Bảo mật và xác thực thông tin trong mạng điều khiển công nghiệp

Nguyễn Đào Trường, Nguyễn Đức Tâm, Nguyễn Thị Nga

***Tóm tắt*— Bài báo trình bày giải pháp bảo mật và xác thực thông tin trong mạng điều khiển công nghiệp. Trên cơ sở phân tích một số mô hình tấn công trong hệ thống điều khiển, đặc biệt là tấn công giả mạo và tấn công DoS. Từ đó đề xuất áp dụng AES để mã hóa bảo mật thông tin và sử dụng hàm băm để xác thực thông tin điều khiển. Đồng thời thực nghiệm đã xây dựng được môđun phát hiện tấn công và môđun phản ứng khi phát hiện bị sai lệch thông tin điều khiển giữa các thiết bị trong hệ thống điều khiển công nghiệp.**

***Abstract*— This paper presents a solution for secure and authentication of industrial control systems based-on the analysis of some attack models in control systems, especially phishing attacks and DoS attacks. We propose a solution that AES encryption is used to protect control signals and the hash function is used to authenticate. In our experiment, we have built two modules: attack detection and reaction to detect misleading control information between devices in industrial control systems.**

Từ khóa— Hệ thống điều khiển; mật mã AES; hàm băm; giả mạo; tấn công từ chối dịch vụ.

I. GIỚI THIỆU

Hệ thống điều khiển công nghiệp là hệ thống dựa trên các máy tính thực hiện giám sát và điều khiển các quá trình công nghiệp. Các hệ thống này đại diện cho các hệ thống công nghệ thông tin được kết nối với nhau thành một chỉnh thể vật lý thống nhất. Hệ thống điều khiển công nghiệp thường là tập hợp các trạm được kết nối mạng, bao gồm các bộ cảm biến, bộ chấp hành, thiết bị điều khiển, thiết bị truyền thông. Tín hiệu trao đổi giữa các thiết bị trong hệ thống này có dung lượng nhỏ (từ vài byte đến vài chục byte) nhưng đòi hỏi với tốc độ nhanh (từ 250µs đến 1ms [10]). Hầu hết các hệ thống điều khiển công nghiệp đều có cấu trúc phân cấp.

Kiến trúc mạng trong hệ thống điều khiển công nghiệp được biểu diễn trên Hình 1. Kiến trúc hệ thống được phân thành các cấp cơ bản như sau:

- Tầng vật lý, thường được gắn với các bộ cảm biến và các cơ cấu chấp hành (gọi là các thiết bị trường). Các thiết bị này được kết nối thông qua mạng trường đến các bộ điều khiển logic có thể lập trình (Programmable Logic Controllers - PLC) hoặc các thiết bị đầu cuối ở xa (Remote Terminal Unit - RTU) để lần lượt thực hiện các hành động điều khiển cục bộ. Mạng điều khiển truyền tải những dữ liệu thời gian thực giữa các bộ điều khiển quá trình với các trạm vận hành. Những trạm đó thường được sử dụng trong khu vực điều khiển giám sát, khu quy hoạch đặt các cơ sở hạ tầng quan trọng.
- Tầng thứ hai là khu vực hoạt động sản xuất, là khu vực quản lý giám sát sản xuất, tối ưu hoá và duy trì các quá trình sản xuất.

Các thiết bị cảm biến và điều khiển có mặt trong phần lõi của các thiết bị chuyên dụng cũng như trong các hệ thống điều khiển trong các nhà máy, xí nghiệp. Sự gián đoạn của các hệ thống này có tác động lớn đến hiệu suất và độ chính xác trong quá trình hoạt động của các thiết bị.

Sự gián đoạn này có thể xuất phát từ nhiều hình thức tấn công của kẻ phá hoại. Đặc biệt, tấn công giả mạo và tấn công từ chối dịch vụ (DoS) có thể làm hệ thống bị tê liệt hoặc thực hiện sai chức năng. Vì vậy, bảo vệ chống tấn công giả mạo và tấn công từ chối dịch vụ trong mạng điều khiển là cấp thiết.

