TRƯỜNG ĐẠI HỌC SÀI GÒN
TẠP CHÍ KHOA HỌC
ĐẠI HỌC SÀI GÒN
ISSN 1859 - 3208
Số 91, Tập 01/2024

SAIGON UNIVERSITY
SCIENTIFIC JOURNAL
OF SAIGON UNIVERSITY
No. 91, Vol 01/2024

Email: tcdhsg@sgu.edu.vn ; Website: http://sj.sgu.edu.vn/

THIẾT LẬP MÔ HÌNH BẢO MẬT KHÔNG ĐỐI XỨNG RSA VÀ PHÁT CHUYỂN TIẾP NHIỄU THÂN THIỆN ĐỂ CẢI THIỆN HIỆU QUẢ CHỐNG NGHE LÉN TRONG MẠNG IOT VÔ TUYẾN ĐA NGƯỜI DÙNG

Establish RSA security model and friendly interference relay to increase anti-eavesdropping effectiveness in multi-user wireless IoT network

Hồ Văn Cừu[1*], Trần Minh Nhật[1], Nguyễn Thị Hậu[1], Nguyễn Thị Thu Hằng[1]
[1]Trường ĐH Sài Gòn

TÓM TẮT

Ngày nay, mạng IoT vô tuyến phát triển rất nhanh về dung lượng, băng thông và yêu cầu bảo mật cao hơn. Đặc tính kênh truyền vô tuyến dễ bị gây nhiễu, kẻ nghe lén có thể truy xuất vào mạng để lấy cắp thông tin người dùng. Trong nghiên cứu này, chúng tôi đề xuất mô hình mạng IoT vô tuyến chuyển tiếp, phát nhiễu thân thiện, kết hợp với giải thuật bảo mật không đối xứng RSA để nâng cao hiệu năng truyền dữ liệu khả năng bảo mật, chống nghe lén.

Từ khóa: *Truy nhập vô tuyến IoT, bảo mật không đối xứng RSA, bảo mật lớp vật lý.*

ABTRACT

Today, wireless IoT networks are growing very quickly in terms of capacity, bandwidth and higher security requirements. Radio channel characteristics are susceptible to interference, eavesdroppers can access the network to steal user information. In this study, we propose a forwarding, interference wireless IoT network model, combined with the RSA asymmetric security algorithm to improve data transmission performance, security, and anti-eavesdropping capabilities.

Keywords: *IoT radio access, RSA asymmetric security, physical layer security.*

1. Tổng quan

1.1. Dẫn nhập

Để thực hiện bảo mật cho kênh truyền dữ liệu người dùng, Shannon, đã phát minh mã hóa kênh truyền [1], vừa chống được lỗi bít, vừa chống nghe lén, ưu điểm của phương pháp mã hóa là cách bảo mật trực tiếp, dễ thực hiện, nhược điểm là khi người nghe lén sử dụng các bộ vi xữ lý hiện đại, thì năng lực bẻ khóa thực hiện nhanh hơn, kênh truyền kém an toàn.

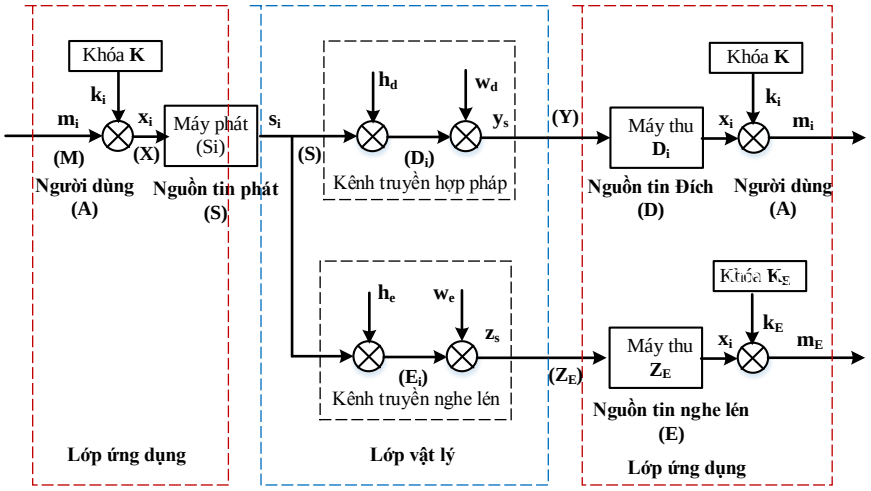
Mạng thông tin di động thế hệ thứ 3, thứ 4, đã ứng dụng kỹ thuật bảo mật trên lớp vật lý, các kết quả nghiên cứu trong [2], [7], tập trung vào chủ đề ứng dụng kỹ thuật trãi phổ trực giao OMA, kỹ thuật điều chế trực giao đa sóng mang OFDM, kỹ thuật đa truy nhập SIMO, MIMO để chống nhiễu fa-đing, và chống nghe lén. Tuy nhiên khi mạng di động hướng tới thế hệ thứ 5 và 6, dung lượng mạng IoT quá lớn, do đó, cần phải sử dụng kỹ thuật trãi

[*]Tác giả liên hệ: cuuhovan@sgu.edu.vn

phổ không trực giao NOMA, công nghệ mạng công tác chuyển tiếp, phát nhiễu thân thiện để nâng cao hiệu quả sử dụng băng thông và bảo mật cho kênh truyền người dùng hữu ích.

Các kết quả nghiên cứu của [6-9], đã thiết kế các cấu hình kênh truyền vô tuyến sử dụng kỹ thuật trãi phổ không trực giao NOMA, đa truy nhập MIMO, phân tích các tham số xác suất dừng OP, xác suất bảo mật IP, theo tỉ số SNR của kênh chính, kênh nghe lén, trên kênh truyền vô tuyến fa-đing. Trong nghiên cứu này, chúng tôi đề xuất mô hình kênh truyền cộng tác chuyển tiếp IoT vô tuyến phát chuyển tiếp nhiễu thân thiện kết hợp với giải thuật bảo mật không đối xứng RSA, việc sử dụng khóa bảo mật K tại đầu phát và đầu thu của kênh truyền chính sẽ tăng hiệu năng bảo mật cho hệ thống, chống nghe lén.

