Journal of Mining and Earth Sciences
Website: http://jmes.humg.edu.vn

# The solution of data transmission security for Gateway IoT

Chinh Manh Dang [1,*], Vinh Quang Thai [1], Minh Ngoc Pham [1], Trung Thanh Dang [2], Mai Thanh Thi Phung [2], Tan Duy Ngo [3]

[1] *Institute of Information Technology, Vietnam Academy of Science and Technology, Vietnam*
[2] *Faculty of Electrical Engineering, Electric Power University, Vietnam*
[3] *Space Technology Institute, Vietnam Academy of Science and Technology, Vietnam*

ARTICLE INFO

*Article history:*
Received 16th Jan. 2020
Revised 27th Mar. 2020
Accepted 29th Apr. 2020

*Keywords:*
Gateway IoT,
Gateway,
Industrial 4.0,
Information security,
Internet of thing.

ABSTRACT

*We are living in the trend of the Internet of Things (IoT), electronic devices that are capable of connecting and exchanging information with each other via the Internet. For automation, monitoring and control systems, there is a need to upgrade existing systems so that users can remotely monitor via the Internet. The solution is to integrate the Gateway device to transmit and receive data. However, in the Internet environment, the issue of information security and safety always needs attention because of the risk of network attacks and data theft. In this paper, the authors present data security solutions for Gateway IoT devices to ensure information security against eavesdropping or sniffers. The device has been integrated into a landslide monitoring system, which has proven to work, increasing the reliability of the system.*



*Corresponding author
*E-mail:* dangmanhchinhbkhn@gmail.com
DOI: 10.46326/JMES.2020.61(2).07

Tạp chí Khoa học Kỹ thuật Mỏ - Địa chất
Trang điện tử: http://tapchi.humg.edu.vn

# Giải pháp bảo mật thông tin cho thiết bị Gateway IoT

Đặng Mạnh Chính [1,*], Thái Quang Vinh [1], Phạm Ngọc Minh [1], Đặng Thành Trung [2], Phùng Thị Thanh Mai [2], Ngô Duy Tân [3]

[1] *Viện Công nghệ Thông tin, Viện Hàn lâm khoa học và Công nghệ Việt Nam, Việt Nam*
[2] *Khoa Kỹ thuật điện, Trường Đại học Điện lực, Việt Nam*
[3] *Viện Công nghệ Vũ trụ, Viện Hàn lâm Khoa học và Công nghệ Việt Nam, Việt Nam*

THÔNG TIN BÀI BÁO

*Quá trình:*
Nhận bài 16/01/2020
Sửa xong 27/3/2020
Chấp nhận đăng 29/4/2020

*Từ khóa:*
Gateway IoT,
Gateway,
Industrial 4.0,
Bảo mật thông tin,
Vạn vật kết nối internet.

TÓM TẮT

*Chúng ta đang sống trong xu hướng công nghệ vạn vật kết nối Internet (Internet of Things - IoT), các thiết bị điện tử đều có khả năng kết nối trao đổi thông tin với nhau qua Internet. Đối với các hệ thống tự động hóa, giám sát, điều khiển, nhu cầu cần thiết được đặt ra là nâng cấp các hệ thống hiện có để người sử dụng có thể theo dõi từ xa qua Internet. Giải pháp được đưa ra là tích hợp thiết bị Gateway để truyền nhận dữ liệu. Tuy nhiên, trong môi trường Internet, vấn đề bảo mật và an toàn thông tin luôn cần được quan tâm bởi nguy cơ tấn công mạng, lấy cắp dữ liệu luôn hiện hữu. Trong bài báo này, nhóm tác giả trình bày giải pháp bảo mật dữ liệu cho thiết bị Gateway IoT nhằm đảm bảo an toàn thông tin chống lại các cuộc tấn công kiểu nghe lén hay sniffers. Thiết bị được tích hợp thử nghiệm trong hệ thống giám sát sạt lở đất và đã chứng minh được khả năng làm việc, tăng độ tin cậy của hệ thống.*



## 1. Mở đầu

Vạn vật kết nối Internet - IoT là một trong những yếu tố cốt lõi của cách mạng công nghiệp 4.0, nó giúp cho các hệ thống công nghiệp, hệ thống giám sát, điều khiển tự động hóa có thể dễ dàng trao đổi dữ liệu, giám sát và điều khiển từ xa (Vu Tien Sinh nnk., 2020). Trong các hệ thống tự động hóa này, giải pháp tích hợp một thiết bị Gateway thường được đưa ra nhằm giải quyết bài toán kết nối các hệ thống công nghiệp tới mạng Internet, tham gia vào hệ sinh thái IoT (Masoud Hemmatpour nnk., 2017).

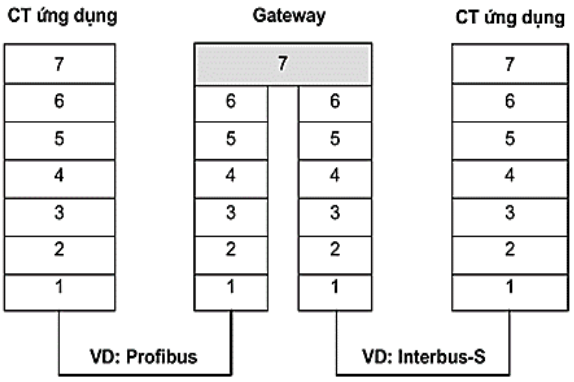
Thiết bị Gateway là thiết bị được sử dụng để liên kết các hệ thống mạng khác nhau (các hệ thống bus khác nhau). Nhiệm vụ chính của gateway là chuyển đổi giao thức ở cấp cao, thường được thực hiện bằng các thành phần phần mềm (Hoàng Minh Sơn, 2007). Trong xu hướng công nghiệp 4.0, khái niệm Gateway được mở rộng cho các kết nối không dây và kết nối trực tiếp tới Internet (Romano Fantacci nnk., 2014).