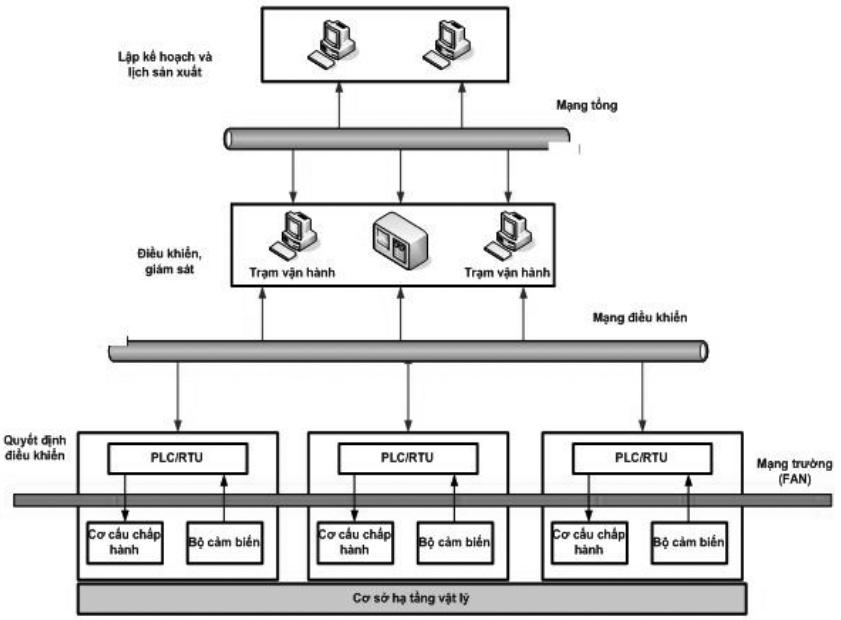
Bài báo trình bày giải pháp bảo mật và xác thực thông tin trong mạng điều khiển công nghiệp trên cơ sở phân tích một số mô hình tấn công trong hệ thống điều khiển, đặc biệt là tấn công giả mạo và tấn công DoS. Từ đó đề xuất áp dụng thuật toán AES để mã hóa bảo mật thông tin và sử dụng hàm băm để xác thực thông tin điều khiển.

Bố cục của bài báo gồm: Mục II trình bày các phương thức tấn công trong mạng điều khiển công nghiệp, Mục III trình bày giải pháp bảo mật cho mạng điều khiển công nghiệp dùng mật mã AES, Mục cuối là kết luận.

II. TẤN CÔNG TRONG HỆ THỐNG ĐIỀU KHIỂN CÔNG NGHIỆP

A. Hệ thống động tuyến tính

Hệ thống động tuyến tính là một trong những mô hình phổ biến nhất đối với hệ thống các thiết bị vật lý trong các hệ thống điều khiển [3].



Hình 1. Kiến trúc của hệ thống điều khiển công nghiệp

Quá trình điều khiển có thể khái quát thành một hệ các phương trình sau:

$$\begin{cases} x_{k+1} = Ax_k + Bu_k + \omega_k & (1a) \\ y_k = Cx_k & (1b) \end{cases}$$

Trong đó: $x_k = (x_{1k}, ..., x_{nk}) \in \mathbb{R}^n$ là trạng thái của hệ thống tại thời điểm *k*, $A = \left(a_{ij}\right) \in \mathbb{R}^{nxn}$ là các mô hình phụ thuộc vật lý của trạng thái *i* vào trạng thái *j*, $B = \left(b_{ij}\right) \in \mathbb{R}^{nxn}$ là ma trận đầu vào của trạng thái *i* từ đầu vào điều khiển *j*, $u_k = \left(u_{1k}, ..., u_{mk}\right) \in \mathbb{R}^m$.