1.2. Mô hình hệ thống kênh truyền bảo mật Shannon



Hình 1. Mô hình kênh truyền bảo mật thông tin Shannon [1]

Mô hình kênh truyền bảo mật Shannon, như hình 1, trong đó, máy phát (S) truyền thông tin từ nguồn người dùng (A) tới máy thu đích (D), trên kênh truyền (H_d), với nguồn nhiễu (W_d), người nghe lén đặt máy thu (Z_E), để lắng nghe tín hiệu kênh truyền (S) và (D). Để chặn máy nghe lén (E) lấy thông tin, máy phát (S) cần phải mã hóa thông điệp của người dùng (A) thành các bản tin (M) với khóa mã bí mật (K) thành từ mã thông tin phát là (X), khóa mã bí mật (K) chỉ được biết tại máy thu (D) hợp pháp. Shannon sử dụng tham số Entropy điều kiện $H(m|x)$ tại máy nghe lén (E), để đo mức độ bảo mật của thông điệp sau khi đã mã hóa, hệ thống bảo mật hoàn hảo nếu $H(m|x)=H(m)$ hoặc độ rò rỉ thông tin đến máy nghe lén $I(m;x)=0$ với $I(m;x)$ là thông tin tương hổ của biến ngẫu nhiên m thông qua giá trị của biến ngẫu nhiên x. Bảo mật hoàn hảo chỉ đạt đươc nếu $H(k)\geq H(m)$, tức là độ bất định của khóa (K) phải lớn hơn độ bất định thông điệp (M).

1.3. Dung lượng bảo mật

Xét kênh nghe lén Gaussian như hình 1, với x là hàm tín hiệu ngõ ra máy phát;

y là hàm tín hiệu ngõ vào máy thu và z là hàm tín hiệu ngõ vào máy thu nghe lén. Quan hệ giữa kênh ngõ vào và kênh ngõ ra như sau [1]:

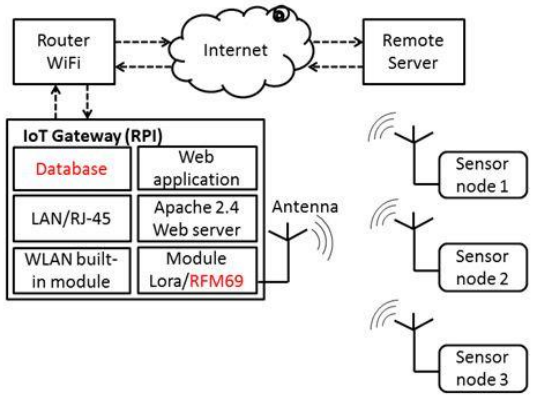
$$y_D = h_d x + w_d \quad (1)$$

$$y_E = h_e x + w_e \quad (2)$$

với h_d, h_e là hệ số kênh truyền và $w_d = (0, \sigma_d^2)$; $w_e = (0, \sigma_e^2)$ là công suất nhiễu của kênh truyền tại máy thu (D) và máy nghe lén (E). Dữ liệu mã hóa trên kênh vô tuyến là các biến ngẫu nhiên, $x(n) = [x_1, x_2, \dots, x_n]$, gọi $E[\cdot]$ là toán tử kỳ vọng, công suất trung bình tín hiệu thu là: $\bar{P} = \frac{1}{n}\sum_{i=0}^{n} E[|x_i|^2]$. Dựa theo công thức tính dung lượng kênh truyền $C(bps) = B_W(Hz)log_a(1 + \frac{S}{N})$, dung lượng bảo mật được định nghĩa như công thức sau:

$$C_S = max\left[log\left(1 + \frac{|h_d|^2.\bar{P}}{\sigma_d^2}\right) - log\left(1 + \frac{|h_e|^2.\bar{P}}{\sigma_e^2}\right)\right] \quad (3)$$

1.4. Mạng Iot vô tuyến



Hình 2: Kiến trúc của IoT vô tuyến [4]

Mạng IoT vô tuyến là hệ thống thiết bị cảm biến IoT vô tuyến được kết nối vào mạng internet qua kênh truyền vô tuyến như hình 2,[4]. Mô hình gồm có: *1. Thiết bị cảm biến/thiết bị IoT; 2. Thiết bị chuyển mạch kết nối trung kế gateway/hub; 3. Web Serve; 4. Thiết bị ứng dụng khác*. Trong đó gateway/hub có chức năng gửi/nhận thông tin giữa thiết bị IoT bằng cách sử dụng các giao thức mạng như Lora, ZigBee, Z-Wave, Bluetooth, TCP/IP và cho phép kết nối truy cập vào mạng internet.

1.3.1. Mã hóa bất đối xứng RSA

Có hai giải pháp bảo mật IoT là sử dụng phần cứng và giải pháp bảo mật bằng phần mềm. Giải pháp bảo mật dựa trên phần cứng, là thiết kế các mô-đun phần cứng chuyên dụng dựa trên dữ liệu gắn thẻ đến từ các nguồn dữ liệu của ứng dụng, bao gồm kiến trúc bộ xử lý và nhiều bộ nhớ, kẻ tấn công có thể thiết kế lại các thành phần phần cứng tương tự trên bo mạch, do đó, không an toàn. Đối với các giải pháp bảo mật phần mềm, thuật toán mã hóa/giải mã bất đối xứng RSA được sử dụng rộng rãi nhất, có hiệu quả cao[4][5]. Thuật toán RSA có hai công đoạn mã hóa ở phần phát và giải mã ở phần thu được thực hiện như sau [3-5]:

1. Mã hóa: Mã hóa là quá trình ngẫu nhiên hóa dữ liệu tin gốc (M) với khóa công khai (K) ở bên phát (A) và truyền cho người dùng (B), ký hiệu là bộ khóa mật mã C[(e, n)]; bên thu (B) nhận dữ liệu sau mã hóa và giải mã bằng khóa bí mật riêng, ký hiệu D[(d, n)]. Để mã hóa bản tin gốc (M), thì trước tiên chuyển bản tin (M) thành các bản tin thành phần (m), với điều kiện $(m < n)$. Quá trình tạo ra một cặp khóa bí mật theo các bước như sau:

Bước 1: Chọn ngẫu nhiên 2 số nguyên tố đủ lớn, độc lập là (p và q); p ≠ q; Bước 2: Tính (n = p.q); Bước 3: Tính giá trị hàm Euler $\emptyset(n) = (p-1).(q-1)$. Bước 4: Chon số nguyên tố [e], sao cho: 1≤ e ≤$\emptyset(n)$. Bước 5: Tính (d) sao cho: $\{(d.e) \equiv 1\ (mod\emptyset(n))\}$, hay tìm một số

tự nhiên (x), sao cho: $\{d = \frac{x.(p-1).(q-1)}{e}\}$, cũng là số tự nhiên, $[d \equiv mod(p-1)(q-1)]$. Khóa công khai, ký hiệu C[(e,n)], trong đó: (n mô-đun) và (e) là số mũ công khai hay mũ mã hóa. Khóa bí mật, ký hiệu D[(d,n)], trong đó (n mô-đun) xuất hiện trong khóa công khai và cả khóa bí mật và (d) là số mũ bí mật. Gọi (C) là bản tin sau mã hóa thành phần, có giá trị như sau: $C = m^e mod(n)$

