Mã hóa dữ liệu AES đường truyền kết nối ZigBee và IoT trong giám sát nước thải công nghiệp

Nguyễn Hữu Trung, Hà Duyên Trung, Nguyễn Thanh Bình

***Tóm tắt*— Bài báo này trình bày kỹ thuật mã hóa dữ liệu môi trường sử dụng tiêu chuẩn mã hóa tiên tiến AES (Advanced Encryption Standard) trong Internet kết nối vạn vật (IoT) kết hợp đường truyền ZigBee vô tuyến tầm ngắn để giám sát nước thải công nghiệp thời gian thực. Trong một số ứng dụng giám sát mang tính đặc thù của mạng IoT, bảo mật dữ liệu đường truyền vô tuyến có ý nghĩa đặc biệt quan trọng. Chúng hạn chế được sự mất mát thông tin do can thiệp vào kênh vật lý bởi bên thứ ba. Chúng tôi lần lượt trình bày cơ bản về một hệ thống IoT sử dụng công nghệ truyền dẫn ZigBee cho mục tiêu giám sát thông số môi trường nước thải công nghiệp. Mẫu sản phẩm phần cứng và phần mềm đã được thực hiện và thử nghiệm dựa trên ba thông số cơ bản của nước là độ pH, độ đục và nhiệt độ. Dữ liệu môi trường sẽ được mã hóa tại các thiết bị đầu cuối IoT trước khi truyền về trung tâm. Các kết quả thử nghiệm bước đầu đánh giá được sự thay đổi theo thời gian các thông số môi trường nước thải công nghiệp, dữ liệu này cũng được so sánh với dữ liệu thu thập được từ mẫu nước sinh hoạt trong cùng điều kiện thí nghiệm.**

***Abstract*— This paper presents environmental data encryption technique using the advanced AES (Advanced Encryption Standard) in the Internet of Things (IoT) combines ZigBee short-range radio transmission links to monitor industrial wastewater in real time. In a number of IoT-specific surveillance applications, the data encryption of radio transmission link is particularly important. It limits the hacked information due to interference with physical channels by third parties. Particularly, we present an IoT system using ZigBee transmission technology for the purpose of monitoring industrial wastewater environment parameters. Prototypes of hardware and software versions were implemented and tested based on three basic parameters of water: pH, turbidity and temperature. Environmental data will be encrypted at the end IoT device before transmitting to the data cloud center. The initial test results assess the change over time of industrial wastewater environment parameters, these data are also compared with that collected from pure water samples under the same experimental conditions.**

***Từ khóa:* Bảo mật IoT; ZigBee; thuật toán AES; nước thải công nghiệp .**

***Keywords*: – IoT security, ZigBee, AES algorithm, wastewater.**

Bài báo được nhận ngày 03/09/2019. Bài báo được nhận xét bởi phản biện thứ nhất vào ngày 05/10/2019 và được chấp nhận đăng vào ngày 16/10/2019. Bài báo được nhận xét bởi phản biện thứ hai vào ngày 06/10/2019 và được chấp nhận đăng vào ngày 20/10/2019.

I. GIỚI THIỆU

Trong những năm gần đây, IoT đã trở thành một chủ đề quan trọng về công nghệ và công nghiệp. IoT bao gồm các thiết bị vật lý như tủ lạnh, ô tô, tòa nhà, hệ thống theo dõi sức khỏe và nhiều thiết bị khác được gắn cảm biến, bộ truyền động, thẻ nhận dạng tần số vô tuyến (RFID) và phần mềm. Những vật này (things) được kết nối với mạng (Internet) cho phép chúng trao đổi và thu thập dữ liệu. IoT đã và đang thay đổi cách nhìn về Internet từ tĩnh thành động [1]. Zigbee, Z-Wave, 6LoWPAN, Wi-Fi, GSM/3G/4G/ LTE, LoRa và Sigfox là những công nghệ truyền dẫn vô tuyến quan trọng được sử dụng trong các hệ IoT. Hiện tại, Zigbee là công nghệ được sử dụng nhiều nhất trong ứng dụng nhà thông thông minh. Zigbee dự kiến sẽ chiếm 34% thị phần smart-home, smart-building và 29% thị trường chiếu sáng thông minh vào năm 2021 với tỷ lệ tăng trưởng hàng năm (GACR) là 26% trong giai đoạn 2016-2020 [2]. Sự tăng trưởng nhanh chóng của việc sử dụng IoT và công nghệ Zigbee đã thu hút sự chú ý của các nhà nghiên cứu để điều tra các mối quan tâm bảo mật mà ngành công nghiệp IoT phải đối mặt.