Nói chung, khó có được một mô hình chính xác của quá trình điều khiển trong hệ thống mạng. Do đó, có thể thêm vào phương trình (1a) một thông tin gọi là nhiễu ω_k, và giả sử $\omega_k \in \mathbb{R}^n$ là một dãy ngẫu nhiên Gaussian với phương sai Q_0 và bậc 0.

Phương trình (1b) được xem là biểu thức quan sát vì chúng ta không trực tiếp đo trạng thái x_k của hệ thống được quan sát tại thời điểm *k*, với giả thiết rằng hệ thống điều khiển công nghiệp được thực hiện bởi một mạng có *p* bộ cảm biến, $y_k = (y_{1k}, ..., y_{pk}) \in \mathbb{R}^p$, $y_{lk} \in \mathbb{R}$ là thông tin thu thập được từ bộ cảm biến *l* tại thời điểm *k*. $C \in \mathbb{R}^{pxn}$.

B. Các mô hình tấn công

Các thuật toán điều khiển và đánh giá được sử dụng trong hệ thống điều khiển mạng công nghiệp được thiết kế thỏa mãn các mục đích hoạt động nhất định chẳng hạn như: sự ổn định an toàn, tồn tại lâu dài của chu trình khép kín hoặc tối ưu hóa hiệu suất hoạt động, nhằm bảo vệ những hoạt động này khỏi sự tấn công giả mạo vào cơ sở hạ tầng mạng công nghiệp.

Trong [3], nhóm tác giả đã xem xét tấn công từ chối dịch vụ (DoS) và các tấn công giả mạo. Trong các tấn công giả mạo, đối phương gửi thông tin sai lệch $\hat{y} \neq y$ hoặc $\hat{u} \neq u$ từ một hoặc nhiều bộ cảm biến hay bộ điều khiển. Thông tin sai lệch này bao gồm: số đo không chính xác, thời gian không chính xác (thời điểm số đo đó được quan sát) hoặc ID của bộ gửi không chính xác. Đối phương có thể thực hiện các tấn công này bằng cách thu nhận "thông tin bí mật" hoặc làm nguy hại đến một số bộ cảm biến hay bộ điều khiển. Do đó, các tác giả trong [3] đã mô hình hóa các tấn công này bằng cách sử dụng một số thay đổi trong hệ phương trình (1) như sau:

$$\begin{cases} x_{k+1} = Ax_k + Bu_k + \omega_k + \Gamma r_k \\ y_k = Cx_k + \Psi z_k \end{cases} \quad (2)$$

Trong đó: $\Gamma r_k, \Psi z_k$ là những thông tin giả mạo đưa vào hệ thống tại thời điểm *k*.

Trong mô hình này, giả sử thời điểm bắt đầu tấn công là $k = t_0$. Để mô hình hóa giả thiết này, nhóm tác giả đã sử dụng hàm đơn vị $1_{\{k \geq t_0\}}$, là một hàm bằng 0 trước thời điểm t_0 và bằng 1 sau thời điểm t_0.

Mô hình tấn công từ chối dịch vụ trên một tập con các tín hiệu điều khiển U như sau:

$$\begin{cases} \Gamma = B \\ \forall i \in U, r_{i,k} = -u_{i,k} 1_{\{k \geq t_0\}} \\ \forall j \notin U, r_{j,k} = 0 \end{cases} \quad (3)$$

Mô hình tấn công từ chối dịch vụ trên một tập con các nút cảm biến Y như sau:

$$\begin{cases} \Psi = C \\ \forall i \in Y, z_{i,k} = -x_{i,k} 1_{\{k \geq t_0\}} \\ \forall j \notin Y, z_{j,k} = 0 \end{cases} \quad (4)$$

Mô hình tấn công giả mạo trên tập con các tín hiệu điều khiển U như sau:

$$\begin{cases} \Gamma = B \\ \forall i \in U, r_{i,k} = (-u_{i,k} + \alpha_{i,k}) 1_{\{k \geq t_0\}} \\ \forall j \notin U, r_{j,k} = 0 \end{cases} \quad (5)$$

với α_k là tín hiệu điều khiển tùy ý được gửi bởi kẻ tấn công.