Như vậy, bên phát (A) sẽ sử dụng khóa công khai để chuyển thông điệp ở dạng bản rõ (m) thành văn bản mật mã C. Quá trình giải mã thực hiện như sau:

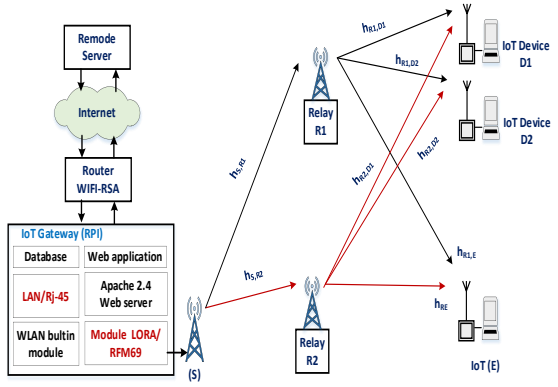
Bên thu B nhận được bản tin (C) ở định dạng văn bản mật mã, sau đó (B) sử dụng khóa riêng để chuyển văn bản mật mã thành văn bản gốc thành phần (m) theo phép toán: $m = C^d mod(n)$. Quá trình giải mã thực hiện được là vì:

$C^d \equiv (m^e)^d \equiv m^{ed}\ (mod\ (n))$;
do $e.d \equiv 1\ mod\ (p-1)$ và $e.d \equiv 1\ mod\ (q-1)$, nên $m^{ed} \equiv m\ mod\ (p)$ và $m^{ed} \equiv m\ mod\ (q)$

2. Thiết kế mô hình cấu trúc mạng vô tuyến cộng tác iot kết hợp giải thuật mã hóa bất đối xứng RSA

Kết quả nghiên cứu mạng cộng tác trong [2],[6],[8], đều chọn mô hình nhiều nhánh rơ-le chuyển tiếp đồng thời và lựa chọn rơ-le (R_S) chuyển tiếp theo tỷ lệ lỗi bit BER, tỷ lệ sử dụng năng lượng PA theo tỷ số tín hiệu trên tạp âm (SNR). Sử dung rơ-le chuyển tiếp dẫn đến hiệu suất phổ cao hơn; tuy nhiên, chi phí phần cứng và độ phức tạp cao hơn. Một số nghiên cứu mới gần đây [9-11] sử dụng công nghệ đa truy nhập không trực giao NOMA để mở rộng dung lượng kênh người dùng, và công nghệ truyền năng lượng và thông tin đồng thời (SWIPT), cho phép máy thu tại các nút mạng thu thập năng lượng vô tuyến song hành với thu tín hiệu thông tin, tín hiệu vô tuyến thu được sẽ chuyển đổi thành năng lượng cung cấp cho việc truyền phát tín hiệu chuyển tiếp, nâng cao hiệu suất sử dụng năng lượng, nên được gọi là hệ thống vô tuyến cộng tác xanh.

Nhóm nghiên cứu đề xuất phác thảo một mạng không dây IoT như hình 3, bao gồm nốt Hub-IoT nguồn (S), nốt chuyển tiếp có hai rơ-le IoT cộng tác (R_1, R_2) và nốt thiết bị IoT người dùng là (D_n); với n=(1,2,3), trong đó có 2 thiết bị IoT người dùng (D_n) và 1 thiết bị IoT nghe lén (E). Mô hình các rơ-le IoT vô tuyến chuyển tiếp cộng tác là (R_1) và (R_2), sử dụng giao thức giải mã chuyển tiếp (DF) để chuyển tiếp các tín hiệu đến các thiết bị IoT người dùng (D_n), sử dụng kỹ thuật phân chia khe thời gian SWIPT thành 2 nhóm khe thời gian truyền gọi là nhóm lẽ (T_1) và nhóm chẵn ($T_{2)}$, để truyền đồng thời tín hiệu thông tin và tín hiệu năng lượng (EH) cho các rơle IoT và sử dụng giao thức phân chia công suất PS có hệ số phân chia công suất là (λ_R.P). Chọn 1 rơ-le IoT để chuyển tiếp nguồn (S) và rơ-le IoT còn lại thực hiện chức năng gây nhiễu đến máy nghe lén (E).



Hình 3. Mô hình mạng IoT vô tuyến kết hợp bảo mật RSA

3. Phân tích mô hình toán mạng vô tuyến cộng tác IoT

Công suất tín hiệu thu năng lượng EH tại máy thu rơ-le (R_1), (R_2), [13-14] theo giao thức phân chia công suất PS, ứng với các khe thời gian truyền T_i, được viết theo các phương trình sau:

$$EH_{S,R_1}^{T_1} = \mu.\lambda_{R_1}.P.\sigma_{S,R_1} \quad (4)$$

$$EH_{S,R_2}^{T_1} = \mu.\lambda_{R_2}.P.\sigma_{S,R_2} \quad (5)$$

$$EH_{S,R_1}^{T_2} = \mu.\lambda_{R_1}.P.\sigma_{S,R_1} \quad (6)$$

$$EH_{S,R_2}^{T_2} = \mu.\lambda_{R_2}.P.\sigma_{S,R_2} \quad (7)$$

Trong đó, $T_1 = \sum_{k=0}^{n} t_i\,;\ i = 2k+1$, $T_2 = \sum_{k=0}^{n} t_i\,;\ i = 2k$, là tổng các khe thời gian lẽ và chẳn,.λi là hệ số phân chia công suất; $0 < \lambda_{R_1} < 1\,;\ 0 < \lambda_{R_2} < 1$, P là công suất phát tại nốt trung tâm IoT(S), μ là hệ số thu nhận tín hiệu, $0 < \mu < 1$; và độ lợi của kênh truyền tại IoT chuyển tiếp là $\sigma_{S,R_1} = E\left\{\left|h_{S,R_1}\right|^2\right\}$,và $\sigma_{S,R_2} = E\left\{\left|h_{S,R_2}\right|^2\right\}$. Khi nốt trung tâm IoT (S) phát chuỗi tín hiệu mã hóa các thông điệp $x_i;\ i = \{N,\dots,1\}$ đến các thiết bị IoT chuyển tiếp theo giải thuật phân chia công suất tương ứng với các nhóm khe thời gian, thì tín hiệu nhận được tại rơ-le IoT chuyển tiếp là (R_1, R_2) được thể hiện theo công thức như sau:

$$y_{R_1}^{T_1} = h_{S,R_1}.\sqrt{\left(1-\lambda_{R_1}\right).P}.\sum_{i=1}^{N}\left(\sqrt{\alpha_i}.x_i\right) + n_{R_1} \quad (8)$$

$$y_{R_2}^{T_1} = h_{S,R_2}.\sqrt{\left(1-\lambda_{R_2}\right).P}.\sum_{i=1}^{N}\left(\sqrt{\alpha_i}.x_i\right) + n_{R_2} \quad (9)$$

$$y_{R_1}^{T_2} = h_{S,R_1}.\sqrt{\left(1-\lambda_{R_1}\right).P}.\sum_{i=1}^{N}\left(\sqrt{\alpha_i}.x_i\right) + n_{R_1} \quad (10)$$

$$y_{R_2}^{T_2} = h_{S,R_2}.\sqrt{\left(1-\lambda_{R_2}\right).P}.\sum_{i=1}^{N}\left(\sqrt{\alpha_i}.x_i\right) + n_{R_2} \quad (11)$$

trong đó, n_{R_1}; n_{R_2} là công suất nhiễu của kênh truyền AWGN, $h_{S,R_1}; = h_{S,R_2}$ là hệ số suy hao kênh truyền vô tuyến Rayleigh tính theo khoảng cách từ IoT Hub (S), đến IoT chuyển tiếp (R_n), $h_{S,R_{i,i=1,2}} = g.d_{S,R_i}^{-\varepsilon}$; tương ứng với hệ số phân chia công suất PA cho rơ-le chuyển tiếp là $\alpha_i = \frac{i}{\sum_{n=1}^{N} n}$; $\sum_{i=1}^{N}\alpha_i = 1$. Tỷ số tín hiệu trên nhiễu SINR nhận được tại rơ-le IoT (R_r) trong khoảng thời gian truyền được thể hiện theo công thức như sau:

$$\gamma_{R_1-x_i}^{T_1} = \frac{\left(1-\lambda_{R_1}\right).\left|h_{S,R_1}\right|^2.\alpha_i.\rho}{\left(1-\lambda_{R_1}\right).\left|h_{S,R_1}\right|^2.\rho.\sum_{j=1}^{i-1}\alpha_j+1}, i = \{N,\dots,1\}, i > 1, \rho = \frac{P}{N_0} \quad (12)$$

$$\gamma_{R_2-x_i}^{T_2} = \frac{\left(1-\lambda_{R_2}\right).\left|h_{S,R_2}\right|^2.\alpha_i.\rho}{\left(1-\lambda_{R_2}\right).\left|h_{S,R_2}\right|^2.\rho.\sum_{j=1}^{i-1}\alpha_j+1}, i = \{N,\dots,1\}, i > 1, \rho = \frac{P}{N_0} \quad (13)$$

Ngưỡng tốc độ bit tức thời có thể đạt được thể hiện theo công thức toán như sau:

$$R_{R_1-x_i}^{T_1} = \frac{1}{2}log_2\left(1+\gamma_{R_1-x_i}^{T_1}\right); i = \{N,\dots,1\} \quad (14)$$

$$R_{R_2-x_i}^{T_2} = \frac{1}{2}log_2\left(1+\gamma_{R_2-x_i}^{T_2}\right); i = \{N,\dots,1\} \quad (15)$$

Trong khung thời gian thiết bị IoT(R) chuyển tiếp tín hiệu đến IoT người dùng (D_n) ứng với giao thức chuyển tiếp tín hiệu DF, và tín hiệu thu được tại thiết bị IoT (D_n) được thể hiện theo công thức như sau:

$$y_{D_n}^{T_1} = h_{S,R_1}.\sum_{i=1}^{N}\left(\sqrt{\alpha_i EH_{S,R_1}^{T_1}}.x_i\right) + n_{D_n} \quad (16)$$

$$y_{D_n}^{T_2} = h_{S,R_2}.\sum_{i=1}^{N}\left(\sqrt{\alpha_i EH_{S,R_2}^{T_1}}.x_i\right) + n_{D_n} \quad (17)$$

trong đó, n_{D_n} là tạp âm nhiễu trắng tại thiết bị đầu cuối D_n, và tỷ số tín hiệu trên nhiễu tức thời của các thiết bị IoT người dùng (D_n) sau giải mã tương ứng với luồng dữ liệu thu $x_i;\ i = \{N, \dots, 1\}$, có công thức biểu thị kết quả như sau:

$$\gamma_{D_n-x_i}^{T_1} = \frac{|h_{S,D_n}|^2.\alpha_i.\mu.\lambda_{R_1}.\sigma_{S,R_1}}{|h_{S,D_n}|^2.\alpha_i.\mu.\lambda_{R_1}.\sigma_{S,R_1}\sum_{j=1}^{i-1}\alpha_j+1}, i = \{N, \dots, 1\}, i > 1 \quad (18)$$

$$\gamma_{D_n-x_i}^{T_2} = \frac{|h_{S,D_n}|^2.\alpha_i.\mu.\lambda_{R_2}.\sigma_{S,R_2}}{|h_{S,D_n}|^2.\alpha_i.\mu.\lambda_{R_2}.\sigma_{S,R_2}\sum_{j=1}^{i-1}\alpha_j+1}, i = \{N, \dots, 1\}, i > 1 \quad (19)$$

Ngưỡng tốc độ bit tức thời có thể đạt được khi thiết bị IoT người dùng (D_n) giải mã các ký hiệu dữ liệu (x_i) được viết như sau:

$$R_{D_n-x_i}^{T_1} = \frac{1}{2}log_2\left(1+\gamma_{D_n-x_i}^{T_1}\right); i = \{N, \dots, 1\} \quad (20)$$

$$R_{D_n-x_i}^{T_2} = \frac{1}{2}log_2\left(1+\gamma_{D_n-x_i}^{T_2}\right); i = \{N, \dots, 1\} \quad (21)$$