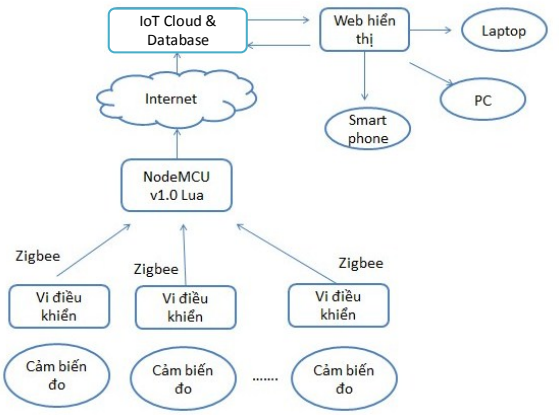
Bảo mật IoT trong công nghệ truyền dẫn là mối quan tâm của nhiều nhà nghiên cứu và công ty tư nhân. Symantec đã báo cáo rằng, 52% ứng dụng y tế được kết nối với thiết bị đeo được không có chính sách bảo mật và 20% thông tin cá nhân, thông tin đăng nhập và mật khẩu có trong các văn bản [3]. Vào tháng 5/2014, hơn 90 người từ 19 quốc gia khác nhau có liên quan đến các trò chơi creepware đã bị FBI và cảnh sát bắt giữ vì sử dụng webcam kết nối Internet để theo dõi mọi người [4].

Nhiều nhà nghiên cứu cũng phát hiện ra rằng, nhiều xe ô tô, bệnh viện, lưới dầu và lưới năng lượng được kết nối với hệ thống IoT dễ bị tấn công mạng [5]. Đối với các mối quan tâm về bảo mật của Zigbee, nhiều nghiên cứu và nhiều thử nghiệm đã được thực hiện để hiểu rõ hơn về các mối đe dọa bảo mật mà nó dễ bị ảnh hưởng [6]-[11]. Mặc dù giao thức Zigbee có thể bị hack theo nhiều cách khác nhau, các công trình nghiên cứu đã chỉ ra rằng, việc giải quyết các vấn đề bảo mật trong IoT không chỉ phụ thuộc vào việc bảo mật các thiết bị IoT và công nghệ truyền dẫn, mà còn bảo vệ toàn bộ hệ thống IoT cũng như phát triển một nền tảng giải pháp IoT đầy đủ bao gồm nhiều lớp bảo mật [12]-[17].

Các mối đe dọa bảo mật của giao thức Zigbee có thể được chia thành: các cuộc tấn công yêu cầu thỏa hiệp khóa và tấn công với thỏa hiệp khóa không được yêu cầu. Để ngăn chặn việc kẻ tấn công chiếm lại khóa Zigbee, các khóa phải được tải sẵn ngoài băng và không thể truyền qua môi trường vô tuyến, và vị trí của thiết bị Zigbee phải được bảo vệ. Bài báo này tập trung vào mã hóa dữ liệu tại thiết bị đầu cuối Zigbee sử dụng thuật toán AES. Chúng tôi sử dụng module PH Sensor E-201-C để đo nhiệt độ và PH của nước, cảm biến đo độ đục để đánh giá độ đục của nước. Các thông số sau khi đo đạc, được xử lý và thực hiện mã hóa dữ liệu AES bằng board Arduino UNO R3 và được gửi đi bằng module ZigBee Xcore2530. Dữ liệu sau khi nhận tại bên thu sẽ được giải mã và đưa lên máy chủ cơ sở dữ liệu và đám mây IoT. Bên phía người dùng, Web hiển thị được phát triển để hiển thị dữ liệu dạng bảng biểu (bảng số liệu, biểu đồ, bảng so sánh giá trị…).

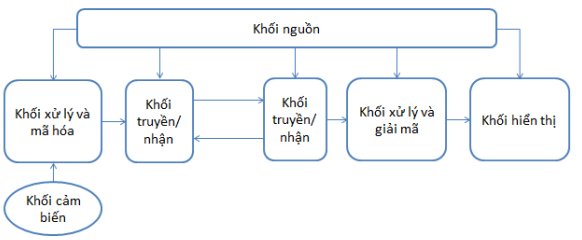
Phần còn lại của bài báo này được tổ chức như sau: Mục II trình bày về thiết kế và thực thi hệ thống, bao gồm thiết kế và thi công phần cứng, phát triển phần mềm mã hóa AES. Các kết quả mã hóa dữ liệu đo đạc cũng như giám sát các thông số môi trường nước được trình bày và thảo luật trong Mục III. Cuối cùng là Mục kết luận.

II. THIẾT KẾ VÀ THỰC THI HỆ THỐNG



Hình 1. Mô hình kiến trúc hệ thống

Một hệ thống giám sát sử dụng công nghệ truyền thông ZigBee được thể hiện chi tiết như trên Hình 1. Chúng bao gồm các khối chức năng sau đây: (1) khối nguồn cung cấp nguồn cho các thiết bị hoạt động; (2) khối cảm biến: Dùng cảm biến đo đạc các thông số cần thiết; (3) khối xử lý và mã hóa: thực hiện xử lý và mã hóa dữ liệu; (4) khối truyền/nhận thực hiện truyền/nhận dữ liệu bằng công nghệ ZigBee; (5) khối xử lý và giải mã thực hiện xử lý và giải hóa dữ liệu; (6) khối hiển thị để đưa ra số liệu lên SQL server và hiển thị ra web hiển thị trực quan.