Khác với các thiết bị Gateway cổ điển, thiết bị Gateway IoT phải đối mặt với nguy cơ tấn công mạng đe dọa an toàn thông tin. Bởi thiết bị Gateway cổ điển chỉ phục vụ cho kết nối mạng nội

*Tác giả liên hệ
*E - mail:* dangmanhchinhbkhn@gmail.com
DOI: 10.46326/JMES.2020.61(2).07

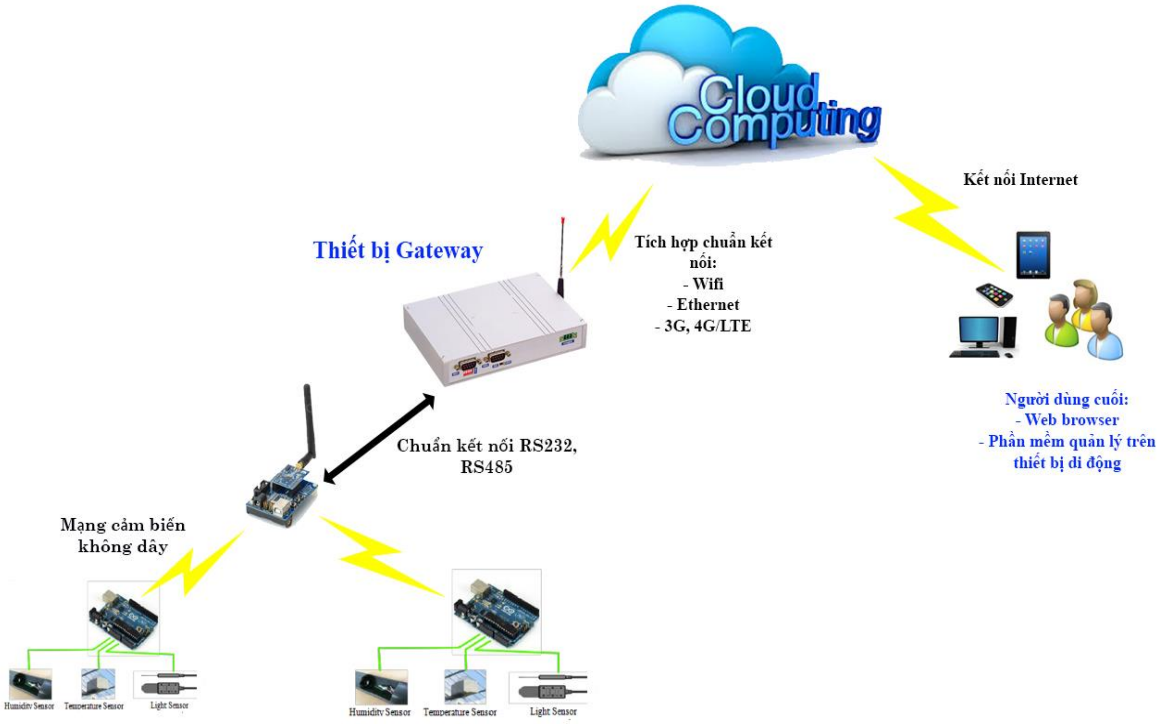
bộ trong mạng truyền thông công nghiệp thuộc phạm vi nhà máy, cơ sở sản xuất như trong mô hình ở Hình 1. Còn đối với thiết bị Gateway IoT hỗ trợ các kết nối tới Internet, dữ liệu được truyền trực tiếp từ nhà máy hoặc các mạng cảm biến (sensor) tới Server đặt trên Internet (Hình 2). Các thiết bị này là cầu nối giữa mạng nội bộ trong nhà máy tới mạng Internet toàn cầu (Chang-Le Zhong nnk., 2015).

Trong môi trường Internet, có rất nhiều kiểu tấn công, nhưng kiểu tấn công phổ biến nhất là kiểu tấn công nghe lén (sniffers). Sniffer được hiểu đơn giản như là một chương trình cố gắng nghe ngóng các lưu lượng thông tin trên (trong một hệ thống mạng). Tương tự như là thiết bị cho phép nghe lén trên đường dây điện thoại. Chỉ khác nhau ở môi trường là các chương trình Sniffer thực hiện nghe lén trong môi trường mạng máy tính.