Tương tự, có thể đề xuất mô hình toán cho kênh nghe lén (E). Nghiên cứu này đề xuất sử dụng IoT rơ-le (R_2) để truyền tín hiệu gây nhiễu tới thiết bị nghe lén (E), máy nghe lén nhận đồng thời tín hiệu từ rơ-le IoT chuyển tiếp (R_1) và rơ-le IoT (R_2) gây nhiễu như sau:

$$y_E^{T_1} = h_{R_{1,},E}.\sum_{i=1}^{N}\left(\sqrt{\alpha_i EH_{S,R_1}^{T_1}}.x_i\right) + h_{R_2,E}.\sum_{i=1}^{N}\left(\sqrt{\alpha_i EH_{S,R_2}^{T_1}}.x_i\right) + n_E \quad (22)$$

$$y_E^{T_2} = h_{R_{1,},E}.\sum_{i=1}^{N}\left(\sqrt{\alpha_i EH_{S,R_1}^{T_2}}.x_i\right) + h_{R_2,E}.\sum_{i=1}^{N}\left(\sqrt{\alpha_i EH_{S,R_2}^{T_2}}.x_i\right) + n_E \quad (23)$$

trong đó n_E là nhiễu {AWGN} tại máy nghe lén E, và tỷ số tín hiệu trên nhiễu sẽ là:

$$\gamma_{E-x_i}^{T_1} = \frac{|h_{S,E}|^2.\alpha_i.\mu.\lambda_{R_1}.\sigma_{S,R_1}}{\mu.\lambda_{R_1}.\rho.\left(|h_{R_1,E}|^2\sigma_{S,R_1}\sum_{j=1}^{i-1}\alpha_j+|h_{R_2,E}|^2\sigma_{S,R_2}\right)+1}, i = \{N, \dots, 1\}, i > 1 \quad (24)$$

$$\gamma_{E-x_i}^{T_2} = \frac{|h_{S,E}|^2.\alpha_i.\mu.\lambda_{R_2}.\sigma_{S,R_2}}{\mu.\lambda_{R_2}.\rho.\left(|h_{R_1,E}|^2\sigma_{S,R_2}\sum_{j=1}^{i-1}\alpha_j+|h_{R_1,E}|^2\sigma_{S,R_1}\right)+1}, i = \{N, \dots, n\}, i > 1 \quad (25)$$

Ngưỡng tốc độ bit tức thời có thể đạt được, sau khi máy nghe lén giải mã các ký hiệu dữ liệu (x_i), được viết theo công thức như sau:

$$R_{E-x_i}^{T_1} = \frac{1}{4} log_2\left(1 + \gamma_{E-x_i}^{T_1}\right); i = \{N, \dots, n\} \quad (26)$$

$$R_{E-x_i}^{T_2} = \frac{1}{4} log_2\left(1 + \gamma_{E-x_i}^{T_2}\right); i = \{N, \dots, n\} \quad (27)$$

Sử dụng lý thuyết về hàm mật độ công suất PDF, $f_{|h|^2}(x) = \frac{1}{\sigma} e^{\left(-\frac{x}{\sigma}\right)}; \sigma = E\{|h|^2\}$ và hàm phân bố công suất CDF $F_{|h|^2}(x) = 1 - \frac{1}{\sigma} e^{\left(-\frac{x}{\sigma}\right)}$, của kênh truyền vô tuyến Rayleigh, để tính công thức tính xác suất dừng của IoT rơ-le chuyển tiếp được tính theo công thức sau:

$$OP_{R_r}(t) = 1 - Pr\left\{mim\left\{R_{R_r-x_i}^{T_1}\right\} \geq R_t\right\};\ R_t\ là\ ngưỡng\ của\ tỷ\ số\ bit\ trên\ Hz \quad (28)$$

$$OP_{R_r}(t) = 1 - exp\left(-\frac{\gamma}{(1-\lambda_{R_r}).\beta.\rho.\sigma_{S,R_r}}\right);\ \beta = min\{\beta_i\};\ \beta_i = \begin{bmatrix} \alpha_i - \gamma.\sum_{j=1}^{i-1}\alpha_j\ if\ i > 1 \\ \alpha_i \qquad\qquad if\ i = 1 \end{bmatrix} \quad (29)$$

Tương tự, từ [1],[13-14], xác suất dừng của IoT người dùng (D_n) được tính như sau:

$$OP_{D_n}(t) = 1 - Pr\left\{mim\left\{R_{R_r-x_i}^{T_1}\right\} \geq R_t, mim\left\{R_{R_r-x_i}^{T_2}\right\} \geq R_t\right\};\ i = \{N, \dots, n\} \quad (30)$$

$$OP_{D_n}(t) = 1 - exp\left(-\frac{\gamma}{\Omega_n}\right);\ \Omega_n = mim\{\omega_n;\ \omega_m\} \quad (31)$$

Trong đó: $\omega_n = min\left\{\left(1 - \lambda_{R_r}\right).\beta_i.\rho.\sigma_{S,R_r}\right\}; i = \{N, \dots, n\}$ (32)

$$\omega_m = min\left\{\left(\lambda_{R_r}\right).\beta_i.\rho.\sigma_{S,R_{r,Dn}}\right\}; i = \{N, \dots, n\} \quad (33)$$

Từ [13-14], xác suất chặn của kênh nghe lén được tính theo công thức:

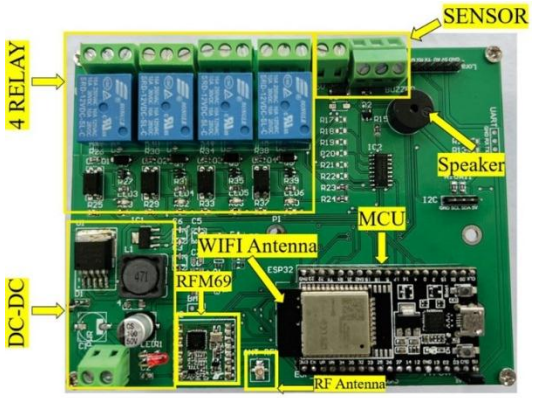
$$IP_{E\to D_n}(t) = 1 - Pr\left\{mim\left\{R_{R_r-x_i}^{T_1}\right\} \geq R_t, mim\left\{R_{E-x_i}^{T_2}\right\} \geq R_t\right\};\ i = \{N, \dots, n\} \quad (34)$$

$$IP_{E\to D_n}(t) \triangleq Pr\left\{mim\left\{R_{E-x_i}^{T_2}\right\} \geq R_t\right\};\ i = \{N, \dots, n\} \quad (35)$$

$$IP_{E\to D_n}(t) = max\left\{1 - \frac{\left(\alpha_i - \gamma.\sum_{j=1}^{i-1}\alpha_j\right).\sigma_{S,R_r}.\sigma_{R_r,E}}{\left(\alpha_i - \gamma.\sum_{j=1}^{i-1}\alpha_j\right).\sigma_{S,R_r}.\sigma_{R_r,E} + \partial.\gamma.\sigma_{S,R_r}.\sigma_{R_r,E}} \times exp\left(\left(-\frac{\gamma}{\lambda_{R_r}.\left(\alpha_i - \gamma.\sum_{j=1}^{i-1}\alpha_j\right).\rho.\sigma_{S,R_r}.\sigma_{R_r,E}}\right)\right)\right\};\ i = \{N, \dots, n\} \quad (36)$$