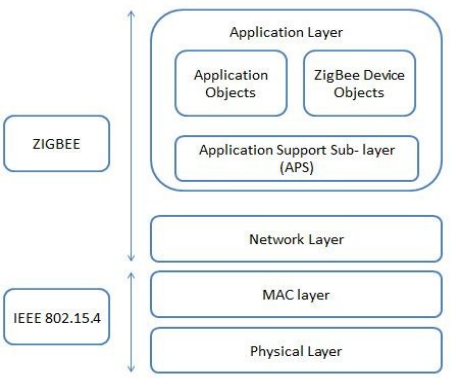


Hình 2. Sơ đồ khối chức năng thiết bị đầu cuối phát/thu kết hợp mã hóa

Hình 2 trình bày sơ đồ tổng quát của bị đầu cuối phát/thu kết hợp mã hóa. Khối xử lý và mã hóa với khối truyền nhận, khối truyền nhận với khối xử lý và giải mã giao tiếp với nhau theo chuẩn giao tiếp truyền nhận dữ liệu không đồng bộ (UART - Universal Asynchronous Receive/Transmit). Vì là giao tiếp không đồng bộ nên thiết bị ở bên truyền và bên nhận phải

thống nhất về khung truyền và tốc độ truyền. Cụ thể trong hệ thống được thực hiện với Baud rate = 38400, số bit dữ liệu =8, không có bit chẵn lẻ.

Trong hệ thống này, ZigBee là giao thức mạng không dây được dùng để kết nối các thiết bị với nhau. Công nghệ ZigBee được xây dựng dựa trên tiêu chuẩn 802.15.4 của tổ chức IEEE. Tiêu chuẩn 802.15.4 sử dụng tín hiệu radio có tần sóng ngắn, và cấu trúc của 802.15.4 có 2 tầng là tầng vật lý và tầng MAC (Medium Access Control). Công nghệ ZigBee vì thế cũng dùng sóng radio và có 2 tầng này. Hơn thế nữa ZigBee còn thiết lập các tầng khác nhờ thế mà các thiết bị của các hãng dù khác nhau nhưng cùng tiêu chuẩn có thể kết nối với nhau và vận hành trong vùng bảo mật của hệ thống [18]. Nhờ chức năng điều khiển từ xa không dây, truyền dữ liệu ổn định, tiêu thụ năng lượng cực thấp, công nghệ mở đã giúp công nghệ ZigBee trở nên hấp dẫn cho các ứng dụng hiện nay, đặc biệt là ứng dụng kết nối truyền dữ liệu tầm ngắn (phạm vi 75m) trong các hệ thống IoT.



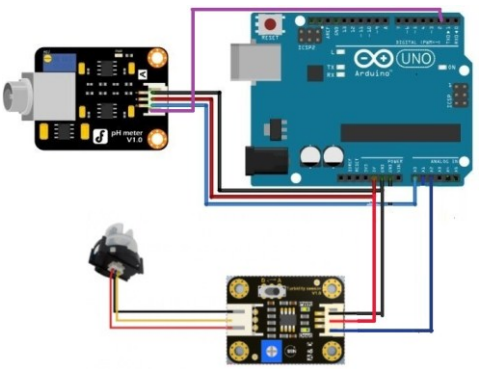
Hình 3. Cấu trúc giao thức ZigBee [18]

Các dữ liệu được truyền theo gói, gói tối đa là 128 bytes cho phép tải xuống tối đa 104 bytes. Tiêu chuẩn này hỗ trợ địa chỉ 64bit cũng như địa chỉ ngắn 16bit. Loại địa chỉ 64bit chỉ xác định được mỗi thiết bị có cùng 1 địa chỉ IP duy nhất. Khi mạng được thiết lập, những địa chỉ ngắn có thể được sử dụng và cho phép hơn 65000 nút được liên kết. Ngoài 2 tầng vật lý và tầng MAC xác định bởi tiêu chuẩn 802.15.4, tiêu chuẩn ZigBee còn có thêm các tầng trên của hệ thống bao gồm: tầng mạng, tầng hỗ trợ ứng dụng, tầng đối tượng thiết bị và các đối tượng ứng dụng. Cấu trúc giao thức ZigBee được thể hiện như trên Hình 3.

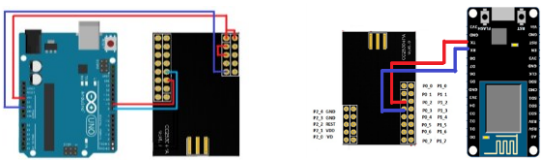
Mạng ZigBee có 3 dạng hình được hỗ trợ: mạng hình sao, mạng hình lưới và mạng hình cây. Mỗi dạng hình đều có những ưu điểm riêng và được ứng dụng trong các trường hợp khác nhau. Trong bài báo này, chúng tôi sử dụng kiến trúc mạng hình sao với nút điều phối trung tâm (coordinator) và các thiết bị đầu cuối (end device).

A. Thiết kế và thi công phần cứng

Thực hiện phương án mã hóa dữ liệu thông qua sơ đồ kết nối mô đun cảm biến với mô đun xử lý và mã hóa thể hiện trên Hình 4. Sơ đồ kết nối chân tín hiệu giữa khối xử lý và mã hóa với module truyền nhận ZigBee được thể hiện như trên Hình 5.