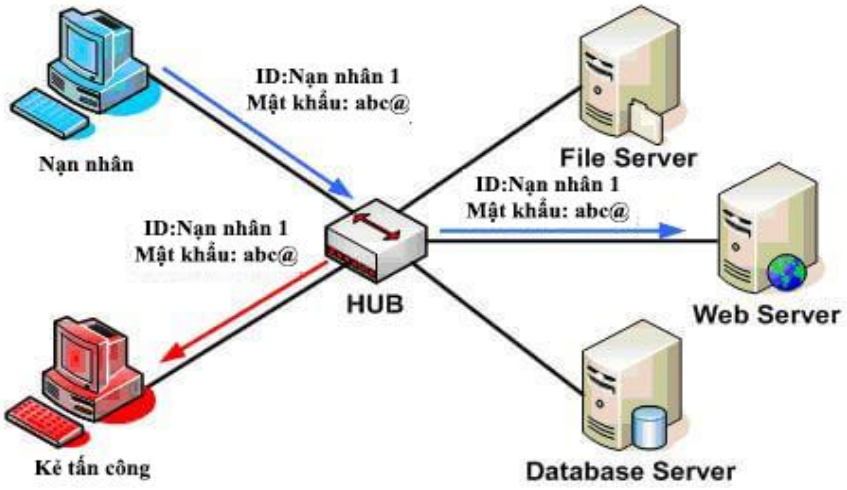



*Hình 1. Mô hình Gateway trong công nghiệp.*

Khi máy tính hoặc phần mềm của kẻ tấn công tham gia vào cùng mạng Ethernet của thiết bị hoặc server, nó có thể nghe lén (sniffer) và bắt (capture) các tập thông tin được truyền qua mạng đó (Hình 3). Vì vậy, các thiết bị Gateway IoT khi kết nối vào mạng Internet hoàn toàn có thể bị tấn công bởi loại tấn công này. Giải pháp thường được đưa ra là mã hóa thông tin trước khi truyền đi, khi đó kẻ tấn công dù có bắt được tập tin gửi đi cũng không thể giải mã và biết được thông tin quan trọng bên trong. Giao thức thường được sử dụng hiện nay là HTTPS (Hypertext Transfer Protocol Secure), đây là một giao thức kết hợp giữa giao thức HTTP và giao thức bảo mật SSL hay TLS cho phép trao đổi thông tin một cách bảo mật trên Internet. Giao thức HTTPS thường được dùng trong các giao dịch nhạy cảm cần tính bảo mật cao. Giao thức này thường được tích hợp sẵn trên các trình duyệt web như Chrome, Firefox, Safari,... cũng như các thiết bị di động có sẵn hệ điều hành.




*Hình 2. Mô hình hệ thống IoT tích hợp thiết bị Gateway.*




*Hình 3. Mô phỏng tấn công Sniffers (Quadeer and nnk., 2010).*

Tuy nhiên, việc phát triển một giao thức bảo mật dữ liệu đường truyền cho các thiết bị nhúng truyền dữ liệu như thiết bị Gateway chưa được chú trọng đúng mức.

Trong khuôn khổ bài báo này, nhóm tác giả trình bày một giải pháp mã hóa thông tin trước khi truyền cho thiết bị Gateway IoT. Giải pháp đã được tích hợp trong thiết bị Gateway nhóm tự phát triển và ứng dụng thử nghiệm trong hệ thống giám sát cảnh báo sạt lở, đem lại kết quả khả quan..

## 2. Giải pháp mã hóa dữ liệu cho thiết bị Gateway

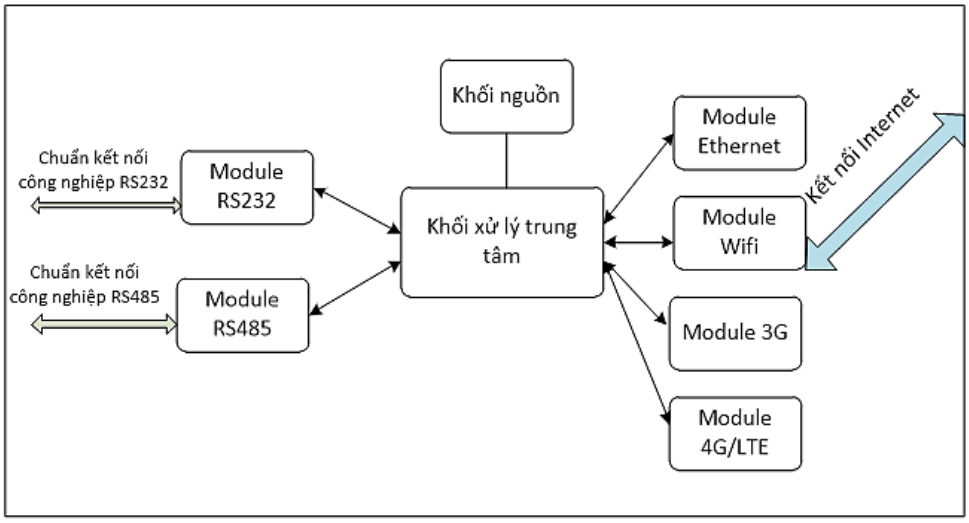
Cùng với sự phát triển nhanh chóng của công nghệ sản xuất vi xử lý, các thiết bị nhúng ngày càng có khả năng tính toán mạnh mẽ. Nhờ đó, việc tích hợp thuật toán mã hóa dữ liệu phức tạp, đòi hỏi nhiều tính toán vào trong thiết bị nhúng truyền dữ liệu trở nên khả thi hơn trước đây. Trong nghiên cứu này, nhóm đã phát triển thiết bị Gateway sử dụng dòng vi xử lý 32 bit của STM, giúp đạt được khả năng tính toán mạnh mẽ và tiết kiệm năng lượng.

Thiết bị Gateway trong khuôn khổ nghiên cứu này được tích hợp kết nối RS232, RS485 theo chuẩn truyền thông công nghiệp Modbus có khả năng giao tiếp rộng rãi với các thiết bị công nghiệp, các hệ cảm biến hiện thời (Hình 4). Đồng thời, thiết bị cũng được trang bị kết nối Ethernet và kết nối Wifi, 3G, 4G, nhằm tăng độ tin cậy của hệ thống, tránh trường hợp mất mát dữ liệu khi một đường truyền gặp sự cố. Trong bài báo này, nhóm tác giả sẽ tập trung trình bày về giải pháp bảo mật thông tin và không bàn về các vấn đề khác.

Các giải pháp mã hóa hiện đại hiện nay thường kết hợp giải pháp mã hóa đối xứng và mã hóa không đối xứng, nhằm kết hợp ưu điểm về tăng cường tính an toàn của hệ thống dựa trên phương pháp không đối xứng với khả năng tính toán nhanh gọn của phương pháp mã hóa đối xứng. Trong khuôn khổ nghiên cứu này, nhóm tác giả sử dụng phương pháp mã hóa không đối xứng để trao đổi khóa bí mật, sau đó sử dụng khóa bí mật đó trong phương pháp mã hóa đối xứng để mã hóa và giải mã dữ liệu để phù hợp với khả năng tính toán của thiết bị nhúng.