Mô hình tấn công giả mạo trên tập con các nút cảm biến Y như sau:

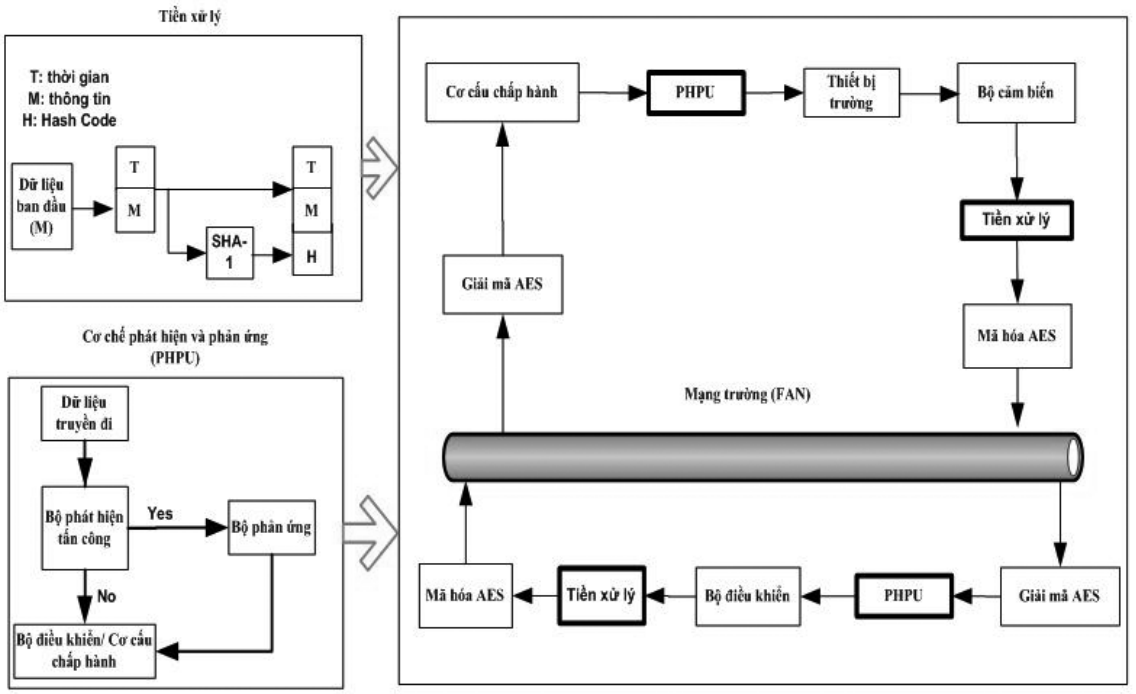
$$\begin{cases} \Psi = C \\ \forall i \in Y, z_{i,k} = (-x_{i,k} + \beta_{i,k}) 1_{\{k \geq t_0\}} \\ \forall j \notin Y, z_{j,k} = 0 \end{cases} \quad (6)$$

với β_k là tín hiệu điều khiển do kẻ tấn công gửi đi.