4. Thiết kế phần cứng mạng iot vô tuyến sử dụng giải thuật RSA

4.1. Cấu trúc phần cứng

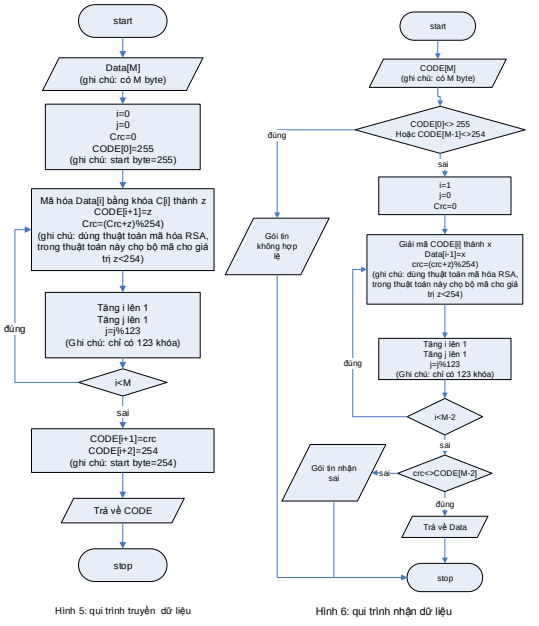


Hình 4: Phần cứng hệ thống IoT thực nghiệm, băng tần 433 MHz ISM [3].

Thiết kế phần cứng của gateway IoT và nút IoT được đề xuất như hình 3, trong đó hệ thống IoT gateway để giao tiếp với máy chủ và gửi/nhận thông tin đến/từ các nút cảm biến thông qua mạng RF. Nút IoT Hub được thiết kế cho hai chức năng chính là thu thập dữ liệu môi trường bằng cách sử dụng cảm biến và bật/tắt thiết bị truyền động thông qua rơ-le trên mạch AD. Các cảm biến được sử dụng bao gồm: 1. Cảm biến đo độ ẩm AM2302, cảm biến đo nhiệt độ SHT10, bộ truyền động có 4 chuyển mạch quang ESP32 (MCU)[9] được thiết kế để hoạt động ở chế độ bật/tắt, MCU sẽ bật / tắt từng rơ-le bằng cách gửi một mức logic (mức logic "1": bật, mức logic "0": tắt) cho các GPIO tương ứng. Mô đun kết nối vô tuyến RFM69HCW được chọn để kết nối các nút IoT với IoT gateway, nó là mô-đun thu phát có khả năng hoạt động trên dải tần rộng, bao gồm ISM 315 MHz, 915 MHz, 868 MHz và 433 MHz ISM. Dữ liệu đám mây (Google Firebase), Firebase là một dịch vụ cơ sở dữ liệu thời gian thực cho phép và hỗ trợ người dùng phát triển đa ứng dụng như web, ứng dụng di động (iOS, Android) và dữ liệu cảm biến phân loại bằng cách tích hợp các chức năng bộ công cụ máy học (ML) với lập trình phía máy chủ tối thiểu và các cấu hình phức tạp cho cơ sở dữ liệu back-end. Giao thức hoạt động của IoT gateway có thể tương tác với cơ sở dữ liệu Firebase thông qua kết nối internet.

4.2. Giải thuật bất đối xứng RSA

Chọn thuật toán bảo mật mã hóa bất đối xứng RSA với bộ mã hóa là **123 mã,** mỗi mã được chứa bởi 1 byte, tương đương 123 byte để dùng chung mã hóa và giải mã với giải thuật như hình vẽ 5, Bộ mã hóa:C[123], bộ giải mã: D[123], và bộ chung mã hóa và giải mã N[123], C[i] và N[i] dùng để mã hóa, D[i] và N[i] để giả mã, được sinh ra từ giải thuật tạo mã trong thuật toán RSA.



Hình 5. Giải thuật RSA

5. Thiết kế mô hình mô phỏng

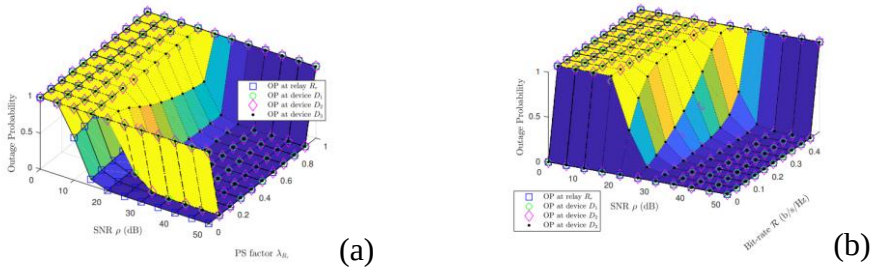
5.1. Tham số mô phỏng

Giả sử IoT gateway phát tín hiệu đến các rơ-le {IoT} công tác và chuyển tiếp dữ liệu đến các IoT người dùng được kết nối với nhau thành vòng kín, sử dụng công nghệ không trực giao NOMA. Chọn khoảng cách từ trung tâm {IoT} S đến rơ-le ghép nối (R_1) và (R_2) là bằng nhau và bằng 10 m. Mạng {IoT} hiển thị 2 thiết bị IoT người dùng là

(D_1) và (D_2) và thiết bị nghe lén (E)} có khoản cách lần lượt là 5m, 7m, 12m. Khung thời gian phát 2048 ms, tương ứng với 2048 mẫu, chia thành 2 khe (T_1) và (T_2), hệ số mũ suy hao kênh truyền vô tuyến fa-đing Rayleigh ε=4, hệ số phân chia công suất λ_R=0.4, hệ số phát nhiễu thân thiện δ=1, độ lợi kênh truyền tới rơ-le là $\sigma_{S,Rn}$=0,01, độ lợi kênh truyền tới IoT người dùng là σ_{Dn}=0,04, tỷ số bít lỗi lơn hơn 10^{-3}, điều chế BPSK, tương đương tỷ số Eb/N0 lớn hơn 10 dB. Sử dụng phần mềm mô phỏng Monte Carlo.