### *2.1. Giải pháp tạo Secret Key dựa trên thuật toán trao đổi khóa Diffie - Hellman*

Phương pháp trao đổi khóa Diffie-Hellman cho phép hai bên (người, thực thể giao tiếp) thiết lập một khóa bí mật chung để mã hóa dữ liệu sử dụng trên kênh truyền thông không an toàn mà không cần có sự thỏa thuận trước về khóa bí mật giữa hai bên. Khóa bí mật tạo ra sẽ được sử dụng để mã hóa dữ liệu với phương pháp mã hóa khóa đối xứng (Nguyễn Khanh Văn, 2014). Nhằm mục đích mã hóa và giải mã dữ liệu giữa thiết bị Gateway và Server, cả 2 bên đều cần nắm giữ 1 khóa bí mật chung (Secret Key). Tuy nhiên, việc trao đổi Secret Key trên môi trường Internet tiềm ẩn nhiều nguy hiểm, nếu như kẻ tấn công có thể bắt được gói tin trao đổi Secret Key chúng ta truyền đi, chúng có thể giải mã tất cả thông tin sau này của chúng ta. Phương pháp trao đổi khóa Diffie - Hellman chính




*Hình 4. Sơ đồ khối thiết bị Gateway.*

là nền tảng của giao thức Transport Layer Security (TLS) cũng như thuật toán RSA được ứng dụng rộng rãi hiện nay.

Trong bài báo này, nhóm tác giả ứng dụng phương pháp trao đổi khóa Diffie-Hellman cho Gateway và Server thông qua các bước sau:

• Server và Gateway sử dụng một nhóm cyclic hữu hạn G và 1 phần tử chung g của G được lưu trữ trong ROM của chip STM và trên Server. Phần tử g là công khai.

• Gateway chọn một số tự nhiên lớn ngẫu nhiên a, đây cũng chính là khóa riêng (Private key) của Gateway, tính toán và gửi ga mod p kèm id của Gateway lên Server. Ở bước này, Gateway gửi Public Key của Gateway lên Server.

• Server nhận Public key của Gateway kèm id. Server chọn một số tự nhiên lớn b ngẫu nhiên, đây là khóa riêng của Server. Sau đó tính toán và gửi gb mod p xuống thiết bị Gateway. Đây chính là Public Key của Server.

• Gateway nhận Public Key của Server, sau đó kết hợp với Private Key của mình là a, tính toán (gb)a mod p.

• Server kết hợp Public Key của Gateway với Private Key của mình là b, tính toán (ga)b mod p.

• Hai giá trị và Gateway và Server tính toán và cuối cùng sẽ trùng khớp nhau, vì cùng nhận được gab mod p. Đây cũng chính là Secret Key được sử dụng để mã hóa cũng như giải mã dữ liệu sau này.

Cùng với sự phát triển của công nghệ vi xử lý, các chip hiện nay càng ngày càng có khả năng tính toán mạnh mẽ hơn, có thể làm việc với các phép tính với hệ số lớn, việc đó cũng tăng tính an toàn của phương pháp trao đổi key đã trình bày ở trên. Phương pháp mã hóa Diffie - Hellman kinh điển bao gồm cả mã hóa và giải mã thông tin. Tuy nhiên, nhóm tác giả chỉ sử dụng phương pháp trao đổi key của Diffie-Hellman, phần mã hóa và giải mã thông tin nhóm tác giả sẽ kết hợp với thuật toán hiện đại hơn để tăng độ tin cậy của phương pháp bảo mật.

### *2.2. Giải pháp mã hóa dữ liệu sử dụng thuật toán mã hóa RC4*

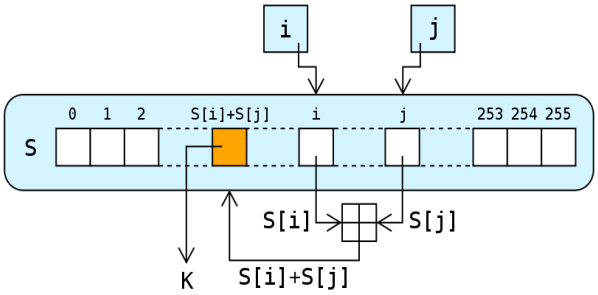
Thiết bị Gateway sẽ nhận dữ liệu từ các chuẩn kết nối RS232, RS485 theo chuẩn truyền thông Modbus. Sau khi bóc tách và xử lý dữ liệu đầu vào, dữ liệu sẽ được mã hóa và truyền lên server. Thuật toán mã hóa được sử dụng ở đây là RC4 (Rivest Cipher 4), đây là thuật toán mã hóa dòng (stream cipher) được ứng dụng rộng rãi trong kỹ thuật mật mã hiện nay bởi tính đơn giản, tốc độ tính toán nhanh nhưng vẫn đảm bảo yêu cầu về bảo mật thông tin. Mặc dù RC4 đã tồn tại từ rất lâu, nhưng đây vẫn là thuật toán mã hóa mật mã được sử dụng rộng rãi nhất trong thực thi nhiều giao thức phổ biến, bao gồm:

- SSL (Secure Socket Layer)
- TLS (Transport Layer Security)
- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access)
- RDP của Microsoft (Remote Desktop Protocol)
- BitTorrent
- Và nhiều giao thức khác

