình 13, với dòng tiêu thụ trung bình là 7,54µA, thời gian ước tính phải thay mới pin cho tag chủ động là 3,5 năm khi pin giảm dưới mức 2.75V là mức các linh kiện CMOS bắt đầu hoạt động không ổn định.

6. KẾT LUẬN

Mặc dù là công nghệ đã phát triển từ lâu, RFID chủ động và thụ động vẫn đóng vai trò rất lớn trong lĩnh vực nhận dạng. Đặc biệt kỹ thuật RFID chủ động 125kHz cho phép nhận dạng xác thực tin cậy trong phạm vi bán kính hẹp, với khả năng chống hack và truy cập trái phép cao, mức năng lượng tiêu thụ nhỏ, nó rất phù hợp cho ứng dụng nhận dạng chủ phương tiện mà hiện nay các hãng xe lớn trên thế giới đang áp dụng. Kỹ thuật bảo mật mã xác thực mà tác giải đề xuất phù hợp với các hệ thống vừa và nhỏ, ở đó tài nguyên MCU hạn hẹp nhưng vẫn yêu cầu đảm bảo tính bảo mật, hiệu quả. Kỹ thuật này cũng có thể được áp dụng cho các thiết bị UWB mà được dự đoán sẽ trở nên rất phổ biến trong tương lai gần.

[3] Tag bao gồm LF receiver AS3933, MCU KL03

TÀI LIỆU THAM KHẢO

[1] Nguyễn Văn Hiệp, "Công nghệ nhận dạng vô tuyến RFID", Khoa Điện-Điện tử, Đại học Sư phạm kỹ thuật TP. HCM, 2017
[2] Lei Cui, Zonghua Zhang, Nan Gao, Zhaozong Meng, Zhen Li, "Radio Frequency Identification and Sensing Techniques and Their Applications—A Review of the State-of-the-Art", 2019-September-17.
[3] Evizal, Tharek Abdul Rahman, Sharul Kamal Abdul Rahim. "Active RFID Technology for Asset Tracking and Management System" TELKOMNIKA, Vol.11, No.1, March 2013, pp 137-146, 2013
[4] Qinmiao Kang ; Zhifeng Xie ; Yongquan Liu ; Ming Zhou, "125KHz wake-up receiver and 433MHz data transmitter for battery-less TPMS", 2017 IEEE 12th International Conference on ASIC (ASICON), pp 1101-1104, 2017
[5] ScioSense, "AS3933 3D Low Frequency Wake-Up Receiver" Revision v1-08, 2015-Sept-02.

Tác giả chịu trách nhiệm bài viết:
Nguyễn Văn Xuân
Trường Đại học Công nghệ thông tin
Email: nvx1047hut@gmail.com