5.2. Kết quả mô phỏng

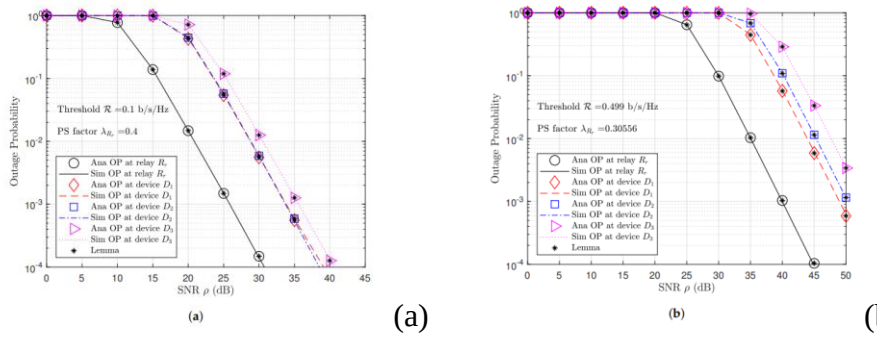
5.2.1. Xác suất dừng OP và xác suất bảo mật IP



(a) (b)

Hình 6. Đồ thi xác suất dừng OP tại các thiết bị IoT chuyển tiếp (R_r) và IoT người dùng

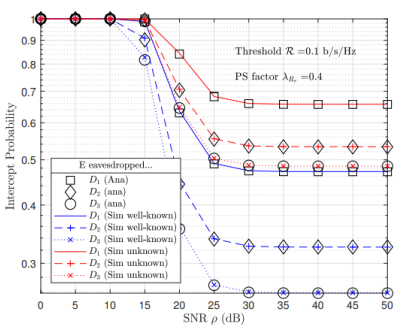
Hình 6.a, vẽ sơ đồ thị xác suất dừng OP theo tác động của hệ số phân bổ công suất {PS:λ_R} lên hiệu suất của xác suấy dừng{OP} khi rơ-le {IoT} chuyển tiếp (R_r) và IoT người dùng chọn ngưỡng tốc độ bit được xác định trước cố định tỷ số bít R=0,1 b/s/Hz, hệ số phân chia công suất PS (λ_R= 0,1, 0,2,…,1), tỷ số bít lỗi lơn hơn 10^{-3}, điều chế BPSK. Hình 6.b, vẽ sơ đồ thị xác suất dừng OP tại các rơ-le {IoT} và thiết bị IoT người dùng ghép nối; theo tác động của ngưỡng tốc độ bít, λ_R=0,4; và R = (0,1, 0.2, 0.3, 0,4) b/s/Hz, tỷ số bít lỗi lơn hơn 10^{-3}, điều chế BPSK. Kết quả: ngưỡng tốc độ bit được xác định trước thấp hơn R dẫn đến hiệu suất xác suất dừng tốt hơn (OP→0), tuy nhiên, thông lượng hệ thống thấp hơn yêu cầu; nếu ngưỡng tốc độ bit được xác định trước có giá trị nhỏ hơn 0,5 b/s/Hz và {SNR} lớn hơn 10 thì xác suất dừng tại tất cả các nút {IoT} sau đó có xu hướng bằng không, mặt khác, nếu ngưỡng tốc độ bit được xác định trước lớn hơn 0,5 b/s/Hz, thì xác suất dừng tại tất cả các nút {IoT} sau đó luôn có xu hướng về một. Như vậy ngưỡng tỷ số dung lượng bít R = 0,5 b/s/Hz là ngưỡng tốc độ bit tối ưu.



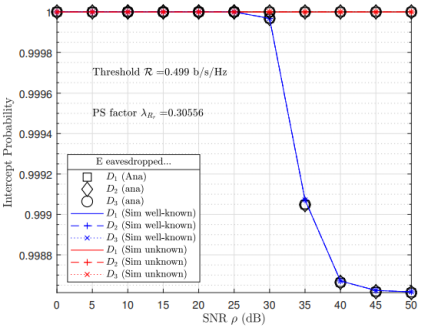
(a) (b)

Hình 7. Hiệu suất OP tại rơ-le {IoT}; a) hệ số PS cố định λ_R=0,4 và ngưỡng tốc độ bit cố định R = 0,1 b/s/Hz; (b) tốc độ bit được tối ưu hóa ngưỡng và các yếu tố PS.

Kết quả thông lượng hệ thống trong hình 5, có xu hướng đạt ngưỡng tốc độ bit được xác định trước khi tỷ số tín hiệu trên nhiễu SNR tiến tới vô cùng lớn. Ngưỡng tốc độ bit của thiết bị IoT được chọn R=0,499 b/s/Hz lớn hơn ngưỡng tốc độ bit cố định tại giá trị R=0,1 b/s/Hz. Xét trường hợp, tập lệnh truyền đến tại máy nghe lén E, máy nghe lén E đã chọn tín hiệu là công thức 30 cho giao thức {SIC} trong khối truyền lẻ và sau đó phát tín hiệu là 34 cho giao thức {SIC} trong khối truyền chẵn. Kết quả mô phỏng như hình 6, thiết bị nghe lén (E) có thể giải mã tin nhắn của các thiết bị hợp pháp từ tín hiệu nghe lén, có xác suất $IP_{E\text{-}Dn}$=0,2, tại SNR=30 dB. Tuy nhiên, hiệu suất của IP của người dùng nghe lén (E) $IP_{E\text{-}Dn}$ = 0,9986 tại SNR có giá trị lớn gần đến vô cùng.



(a)



(b)

Hình 8. Đồ thị biểu diễn hiệu suất IP của mạng {NOMA}-{IoT} hợp tác có tín hiệu gây nhiễu, (a) hệ số PS cố định λ_R=0,4 và ngưỡng tốc độ bit cố định R = 0,1 b/s/Hz; (b) tốc độ bit được tối ưu hóa ngưỡng và các yếu tố PS.

5.2.2. Kết quả mô phỏng giai thuật bảo mật RSA

Sau đây là một số kết quả thu được trong quá trình chạy thực nghiệm: Dữ liệu thô: {"PH":3,"EC":3}; dữ liệu dạng số: 7B225048223A332C224543223A337D; Dữ liệu cảm biến đo được sẽ được lưu trữ trong cơ sở dữ liệu Google Firebase như được hiển thị trong hình 7.

(a)

(b)

Hình 9. Giao diện chính của ứng dụng di động được đề xuất.