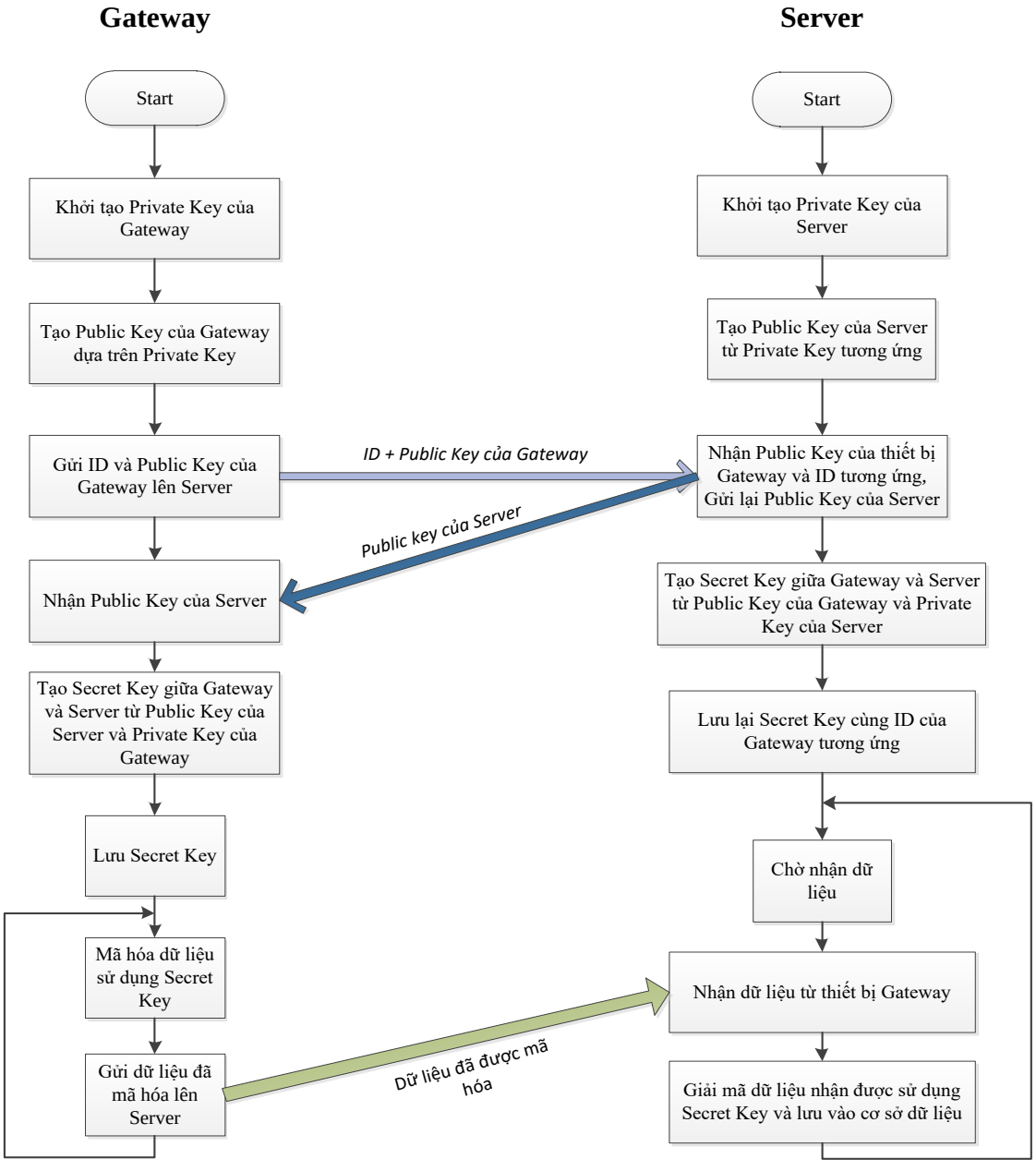
RC4 là thuật toán mã hóa đối xứng. Vì thế để

tích hợp thuật toán này, thiết bị Gateway và Server phải sử dụng chung một khóa bí mật (Secret key) (Hình 5). Khóa bí mật được sử dụng ở đây chính là khóa bí mật Server và thiết bị Gateway nhận được thông qua phương pháp trao đổi khóa Diffie-Hellman.

Hình 6 trình bày về thuật toán mã hóa và trao đổi dữ liệu giữa thiết bị Gateway và Server. Thuật toán này là sự kết hợp giữa phương pháp trao đổi khóa Diffie-Hellman và giải pháp mã hóa sử dụng




*Hình 5. Mô hình mã hóa từng bit theo thuật toán RC4.*




*Hình 6. Cơ chế truyền nhận dữ liệu giữa Gateway và Server.*

thuật toán RC4 nhằm kết hợp ưu điểm của thuật toán mã hóa đối xứng và không đối xứng. Mỗi thiết bị Gateway sẽ có một quy trình tương tự nhau để thiết lập Secret Key với Server.

## 3. Kết quả thử nghiệm

Bài Thiết bị Gateway được tích hợp vào hệ thống giám sát, cảnh báo sạt lở đất. Hệ thống được ứng dụng thử nghiệm tại khu vực vùng núi huyện Tam Đường, tỉnh Lai Châu. Hệ thống thu thập các thông số môi trường đất, môi trường không khí từ các cảm biến đo độ ẩm đất, nhiệt độ và độ ẩm không khí, từ đó truyền dữ liệu về máy chủ trên Internet thông qua kết nối 3G. Các bo mạch nhỏ gọn đọc dữ liệu, truyền tới thiết bị Gateway qua chuẩn kết nối RS232. Tại đây, dữ liệu sẽ được mã hóa trước khi truyền tới server.