Hình 4. Sơ đồ kết nối chân giữa mô đun cảm biến với module xử lý và mã hóa



Hình 5. Sơ đồ kết nối chân giữa khối xử lý và mã hóa với module truyền nhận

Chúng tôi sử dụng các cảm biến đo PH, E-201-C, đo nhiệt độ, DS18B20, và đo độ đục module cảm biến đo pH (Hình 6a) bao gồm 1 cảm biến đo pH hay còn gọi là đầu dò pH và một board mạch điều hòa tín hiệu có đầu ra tỉ lệ với giá trị pH và có thể giao tiếp trực tiếp với bất kì vi điều khiển nào. Một điện cực pH được cấu tạo bởi hai loại thủy tinh. Thân điện cực được làm bằng loại thủy tinh không dẫn điện, đầu điện cực có dạng hình cầu và cấu tạo bởi loại thủy tinh có công thức gồm các oxit, sillica, lithium, canxi và các nguyên tố khác

cho phép ion lithiun xuyên qua. Cấu trúc của điện cực thủy tinh cho phép ion lithium trao đổi với các ion hydro trong chất lỏng tạo thành lớp thủy hợp. Một điện thế cỡ mV được sinh ra giữa tiết diện của đầu thủy tinh đo pH với dung dịch lỏng bên ngoài. Độ lớn của điện thế này phụ thuộc vào giá trị pH của dung dịch.

(a) Cảm biến đo PH, E-201-C

(b) Cảm biến đo nhiệt độ, DS18B20

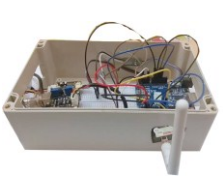
(c) Cảm biến đo độ đục

Hình 6. Các loại cảm biến được sử dụng

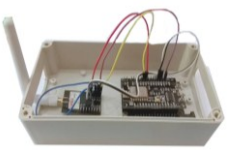
Cảm biến DS18B20 chống nước, đây là loại cảm biến kỹ thuật số đo nhiệt độ của hãng MAXIM với độ phân giải cao (12bit). Cảm biến sử dụng giao tiếp 1 dây rất gọn gàng và có chức năng cảnh báo nhiệt độ khi vượt ngưỡng. Cảm biến độ đục phát hiện chất lượng nước bằng cách đo mức độ đục. Nó sử dụng ánh sáng để phát hiện các hạt lơ lửng trong nước bằng cách đo độ truyền ánh sáng và tốc độ tán xạ, thay đổi theo tổng lượng chất rắn lơ lửng (TSS) trong nước. Khi TSS tăng, mức độ đục của chất lỏng tăng và ngược lại. Cảm biến chất lỏng này cung cấp chế độ đầu ra tín hiệu analog và digital.

Biểu thức biểu thị mối quan hệ giữa độ đục (Y) và điện thế (X) là: $Y = -1120.4X^2 + 5742.3X - 4352.9$. Chẳng hạn, khi đo được điện áp V=3 (V) => độ đục = 2790 (NTU).

Hình 7 mô tả bộ sản phẩm thiết bị đầu cuối phát/thu ZigBee phục vụ đo lường và mã hóa 3 tham số môi trường nước.



(a) Bộ phát Zigbee



(b) Bộ thu Zigbee

Hình 7. Bộ thiết bị đầu cuối phát/thu ZigBee

B. Phát triển phần mềm

1. Phương pháp mã hóa AES

AES là một thuật toán mã hóa khóa đối xứng với độ dài khóa 128 bits, 192 bits và 256 bits tương ứng được gọi là AES-128, AES-192 và AES-256. Chúng lần lượt sử dụng 10 vòng (round), 12 vòng và 14 vòng [18]. Vòng lặp chính của AES thực hiện các hàm sau: SubBytes(), ShiftRow(), MixColumns() và AddRoundKey(). Trong đó, ba hàm đầu của một vòng AES được thiết kế để ngăn chặn phân tích mã bằng phương thức "mập mờ" (confusion) và phương thức "khuếch tán" (diffusion), còn hàm thứ tư mới thực sự được thiết kế để mã hóa dữ liệu.

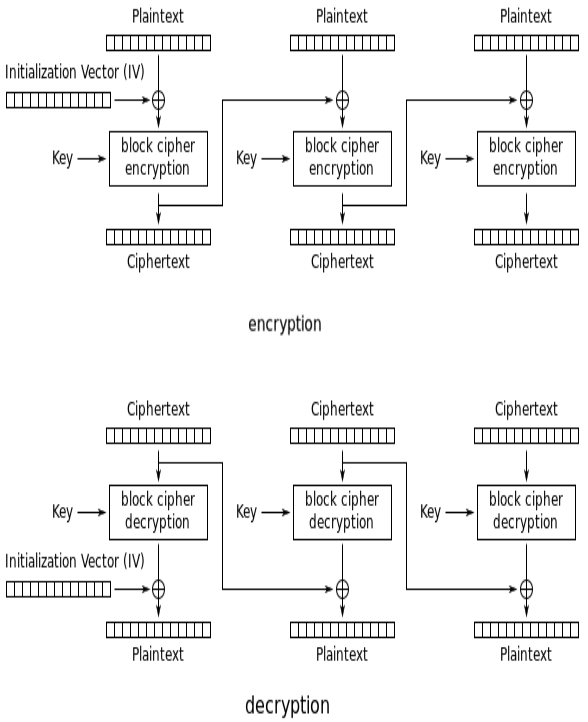
Trong thuật toán AES, độ dài khóa mã K có thể là 128,192 hay 256 bits. Độ dài khóa được biểu diễn bằng Nk=4, 6 hoặc 8 thể hiện số lượng các từ 32 bits (số cột) của khóa mã. Đối với thuật toán mã hóa AES, số vòng được thay đổi trong quá trình thực hiện thuật toán phụ thuộc và kích cỡ khóa. Số vòng này được ký hiệu là Nr=10 khi Nk=4, Nr=12 khi Nk=6 và Nr=14 khi Nk=8.