Giao diện Gateway IoT cập nhật đã điều khiển thành công vào thẻ "/status": để khẳng định nút IoT đã nhận được lệnh, thông báo xác nhận sẽ tải trở lại cơ sở dữ liệu Firebase với mã khác của thẻ ("/status"). Nút IoT gởi trả lời đã nhận lệnh

thành công: để khẳng định nút IoT đã nhận được thông báo, thông báo xác nhận sẽ tải trở lại gateway, các xác nhận này cũng phải được mã hóa. Phát hiện các sự kiện từ thẻ "/ status", xác nhận với Mobile App rằng nút IoT đã nhận thông báo người dùng.

Hình 10: Ảnh màn hình cài đặt lịch trình ứng dụng di động dùng hệ điều hành android

Từ sơ đồ được hiển thị trong hình 8, chúng ta có thể thấy cách tương tác giữa người dùng thiết bị di động và hệ thống phụ trợ Firebase có thể nhận được nhiều hơn các giá trị cảm biến và điều khiển rơ le trên nút IoT, chẳng hạn như lịch trình, cài đặt giá trị ngưỡng cho từng cảm biến.

6. Kết luận

Đề xuất mô hình kênh truyền cộng tác chuyển tiếp IoT vô tuyến phát chuyển tiếp nhiễu thân thiện kết hợp với giải thuật bảo mật không đối xứng RSA, việc sử dụng khóa bảo mật K tại đầu phát và đầu thu của kênh truyền chính sẽ tăng hiệu năng bảo mật cho hệ thống, chống nghe lén. Kết quả mô phỏng tìm được tối ưu hóa hiệu suất dừng OP và xác suất bảo mật IP, tại các giá trị mô phỏng là hệ số PS cố định λ_R=0,4 và ngưỡng tốc độ bit cố định R = 0,5 b/s/Hz.

Bằng cách sử dụng cơ sở dữ liệu Firebase thời gian thực và ứng dụng di động dùng hệ điều hành android, và thuật toán bảo mật RSA để thiết lập mô hình giám sát an toàn các thông số môi trường xung quanh trong các tòa nhà thông minh và các lĩnh vực nông nghiệp. Mô-đun bảo mật bộ thu phát không dây được triển khai RFM69HCW hoạt động ở băng tần wifi 433 MHz với thuật toán RSA 123 được thiết kế và thử nghiệm với các thông số cài đặt cụ thể của các loại cảm biến nhiệt độ, độ ẩm, trên di động dùng hệ điều hành android theo thời gian đáp ứng nhanh, mở ra nghiều triển vọng để phát triển nhiều ứng dụng thương mại khác nhau trong thực tế.

Từ viết tắt: *AF: Amplify-and-Forward; BER: Bit Error Rate; DF: Decode-and-Forward; IoT: Internet of thing; EH: Energy harvesting; NOMA: Non-othorgonal multiple access; OP: Outage Probability; SOP: Secrecy Outage Probability; IP: Intercept Probability*

TÀI LIỆU THAM KHẢO

[1] Nguyễn Anh Tuấn, Trần Thiên Thanh, Võ Nguyễn Quốc Bảo, (2018), *"Phân tích xác suất dừng hệ thống chuyển tiếp hai chiều sử dụng công nghệ thu thập năng lương từ nguồn phát"*, Tạp chí khoa học công nghệ thông tin và truyền thông, số 01 & 01, (CS01), 2018.

[2] R. S. Denavit, Jacques; Hartenberg, (2021) "*A kinematic notation for lower-pair mechanisms based on matrices"*. Trans ASME J. Appl. Mech 23: 215–221."

[3] NIST, "*Advanced Encryption Standard:U.S. National Institute of Standards and Federal Information Processing Standards Publication (FIPS PUBS)*" vol. Vol.197, 2. 2018

[4] PKCS,"*RSA, Public-Key Cryptography Standards (PKCS)*", RSA Cryptography Specifications Version 2.1, 2003."

[5] Hellman Groups, "*Security techniques, Available*"; 2020; *(https://wiki.mikrotik.com)*

[6] Qian, L.P.; Feng, A.; Huang, Y.; Wu, Y.; Ji, B.; Shi, Z. *"Optimal SIC ordering and computation resource allocation in MEC-aware NOMA NB-IoT networks*". IEEE Internet Things J. 2018, 6, 2806–2816.

[7] Qian, L.P.; Shi, B.; Wu, Y.; Sun, B.; Tsang, D.H. "*NOMA-enabled mobile edge computing for Internet of Things via joint communication and computation resource allocations*". IEEE Internet Things J. 2019, 7, 718–733.

[8] Khan, W.U.; Jameel, F.; Sidhu, G.A.S.; Ahmed, M.; Li, X.; Jäntti, R. Multiobjective, "*Optimization of uplink NOMA-enabled vehicle-to-infrastructure communication*". IEEE Access 2020, 8, 84467–84478. 2020

[9] Tran, T.N.; Voznak, M. Switchable,*"Coupled Relays Aid Massive Non-Orthogonal Multiple Access Networks with Transmit Antenna Selection and Energy Harvesting*". Sensors 2021, 21, 1101, (2021).

[10] Yang, Z.; Ding, Z.; Fan, P.; Al-Dhahir, N. *"The impact of power allocation on cooperative non-orthogonal multiple access networks with SWIPT*". IEEE Trans. Wirel. Commun. 2017, 16, 4332–4343.

[11] Tran, T.N.; Voznak, M.; Fazio, P.; Ho, V.C."*Emerging cooperative MIMO-NOMA networks combining TAS and SWIPT protocols assisted by an AF-VG relaying protocol with instantaneous amplifying factor maximization*", Aeu-Int. J. Electron. Commun. 2021, 135, 153695.

[12] Tran, T.N.; Vo, T.P.; Fazio, P.; Voznak, M. *"SWIPT Model Adopting a PS Framework to Aid IoT Networks Inspired by the Emerging Cooperative NOMA Technique*". IEEE Access 2021, 9, 61489–61512 ; 2021.

[13] Lv, L.; Zhou, F.; Chen, J.; Al-Dhahir, N. *"Secure Cooperative Communications With an Untrusted Relay: A NOMA-Inspired Jamming and Relaying Approach*". IEEE Trans. Inf. Forensics Secur. 2019, 14, 3191–3205. 2019

[14] Perera, T.D.P.; Jayakody, D.N.K. "*Analysis of time-switching and power-splitting protocols in wireless-powered cooperative communication system*", Phys. Commun. 2018, 31, 141–151. 2018

Ngày nhận bài: 17/11/2023 Ngày chấp nhận đăng: 04/01/2024