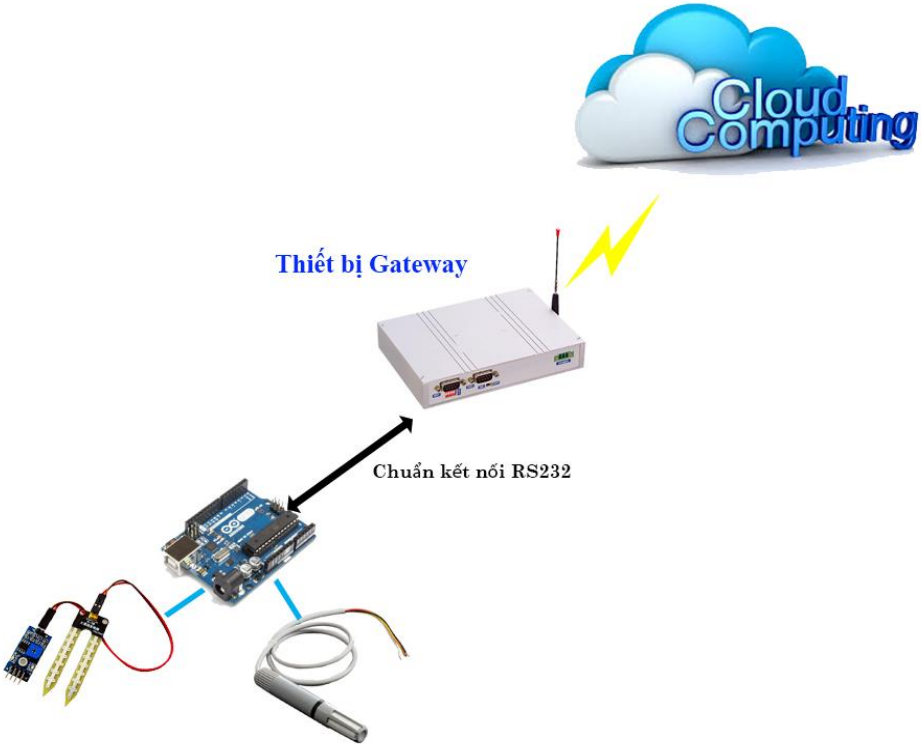
Để minh chứng tính an toàn của giải pháp, nhóm tác giả giả lập tấn công kiểu sniffer trong mô hình hệ thống IoT đặt tại phòng thí nghiệm (Hình 7). Để giả lập tấn công, nhóm tác giả sử dụng phần mềm WireShark, đây là một công cụ kiểm tra, theo dõi và phân tích thông tin mạng được phát triển bởi Gerald Combs. Phiên bản đầu tiên của Wireshark mang tên Ethereal được phát hành năm 1988. Đến nay, WireShark vượt trội về khả năng hỗ trợ các giao thức (khoảng 850 loại), từ những loại phổ biến như TCP, IP đến những loại đặc biệt như là AppleTalk và Bit Torrent (Hình 8).

Phần mềm sẽ được cài vào máy tính kết nối cùng mạng với máy tính đặt server, theo nguyên tắc, tất cả các gói tin nhận và gửi trên cùng mạng sẽ được Wireshark ghi lại.

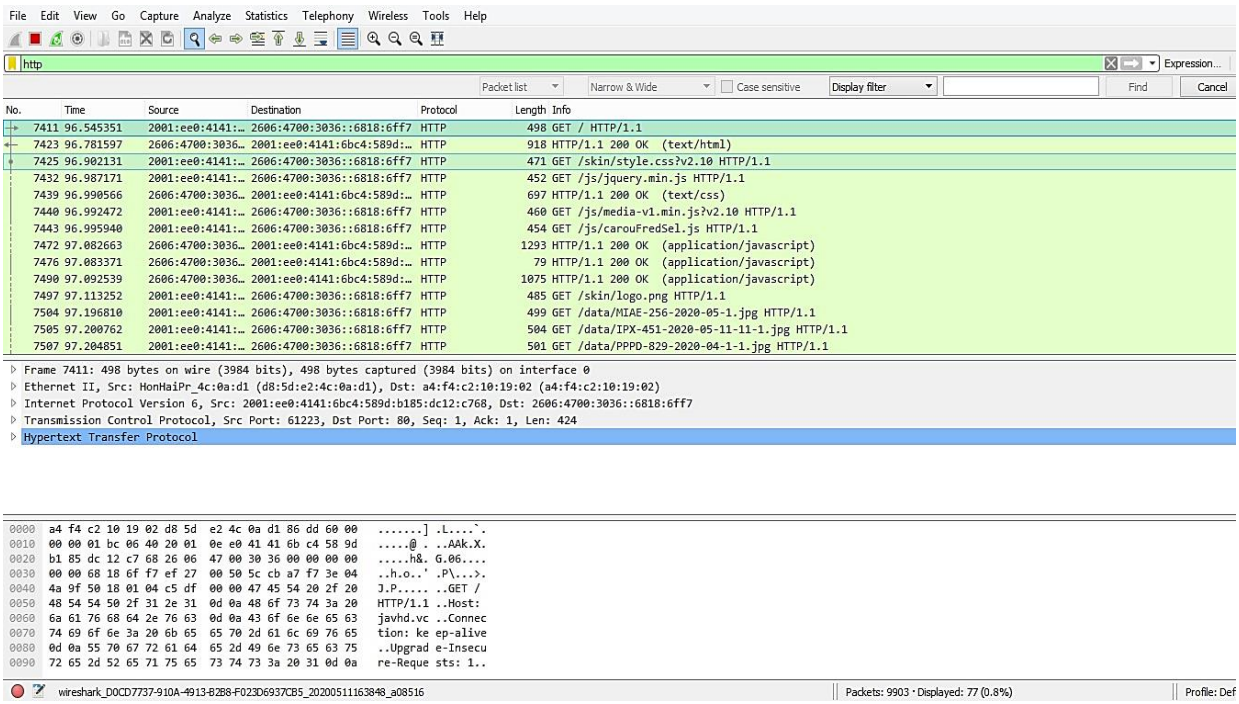
Trước tiên, giả lập tấn công sniffer vào hệ thống khi chưa sử dụng giải pháp mã hóa.

Dữ liệu truyền đi khi không được mã hóa sẽ được ghi lại như trong Hình 9.