Đối với phép mã hóa và phép giải mã, thuật toán AES sử dụng một hàm vòng gồm bốn phép biến đổi byte như sau: Phép thay thế byte (một nhóm gồm 8 bit) sử dụng một bảng thay thế (Hộp-S), phép dịch chuyển hàng của mảng trạng thái theo các offset khác nhau, phép trộn dữ liệu trong mỗi cột của mảng trạng thái, phép cộng khóa vòng và trạng thái.

Vector khởi tạo trong mật mã hóa: Trong mật mã, một vecto khởi tạo (IV) là một khối bit được yêu cầu để cho phép một mật mã dòng hoặc một mã khối được thực hiện ở bất kỳ chế độ tuyến tính hoạt động để tạo ra luồng duy nhất độc lập với các luồng khác được tạo ra bởi cùng một khóa mã hóa, mà không phải trải qua quá trình tái tạo keying.

Thông thường, để mã hóa một đoạn dữ liệu độ dài bất kì, người ta phải chia khối đó thành những block đơn vị rồi mã hóa cho từng khối đó [18]. Để tăng độ phức tạp cho việc mã hóa, người ta có thể tạo ra mối liên hệ giữa các block với nhau. Chế độ liên kết khối mã CBC (Cipher block Chaining) là phương pháp mã hóa mà mỗi khối bản rõ được XOR với khối mã hóa trước đó trước khi được mã hóa. Có các đặc điểm: Không có khối nào có thể mã hóa mà

không mã hóa tất cả các khối trước nó; Một vector khởi tạo phải được sử dụng cho khối đầu tiên. Nó có thể ngẫu nhiên, giả ngẫu nhiên hoặc được sử dụng over and over (lặp đi lặp lại).



Hình 8. Chế độ CBC trong mã hóa và giải mã hóa AES

Chuẩn mã hóa Base64: Sau khi mã hóa bằng thuật toán mã hóa AES, nhưng kết quả thu được dưới dạng các hexcode. Đây là do trong quá trình mã hóa/giải mã, AES làm việc với các dữ liệu thô ở dạng nhị phân, chứ không phải các chuỗi, vậy nên thông tin này sẽ khó đọc và thường là khó truyền đi qua Internet (dễ mất mát). Do đó trước khi truyền đi, ta mã hóa toàn bộ dữ liệu thô này về dạng Base64. Nó là một chương trình mã hóa chuỗi ký tự bằng cách thay thế các ký tự trong bảng mã ASCII 8 bits thông dụng thành bảng mã 6 bit.

Chuẩn Base64 là một tập hợp gồm các ký tự (theo đúng thứ tự): từ A đến Z, từ a đến z, từ 0 đến 9, dấu +, dấu /. Tổng cộng là 64 ký tự biểu diễn 64 giá trị từ 0 đến 63. Như vậy, ký tự từ A đến Z biểu diễn cho các giá trị từ 0 đến 25, từ a đến z biểu diễn cho giá trị từ 26 đến 51, từ 0 đến 9 biểu diễn cho giá trị từ 52 đến 61, dấu + biểu diễn cho giá trị 62, dấu / biểu diễn cho giá trị 63. Một ký tự biểu diễn theo mã ASCII sẽ dùng 8 bits. Một ký tự theo Base64 sẽ dùng 6 bits. Như vậy, một file ở dạng Base 64 sẽ có kích thước lớn hơn khi ở dạng ASCII (cụ thể sẽ lớn gấp 4/3). Để chuyển đổi file sang dạng Base64, ta thực hiện theo trình tự sau:

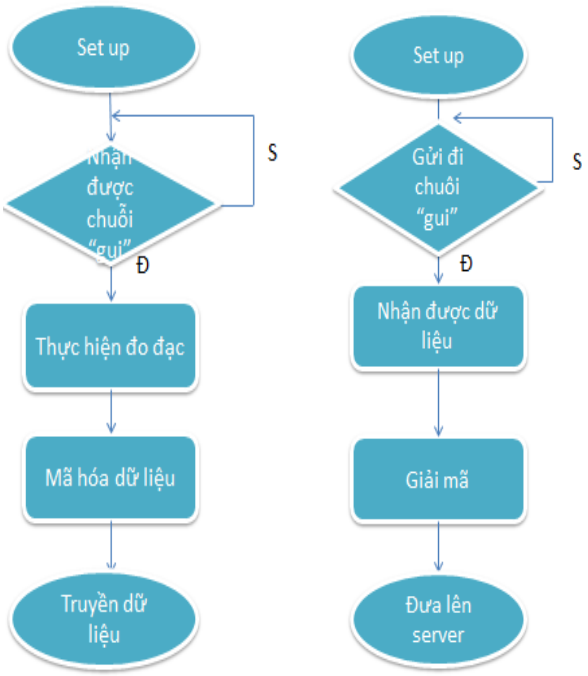
1: Đọc nội dung file dưới dạng bit;

2: Tách mỗi 6 bit thành một nhóm để xử lý;

3: Tra bảng mã Base 64, mỗi nhóm 6 bits sẽ có giá trị tương ứng với một ký tự;

4: Ghi ra các ký tự đó.