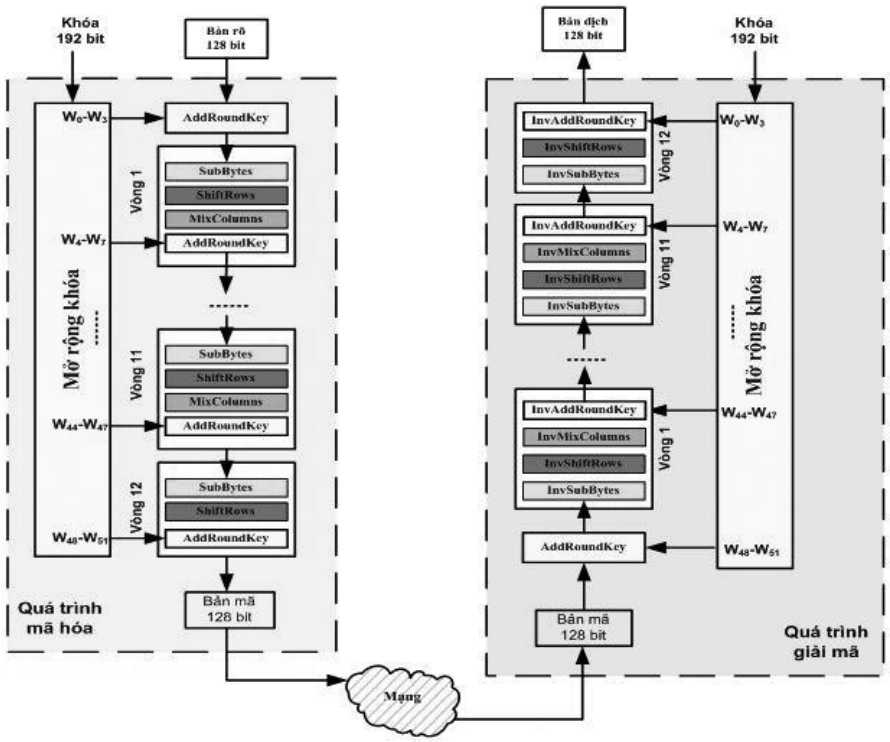
III. GIẢI PHÁP ỨNG DỤNG MẬT MÃ AES

Trong [11] nhóm tác giả đã sử dụng phương pháp bảo mật bằng DES, tuy nhiên sau khi sử dụng một số công cụ tấn công thì DES không còn bền vững trong thời gian yêu cầu đối với hệ thống mạng điều khiển công nghiệp. Với RSA, đòi hỏi cơ sở hạ tầng về nguồn lực tính toán lớn với những phép tính số có độ dài theo bit là 2048 (theo NIST công bố về tiêu chuẩn an toàn cho RSA từ năm 2013) [12]. Bên cạnh đó, theo sự phát triển của mật mã hiện đại, AES được sử dụng rộng rãi, an toàn hơn trong các mạng truyền dữ liệu. Do đó nhóm tác giả chọn AES để triển khai hệ thống bảo mật mô tả trong bài báo này.

Dựa trên những phân tích ở trên, chúng tôi xây dựng một số giải pháp bảo mật cho các hệ thống điều khiển mạng (bộ cảm biến với các bộ điều khiển và cơ cấu chấp hành) (Hình 2), bao gồm: Thiết kế, sử dụng thuật toán mã hóa AES để bảo vệ thông tin truyền giữa các thiết bị (bộ cảm biến, cơ cấu chấp hành và bộ điều khiển); xây dựng giải pháp phát hiện tấn công và cơ chế phản ứng.



Hình 2. Kiến trúc hệ thống truyền thông an toàn trong mạng điều khiển công nghiệp



Hình 3. Sơ đồ thuật toán mã hóa và giải mã AES

A. Mật mã AES

Thuật toán AES (Hình 3) là thuật toán mã hóa đối xứng khóa bí mật, thường được sử dụng cho trường hợp yêu cầu tốc độ nhanh. Nó dựa trên chế độ mã khối với kích thước khối dữ liệu 128 bit và độ dài khóa tùy biến (128, 192, hoặc 256 bit). Trong hệ thống mô phỏng mà chúng tôi thực hiện, các dữ liệu truyền qua mạng, sử dụng các số thập phân trong phạm vi từ 1 đến -1, vì vậy sẽ xử lý dữ liệu theo một khối định dạng trước. Dữ liệu đó chính là bản rõ, mỗi byte của bản rõ được kết hợp với khóa con (*W0-W3*) được tạo ra từ quá trình tạo khóa của Rijndael. Sau đó, thực hiện 12 vòng mã hóa với các khóa con tiếp theo từ quá trình mở rộng khóa (chi tiết ở Mục II.B). Cuối cùng, đầu ra là bản mã có độ dài 128 bit (dữ liệu đã được mã hóa) được truyền đi.