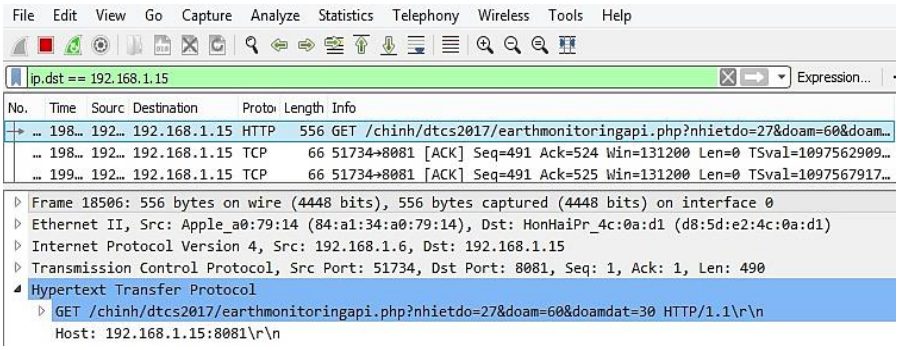
Khi tin tặc tấn công bằng phương pháp này, chúng sẽ lấy được thông tin về nhiệt độ môi trường, độ ẩm không khí và độ ẩm đất. Điều này rất nguy hiểm, chúng vừa có thể lấy thông tin, đồng thời cũng vừa có thể chèn dữ liệu giả về các thông số môi trường vào hệ thống. Bởi chúng đã nghe lén (sniffer) được cú pháp cũng như giao thức truyền tin. Điều này gây ra các sai lệch trong cảnh báo hệ thống. Tiếp theo, sử dụng giải pháp mã hóa đã được trình bày trong bài báo (Hình 10, 11, 12). Sau khi thiết lập Secret Key tại Server và Gateway, thiết bị tiến hành mã hóa dữ liệu nhận được và gửi đi (Hình 13, 14):




*Hình 7. Mô hình thử nghiệm hệ thống giám sát, cảnh báo sạt lở đất.*




*Hình 8. Giao diện của WireShark.*




*Hình 9. Giả lập tấn công Sniffer khi hệ thống chưa mã hóa.*

```
--------------------------- Protocol ---------------------------
The public data is p= 2147483647 and g= 1903411193
Random value of 'a': 2015862345
Waiting for value g^b
```

*Hình 10. Thiết bị Gateway tạo khóa riêng ngẫu nhiên.*

```
--------------------------- Protocol ---------------------------
The public data is p= 2147483647 and g= 1903411193
Random value of 'b': 2035698475
Value g^b sent
Waiting for value g^a
Value g^a received
The secret key is 135688587
```

*Hình 11. Server tạo khóa riêng ngẫu nhiên đồng thời tạo Secret Key.*

```
--------------------------- Protocol ---------------------------
The public data is p= 2147483647 and g= 1903411193
Random value of 'a': 2015862345
Waiting for value g^b
Value g^b received
Value g^a sent
The secret key is 135688587
```

*Hình 12. Gateway nhận Public key trả về của server, tạo Secret Key tương ứng.*

```
--------------------------- Protocol ---------------------------
The public data is p= 2147483647 and g= 1903411193
Random value of 'a': 2015862345
Waiting for value g^b
Value g^b received
Value g^a sent
The secret key is 135688587

--------------------------- Cryptosystem ---------------------------
Introduce the plaintext you want to send: nhietdo=22.3&doam=76.3&doamdat=56.2
I send cryptosystem f162b76420f4738023c171c298ff551b80f29ffb81d1f4dd7d13c76026696b8a647650
```

*Hình 13. Dữ liệu được mã hóa trước khi truyền đi*

Thông qua giả lập tấn công kiểu sniffer, có thể thấy dữ liệu mà kể tấn công thu được là một chuỗi mã hóa, kẻ tấn công không có trong tay Secret Key nên không thể nào giải mã được chuỗi thông tin này (Hình 15). Như vậy, giải pháp này có thể đảm bảo an toàn thông tin trước kiểu tấn công nghe lén sniffer đang được sự dụng phổ biên trên mạng Internet nhằm đánh cắp thông tin của người sử dụng.

## 4. Kết luận

Trong khuôn khổ bài báo này, nhóm nghiên cứu đã trình bày các kết quả đạt được trong giải pháp bảo mật an toàn thông tin cho thiết bị Gateway sử dụng thuật toán kết hợp giữa trao đổi khóa Diffie-Hellman và giải pháp mã hóa đối xứng RC4. Mặc dù trong phương pháp Diffie và Hellman cổ điển cũng có giải pháp mã hóa và giải mã dữ liệu, nhóm nghiên cứu không sử dụng giải pháp đó mà tích hợp bước giải mã và mã hóa dữ liệu thông qua RC4. Việc kết hợp này làm tăng độ tin cậy của hệ thống, tích hợp giải pháp mã hóa theo các chuẩn hiện đại như HTTPS, SSL,... Đồng thời cũng ứng dụng được ưu điểm tính toán nhanh gọn của phương pháp mã hóa đối xứng.

Giả lập tin tặc tấn công theo phương thức sniffer, có thể nhìn thấy sự hiệu quả của phương pháp khi tất cả thông tin tin tặc nhận được là một chuỗi mã hóa. Nếu thông tin trước khi truyền đi không được mã hóa, tin tặc dễ dàng lấy được thông tin quan trọng của chúng ta.