2. Lưu đồ thuật toán mã hóa



Hình 9. Lưu đồ thuật toán phía bên truyền (bên trái) và phía bên nhận (bên phải)

- Mã hóa bên truyền dữ liệu đo đạc

Trong quá trình mã hóa, chúng ta sử dụng khóa: Key = {0x15, 0x2B, 0x7E, 0x16, 0x28, 0xAE, 0xD2, 0xA6, 0xAB, 0xF7, 0x15, 0x88, 0x09, 0xCF, 0x4F, 0x3C, 0x15, 0x2B, 0x7E, 0x16, 0x28, 0xAE, 0xD2, 0xA6, 0xAB, 0xF7, 0x15, 0x88, 0x09, 0xCF, 0x4F, 0x3C}; và sử dụng vector khởi tạo: Dec_iv = {0, 0, 0x15, 0, 0, 0, 0x3B, 0, 0, 0, 0, 0, 0, 0, 0, 0}.

- Giải mã hóa bên nhận dữ liệu đo đạc

Gửi chuỗi đi địa chỉ ngắn của từng module Zigbee. Chẳng hạn, trong hệ thống sử dụng 3 module zigbee có địa chỉ của Coordinator là 0x0000; địa chỉ của các Router_1 là 0x4047, Router_2 là 0x4325. Trong quá trình giải mã, vì AES là kỹ thuật mã hóa khóa đối xứng nên cũng sử dụng khóa

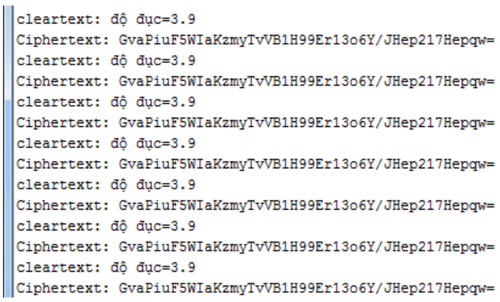
Key = {0x15, 0x2B, 0x7E, 0x16, 0x28, 0xAE, 0xD2, 0xA6, 0xAB, 0xF7, 0x15, 0x88, 0x09, 0xCF, 0x4F, 0x3C, 0x15, 0x2B, 0x7E, 0x16, 0x28, 0xAE, 0xD2, 0xA6, 0xAB, 0xF7, 0x15, 0x88, 0x09, 0xCF, 0x4F, 0x3C}; và sử dụng vector khởi tạo: Dec_iv = {0, 0, 0x15, 0, 0, 0, 0x3B, 0, 0, 0, 0, 0, 0, 0, 0, 0}.

III. KẾT QUẢ VÀ LUẬN BÀN

Trong phần này chúng tôi sẽ trình bày về một số kết quả đã đạt được trong các mẫu đo lường khác nhau của môi trường nước thải công nghiệp và nước sinh hoạt (với mục đích so sánh) (Hình 11).

A. Mã hóa dữ liệu

Hình 10 dưới đây là kết quả đo đạc và thực hiện mã hóa dữ liệu về độ đục.



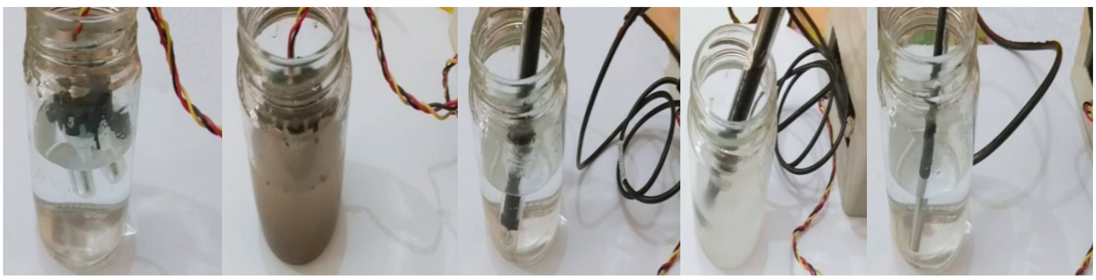
Hình 10. Kết quả mã hóa dữ liệu đo độ đục bằng mô đun ZigBee

B. Giám sát thông số môi trường nước

Các trường hợp đo đạc trong điều kiện thực tế Nhiệt độ của nước và Biên độ dao động nhiệt trong ngày 2/6/2019. Thông tin chi tiết sẽ đưa ra kết quả truy vấn dữ liệu, vẽ biểu đồ dữ liệu theo khu vực – Thời gian và giá trị trung bình ngày.