Quá trình giải mã được thực hiện ngược lại. Tuy nhiên, các khóa con được đưa vào ngược với quá trình mã hóa và dữ liệu sau khi được giải mã sẽ được khôi phục lại đúng dạng ban đầu (sử dụng khóa bí mật dùng chung cho cả quá trình mã hóa và giải mã).

B. Mở rộng khóa

AES trong hệ thống mà chúng tôi triển khai sử dụng một khóa có độ dài 192 bit. Khóa mã được mở rộng thành 12 vòng, tương ứng với 12 vòng trong quá trình mã hóa, sử dụng thuật toán mở rộng khóa. Thuật toán mở rộng khóa này chỉ phụ thuộc vào khóa mã và độc lập với quá trình xử lý dữ liệu. Vì vậy, quá trình mở rộng khóa được thực hiện trong một môđun độc lập với quá trình mã hóa và giải mã. Trọng tâm của thuật toán là tạo ra các khóa vòng được kết hợp với các hàm biến đổi *SubWord(RotWord(temp))*, *SubWord(temp)* và sử dụng giá trị *RCON*.

```
Nb=4; //Số cột trong các word 32 bit trong các State
Nk=6; //Số các word 32 bit trong khóa mã
Nr=12; // Số vòng thực hiện mã hóa và giải mã
KeyExpansion(byte key[4*Nk], word w[Nb*(Nr+1)], Nk)
{
word temp;
i=0;
while (i<Nk)
    {
     w[i]=word(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3]);
     i=i+1;
    }
i=Nk;
while (i<Nb*(Nr+1))
    {
    temp=w[i-1];
    if (i mod Nk = 0)
        temp=SubWord(RotWord(temp)) xor RCON[i/Nk];
    else
        if (Nk > 6  and (i mod Nk =4))
            temp=SubWord(temp);
    w[i]=w[i-Nk] xor temp;
    i=i+1;
    }
}
```

Hình 4. Thuật toán mở rộng khóa AES-192

C. Môđun phát hiện tấn công

Dữ liệu được truyền đi có thể bị thay đổi trên đường truyền trong hệ thống điều khiển (bao gồm dữ liệu mẫu từ các bộ cảm biến, thông tin đầu ra

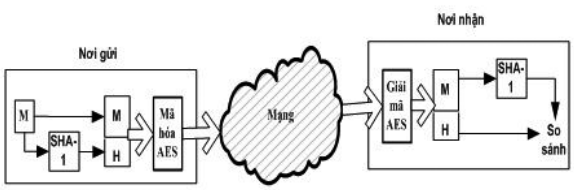
của các bộ điều khiển) và sẽ ảnh hưởng đến sự ổn định, chính xác của hệ thống điều khiển công nghiệp thậm chí có thể gây những tổn thất lớn về kinh tế - xã hội.

Phát hiện các cuộc tấn công bằng cách kiểm tra xem dữ liệu có bị thay đổi hay không có thể sử dụng hàm băm SHA-1. Quá trình xử lý (Ví dụ, quy trình truyền tín hiệu từ bộ cảm biến đến bộ điều khiển trên Hình 2) được thể hiện trong Hình 5.