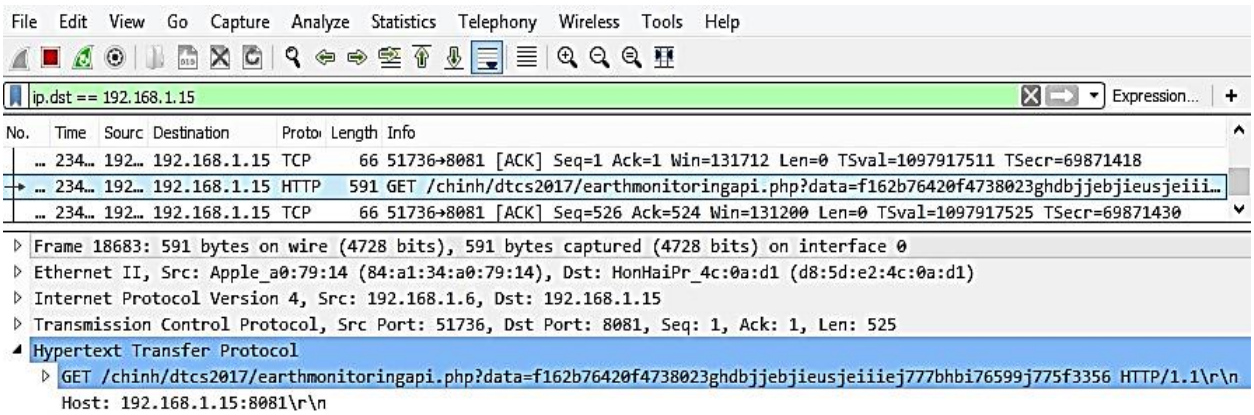
Bên cạnh đó, trong phương pháp này, có thể nhận thấy mỗi thiết bị Gateway đều tạo ra một chuỗi khóa riêng một cách ngẫu nhiên, điều đó đảm bảo độ tin cậy cao cho toàn bộ hệ thống. Trong trường hợp khi một thiết bị Gateway bị giải mã, kẻ tấn công không thể dùng kết quả đó để giải mã hệ thống các thiết bị Gateway còn lại.

Trong tương lai, với sự phát triển không ngừng của nền công nghiệp sản xuất vi xử lý, với các vi xử lý mạnh mẽ hơn, khả năng tính toán cao hơn sẽ được ra đời, khi đó các thiết bị nhúng có thể làm việc với tập số nguyên lớn (BigInteger) và lúc đó, khả năng bảo mật của phương pháp sẽ càng được tăng cường hơn nữa. Hiện tại, các chuẩn truyền thông công nghiệp đang sử dụng nhiều các chuẩn kết nối và truyền dữ liệu nối tiếp. Có thể kể tới như Modbus, Profibus theo chuẩn nối tiếp. Bởi đặc thù mạng truyền thông công nghiệp chủ yếu để giám sát và điều khiển các quá trình công nghiệp, nên

```
--------------------------- Protocol ---------------------------
The public data is p= 2147483647 and g= 1903411193
Random value of 'b': 2035698475
Value g^b sent
Waiting for value g^a
Value g^a received
The secret key is 135688587

--------------------------- Cryptosystem ---------------------------
Waiting for encrypted text
I receive encrypted text f162b76420f4738023c171c298ff551b80f29ffb81d1f4dd7d13c76026696b8a647650
The plaintext message is nhietdo=22.3&doam=76.3&doamdat=56.2
```

*Hình 14. Dữ liệu nhận được tại Server, đồng thời giải mã để lấy dữ liệu.*




*Hình 15. Kết quả thu được khi giả lập tấn công vào hệ thống.*

tốc độ và dữ liệu truyền trong mạng công nghiệp không yêu cầu quá lớn. Vì vậy, thiết bị Gateway sử dụng chip STM 32 bit đủ khả năng tính toán mã hóa dữ liệu, đảm bảo tính thời gian thực của hệ thống điều khiển.

Qua nghiên cứu trên, có thể khẳng định Việt Nam có thể làm chủ công nghệ sản xuất thiết bị Gateway, hướng tới cách mạng công nghiệp 4.0, đồng thời chủ động trong việc mã hóa và giải mã dữ liệu, đảm bảo tính an toàn thông tin cho hệ thống, không phụ thuộc vào các thiết bị nhập ngoại.

## Lời cảm ơn

Bài báo này được hoàn thành với sự tài trợ của đề tài cấp Viện Hàn lâm Khoa học và Công nghệ Việt Nam: "Nghiên cứu và tích hợp chuẩn kết nối công nghiệp cho thiết bị Gateway dùng cho hệ thống điều khiển công nghiệp", VAST01.07, 2018 - 2019.

## Tài liệu tham khảo

Chang-Le Zhong, Zhen Zhu, Ren-Gen Huang, (2015). Study on the IOT Architecture and Gateway Technology. *14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)*: 196 - 199.

Hoàng Minh Sơn, (2007). Mạng truyền thông công nghiệp. *Nhà xuất bản Khoa học Kỹ thuật*, Hà Nội.

Masoud Hemmatpour, Mohammad Ghazivakili, Bartolomeo Montrucchio, Maurizio Rebaudengo, (2017), DIIG: A Distributed Industrial IoT Gateway. *IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*. 1: 755 - 759.

Nguyễn Khanh Văn, (2014). Giáo trình cơ sở an toàn thông tin. *Nhà xuất bản Bách khoa Hà Nội*.

QADEER, Mohammed Abdul, (2010). Network traffic analysis and intrusion detection using packet sniffer. In: *2010 Second International Conference on Communication Software and Networks. IEEE*, 2010. p. 313-317.

Romano Fantacci, Tommaso Pecorella, Roberto Viti, Camillo Carlini, (2014). Short paper: Overcoming IoT fragmentation through standard gateway architecture. *2014 IEEE World Forum on Internet of Things (WF-IoT)*: 181 - 182.

Vu Tien Sinh, Vu Thi Quyen, Le Ngoc Huan, (2020). Design information orientation supporting system for user (Vietnamese). *Journal of Mining and Earth Sciences* 61 (1), 41-51