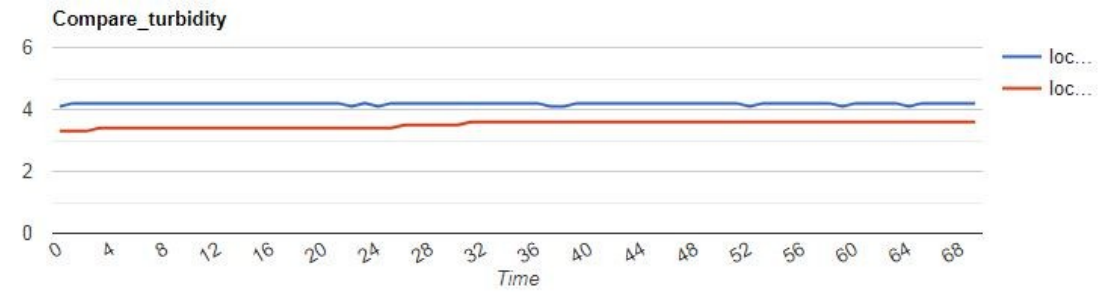
Kết quả so sánh độ đục của các mẫu nước sinh hoạt và nước thải. Dữ liệu biểu thị trên Hình 13 và 14 là giá trị analog của cảm biến. Trên Hình 13, đường màu đỏ biểu thị nước ở kênh rạch, đường màu xanh biểu thị nước sinh hoạt. Độ đục thay đổi khi nhiệt độ thay đổi hoặc xảy ra hiện tượng lắng đọng. Khi điện áp càng nhỏ tương đương với độ đục càng lớn. Kết quả trên Hình 14 so sánh độ pH của nước sinh hoạt và nước thải công nghiệp là những dữ liệu có giá trị analog đo lường từ cảm biến. Đường màu đỏ biểu thị nước sinh hoạt, đường màu xanh biểu thị cho nước thải sinh hoạt.

Hình 12. Nhiệt độ đo trong ngày (trên) và biên độ dao động nhiệt trong ngày 2/6/2019 (dưới)

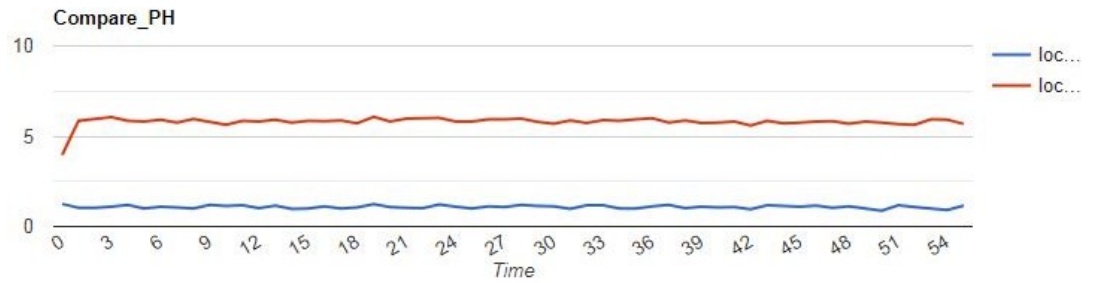


(a) Đo độ đục mẫu nước sinh hoạt | (b) Đo độ đục mẫu nước thải | (c) Độ PH mẫu nước sinh hoạt | (d) Độ PH mẫu nước thải | (e) Đo nhiệt độ mẫu nước

Hình 11. Các mẫu đo độ đục, độ pH và nhiệt độ của nước sinh hoạt và nước thải công nghiệp



Hình 13. So sánh độ đục của nước sinh hoạt và nước thải công nghiệp



Hình 14. So sánh độ pH của nước sinh hoạt và nước thải công nghiệp

IV. KẾT LUẬN

Bài báo nghiên cứu áp dụng thuật toán mã hóa thông tin AES trong bảo mật mạng IoT kết nối ZigBee, ứng dụng trong đo lường thông số môi trường nước thải công nghiệp. Một hệ thống mẫu hoàn thiện có khả năng đo đạc, mã hóa, truyền dẫn 3 thông số môi trường nước từ thiết bị đầu cuối về trung tâm dữ liệu IoT, xử lý và hiển thị dữ liệu đo được, hỗ trợ công tác quản lý và giám sát.

LỜI CẢM ƠN

Nghiên cứu này được tài trợ bởi Bộ Khoa học và Công nghệ, thuộc chương trinh KC01/16-20. Mã nhiệm vụ: KC.01.17/16-20.

TÀI LIỆU THAM KHẢO

[1]. Gubby, J.; Buyya, R.; Marusic, S.; Palaniswami, M. "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Technical Report, The University of Melbourne*, Australia, 29 June 2012.

[2]. Milman, R.; "Bluetooth and Zigbee to Dominate Wireless IoT Connectivity," *Internet of Business*.

[3]. Nurse, J.R.C.; Creese, S.; Roure, D.D. "Security Risk Assessment in Internet of Things Systems," *IT Prof*. 2017, 19, 20–26.

[4]. Khan, R.; Khan, S.U.; Zaheer, R.; Khan, S. "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," In *Proc. of the 10th Int. Conf. on Frontiers of Information Tech.*, 17–19 Dec. 2012; pp. 257–260.

[5]. Al-Fuqaha, A.; Guizani, M.; Aledhari, M.; Ayyash, M. "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications*," IEEE Commun. Surv. Tutor.* 2015, 17, 2347–2376.

[6]. Ali, B.; Awad, D.A.I. "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes," *Sensors* 2018, 18, 817.