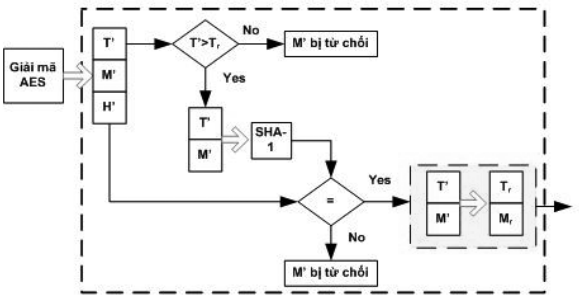
Thông tin gửi đi *M* sẽ được cho qua hàm băm SHA-1 để tạo ra mã băm *H*. Mã băm này sẽ được gửi cùng với thông tin *M*. Tiếp theo, toàn bộ những thông tin này sẽ được mã hóa AES và gửi tới bên nhận. Tại bên nhận, gói tin sẽ được giải mã để thu được thông tin *M* cùng với mã băm *H*. Tiếp theo, *M* được cho qua hàm băm SHA-1 để tạo ra mã băm mới *H*'. Nếu mã băm mới H' và mã băm *H* được gửi đến tương ứng với nhau thì thông tin được xác thực và chuyển cho cơ cấu chấp hành hoặc bộ điều khiển. Nếu hai mã băm này không bằng nhau, chứng tỏ thông tin đã bị sửa đổi trên đường truyền hoặc bị giả mạo. Lúc này, thông tin *M* sẽ chuyển sang môđun phản ứng được trình bày trong mục tiếp theo.

D. Môđun phản ứng

Tại môđun này ta phải xác thực hai yếu tố là thời gian và mã băm. Khi môđun phát hiện tấn công nhận thấy hai thông tin thu được có sự sai lệch thì sẽ chuyển chúng sang môđun phản ứng. Tại đây, thông tin sau khi giải mã sẽ chứa ba thông tin là mốc thời gian *T'*, thông tin *M'*, mã băm *H'*. Môđun sẽ tách phần thời gian để so sánh với thời gian đăng ký. Nếu thời gian đó lớn hơn thời gian đăng ký thì thông tin sẽ bị từ chối (huỷ bỏ vì nghi ngờ có giả mạo hoặc bị tấn công). Ngược lại, sẽ cho thông tin và thời gian qua hàm băm SHA-1 một lần nữa để được mã băm mới, rồi so với mã băm *H* trong phần giải mã. Nếu bằng nhau thì đó chính là thông tin đã đăng ký, ngược lại, thông tin sẽ bị từ chối (huỷ bỏ). Như vậy, hệ thống sẽ nhanh chóng phát hiện thông tin sai và không bị điều khiển sai lệch.



Hình 5. Môđun phát hiện tấn công



Hình 6. Môđun phản ứng

E. Thử nghiệm

BẢNG 1. THỜI GIAN MÃ HÓA, GIẢI MÃ VÀ XÁC THỰC VỚI AES-192 VÀ HÀM BĂM SHA-1

Kích thước dữ liệu	**Thời gian mã hóa AES-192 (s)**	**Thời gian giải mã AES-192 (s)**	**Thời gian xác thực SHA-1 (s)**
25 Kb	0,822	0,825	0,459
50Kb	1,224	1,241	0,643
100Kb	2,336	2,417	0,949
120Kb	3,015	3,109	1,211
150Kb	3,998	4,022	2,029

Chạy thử nghiệm hệ thống mã hóa AES-192 kết hợp với hàm băm SHA-1 với kích thước dữ liệu khác nhau, Bảng 1 đưa ra kết quả chi tiết về thời gian thực hiện mã hóa, giải mã và xác thực trong quá trình xử lý dữ liệu truyền giữa các thiết bị trong hệ thống, mô phỏng trong môi trường MATLAB.

IV. KẾT LUẬN

Hệ thống điều khiển công nghiệp đòi hỏi việc xử lý thông tin phải an toàn, chính xác và tốc độ nhanh. Mật mã AES đáp ứng được yêu cầu về tốc độ trong môi trường truyền mạng khu vực trường. Với giải pháp này, thông tin được mã hóa và giải mã với tốc độ cao, đáp ứng được việc truyền thông tin điều khiển giữa các bộ cảm biến với các bộ điều khiển và giữa các bộ điều khiển với cơ cấu chấp hành và các thiết bị khác.

Chúng tôi đã trình bày mô hình hệ thống đưa ra giải pháp ứng dụng mật mã AES-192 và xây dựng thực nghiệm thành công hai môđun phát hiện tấn công và phản ứng, nhằm đảm bảo thông tin điều khiển giữa các thiết bị trên an toàn, chính xác và đáp ứng yêu cầu tốc độ.