[7]. Betzler, A.; Gomez, C.; Demirkol, I.; Paradells, J. "A Holistic Approach to Zigbee Performance Enhancement for Home Automation Networks," *Sensors* 2014, 14, 14932–14970.

[8]. Radmand, P.; Domingo, M.; Singh, J.; Arnedo, J.; Talevski, A.; Petersen, S.; Carlsen, S. "Zigbee/Zigbee PRO security assessment based on compromised cryptographic keys," In *Proc. of the Inter. Conf. on P2P, Parallel, Grid, Cloud and Internet Computing*, Poland, 4–6 Nov. 2010.

[9]. Olawumi, O.; et. al. "Three Practical Attacks Against Zigbee Security: Attack Scenario Definitions, Practical Experiments, Countermeasures, and Lessons Learned," In *Proc. of the HIS2014*, 14–16 Dec. 2014.

[10]. Kocher, I.S.; Chow, C.-O.; Ishii, H.; Zia, T.A. "Threat Models and Security Issues in Wireless Sensor Networks," *Int. J. Comput. Theory Eng*. 2013, 5, 5.

[11]. Brodsy, J.; McConnell, A. "Jamming and Interference Induced Denial-of-Service Attacks on IEEE 802.15.4-Based Wireless Networks," In *Proc. of the Digital Bond's SCADA Security Scientific Symposium*, Miami, 21–22 Jan. 2009.

[12]. CISCO. Securing the Internet of Things: A Proposed Framework.

[13]. Pasquier, I.B.; Kalam, A.A.E.; Ouahman, A.A.; Montfort, M.D. "A Security Framework for Internet of Things," *Springer International Publishing*, 2015.

[14]. Wu, T.; Zhao, G. "A Novel Risk Assessment Model for Privacy Security in Internet of Things," *Wuhan Univ. J. Nat. Sci. 2014*, 19, 398–404.

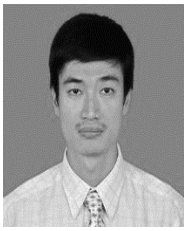
[15]. Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications. 2006.

[16]. Durech, J.; Franekova, M. "Security attacks to Zigbee technology and their practical realization," In *Proc. of the IEEE SAMI 2014*, 23–25 January 2014.

[17]. Vidgren, N.; et. al. "Security Threats in Zigbee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned," In *Proc. of the 46th Hawaii Inter. Conf. on Sys. Sciences*, January 2013.

[18]. "ZigBee technology: Current status and future scope," *2015 Inter. Conf. on Computer and Computational Sciences (ICCCS)*, 27-29 Jan. 2015.

SƠ LƯỢC VỀ TÁC GIẢ



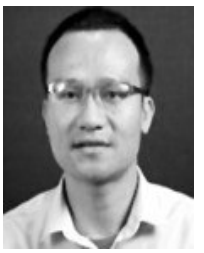
PGS. TS. Nguyễn Hữu Trung

Đơn vị công tác: Viện Điện tử - Viễn Thông, Đại học Bách khoa Hà Nội.

E-mail: Trung.nguyenhuu@hust.edu.vn

Quá trình đào tạo : Tốt nghiệp chuyên ngành Điện tử - viễn thông, Đại học Bách khoa Hà Nội năm 1996. Tốt nghiệp Thạc sĩ và Tiến sĩ Điện tử - Viễn thông tại Đại học Bách khoa Hà Nội năm 1998 và 2004. Được phong hàm Phó Giáo sư chuyên ngành Điện tử Viễn thông, ngành Điện - Điện tử - Tự động hóa năm 2010.

Hướng nghiên cứu hiện nay: Xử lý tín hiệu, Công nghệ nhúng, Công nghệ FPGA, Công nghệ DSP.



PGS.TS. Hà Duyên Trung

Đơn vị công tác: Viện Điện tử - Viễn Thông, Đại học Bách khoa Hà Nội.

Email : trung.haduyen@hust.edu.vn

Quá trình đào tạo : tốt nghiệp Kỹ sư Điện tử Viễn thông tại trường Đại học Bách khoa Hà Nội, Việt Nam năm 2003, thạc sĩ và tiến sĩ kỹ thuật Thông tin từ Đại học Chulalongkorn, Bangkok, Thái Lan, tương ứng vào các năm 2005 và 2009. Được phong hàm Phó giáo sư năm 2012.

Hướng nghiên cứu hiện nay: IoT, công nghệ truyền thông quang vô tuyến bao gồm quang học không gian tự do (FSO) và truyền thông ánh sáng nhìn thấy (VLC), xử lý tín hiệu băng gốc.

ThS. Nguyễn Thanh Bình

Đơn vị công tác: Vụ Khoa học - Công nghệ, Ban Cơ yếu Chính phủ.

Email: binhbcy@gmail.com

Quá trình đào tạo : Tốt nghiệp Học viện Kỹ thuật Mật mã năm 1996. Nhận bằng Thạc sĩ tại Học viện Kỹ thuật Quân sự năm 2003. Đang là nghiên cứu sinh của Học viện Công nghệ Bưu chính Viễn thông.

Hướng nghiên cứu hiện nay: Thông tin vô tuyến, Mạng di động GSM, Mạng vô tuyến Wireless, công nghệ mật mã.