TÀI LIỆU THAM KHẢO

[1]. Eric D.Knapp, "Industrial Network Security", Elsevier Inc, 2011.

[2]. Sjoerd Peerkamp, "Process Control Network Security", ICT Security and Control, 2010.

[3]. Alvaro A.Cárdenas, Saurabh Amin, Shankar Sastry, "Research Challenges for the Security of Control Systems", University of California, Berkeley, 2008.

[4]. A. Treytl, T. Sauter, C. Schwaiger, "Security measures for Industrial Fieldbus Systems – State of the Art and Solutions for IP-Based Approaches" in Proc. WFCS 2004 IEEE International Workshop on Factory Communication System, 2004.

[5]. M. Tangermann, D. Reinetl, "Security concept for automation networks" in Praxis Profiline Industrial Ethernet Volume D/E, Vogel Industrie Medien GmbH & Co. KG, Wurzburg, 2006.

[6]. Alvaro A.Cárdenas, Saurabh Amin, Shankar Sastry, S. Secure control: Towards survivable cyber-physical systems. In Proceedings of the First International Workshop on Cyber-Physical Systems, June 2008.

[7]. William Stallings, "Cryptography and Network security Principles and Practice", Fifth Edition, 2011.

[8]. FIPS-197, National Institue of Standards and Technology, 11-2001.

[9]. AES page http://www.nist.gov/CryptoToolkit

[10]. P. Neumann, "Communication in industrial automation - what is going on?" in Control Engineering Practice. Elsevier Ltd, 2006, vol. 15, pp. 1332–1347.

[11]. Nguyễn Đào Trường, Nguyễn Đức Tâm, "Một phương pháp chống tấn công giả mạo trong hệ thống điều khiển", Tạp chí Nghiên cứu KH-CN số 31, 06-2014, Tr. 104-108.

[12]. NIST SP 800-131A, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", 2011.

SƠ LƯỢC VỀ TÁC GIẢ

ThS. Nguyễn Đào Trường

Đơn vị công tác: Học viện Kỹ thuật Mật mã, Ban Cơ yếu Chính phủ, Hà Nội.

E-mail: truongnguyendao@gmail.com

Tốt nghiệp Học viện Kỹ thuật Mật mã và Học viện Kỹ thuật Quân sự năm 2001. Nhận bằng Thạc sĩ, Học viện Kỹ thuật Quân sự năm 2010.

Hướng nghiên cứu hiện nay: An toàn thông tin.

ThS. Nguyễn Đức Tâm

Đơn vị công tác: Học viện Kỹ thuật Mật mã, Ban Cơ yếu Chính phủ, Hà Nội.

E-mail: nguyenductamkma@gmail.com

Tốt nghiệp chuyên ngành Kỹ thuật điện, điện tử và truyền thông, Học viện Kỹ thuật Mật mã năm 1996 ; Công nghệ thông tin, Đại học Bách khoa Hà nội, năm 2000. Nhận bằng Thạc sĩ Kỹ thuật điện - điện tử và truyền thông, Học viện Kỹ thuật Mật mã năm 2005.

Hướng nghiên cứu hiện nay: Khoa học và công nghệ mật mã, An toàn thông tin.

ThS. Nguyễn Thị Thu Nga

Đơn vị công tác : Sở Giáo dục và Đào tạo Bắc Ninh, Bắc Ninh.

E-mail: ngant1983@hotmail.com

Tốt nghiệp chuyên ngành sư phạm tin học, Đại học Sư phạm Huế năm 2007. Nhận bằng Thạc sĩ chuyên ngành Khoa học máy tính, Đại học Công nghệ thông tin và truyền thông - Đại học Thái Nguyên năm 2014.

Hướng nghiên cứu hiện nay: Phương pháp nâng cao hiệu năng một số thuật toán Mã hóa.