Kỷ yếu Hội nghị Quốc gia lần thứ X về Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR), Đà Nẵng, ngày 17-18/08/2017
DOI: 10.15625/vap.2017.00093

PHƯƠNG PHÁP MÃ HÓA XÁC THỰC AN TOÀN VÀ HIỆU QUẢ TRONG MẠNG ĐIỀU HÀNH GIÁM SÁT CÔNG NGHIỆP

Nguyễn Đào Trường

Học viện Kỹ thuật Mật mã

truongnguyendao@hotmail.com

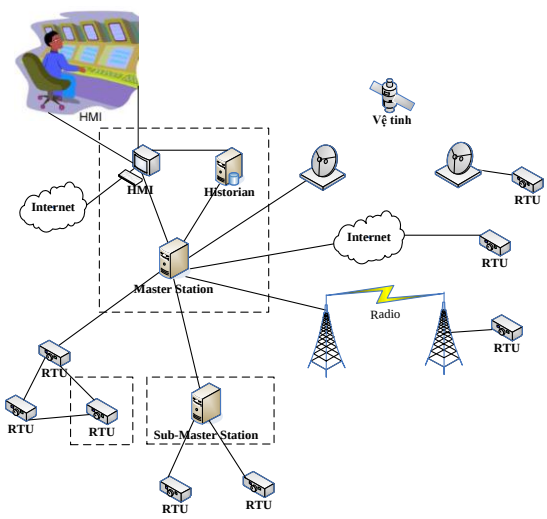
TÓM TẮT: *Mạng điều hành giám sát công nghiệp được sử dụng rộng rãi trong các cơ sở hạ tầng quan trọng của các quốc gia. Sự ngưng hoạt động của mạng này có thể gây ra những hậu quả nghiêm trọng đối với quốc gia đó. Do các giao thức được sử dụng trong mạng truyền thông của hệ thống này thường không có những giải pháp tốt về vấn đề an toàn. Bài báo đề xuất một giải pháp mã hóa xác thực an toàn với nhiều mức độ khác nhau nhằm đảm bảo truyền thông an toàn và hiệu quả trong toàn bộ hệ thống. Giải pháp đề xuất sử dụng thuật toán mã hóa/giải mã AES (Advanced Encryption Standard) kết hợp với những tham số bí mật mà hai bên cùng thỏa thuận để tạo ra hàng rào bảo vệ nhiều mức. Với giải pháp đề xuất, có khả năng chống lại những tấn công trong mạng điều hành giám sát công nghiệp như tấn công DoS, tấn công giả mạo. Thời gian đáp ứng của giải pháp đề xuất tốt hơn rất nhiều so với giải pháp hiện có.*

Từ khóa: *AES (Advanced Encryption Standard), SSL (Secure Socket Layer), TLS (Transport Layer Security).*

I. GIỚI THIỆU

Hệ thống mạng điều hành giám sát công nghiệp (ĐHGSCN) được sử dụng rộng rãi trong các cơ sở hạ tầng quan trọng để điều khiển tự động, thu thập dữ liệu thời gian thực và theo dõi quá trình xử lý của hệ thống. Khi chúng bị tấn công có thể gây ra những thảm họa cho quốc gia, thiệt hại không chỉ về kinh tế mà còn liên quan tới an ninh của đất nước. Ngày nay, do nhu cầu mà mạng ĐHGSCN có những kết nối phức tạp, đặc biệt là những đường kết nối ra bên ngoài thông quan các đường truyền công cộng như Internet [1]. Do đó, nó lại là hiểm họa cho hệ thống mạng ĐHGSCN từ những tấn công trên mạng vào các giao thức truyền thông mà thường được sử dụng trong hệ thống mạng nhưng không có những cơ chế an toàn như DNP3 [2], [3]. Bài báo tập trung nghiên cứu đề xuất một thuật toán mã hóa xác thực an toàn dựa trên giao thức DNP3 để bảo vệ dữ liệu trong quá trình truyền trên mạng.

Hệ thống ĐHGSCN thông thường có ba loại thiết bị truyền thông gồm HMI (Human Machine Interface), MTU (Master Terminal Unit) và RTU (Remote Terminal Unit) [7]. Kiến trúc mạng của hệ thống ĐHGSCN thường là tĩnh ít có những biến động. Các đường truyền giữa các nút được biết trước, chỉ có một vài thay đổi trong mạng khi thêm hoặc bớt RTU. Quá trình truyền thông chỉ xuất hiện giữa HMI với MTU, MTU với SUB-MTU, hai SUB-MTU với nhau, MTU với RTU, hai RTU với nhau. Truyền thông HMI-MTU có thể được thực hiện dễ dàng qua dịch vụ web sử dụng các giao thức cơ bản trong bộ giao thức TCP/IP. Tuy nhiên, truyền thông HMI-MTU ít có những giới hạn về tài nguyên hơn so với các truyền thông còn lại (hình 1).



Hình 1. Kiến trúc mạng ĐHGSCN

Có ba yêu cầu cơ bản về an toàn truyền thông trong mạng ĐHGSCN: bí mật, toàn vẹn và tin cậy [4]. Bí mật dữ liệu là bảo vệ dữ liệu truyền trên đường truyền trước các tấn công thụ động [5] như nghe trộm và theo dõi đường truyền. Mã hóa là giải pháp hiệu quả nhất để đảm bảo tính bí mật của dữ liệu trên đường truyền. Có nhiều thuật toán mã hóa nổi tiếng như DES (Data Encryption Standard), 3DES (Triple DES), RSA và AES. Trong bài báo này chúng tôi lựa chọn sử dụng AES vì theo công bố của NIST (National Institute of Standards and Technology) [6] thì AES [9] đáp

ứng yêu cầu an toàn cho các hệ thống còn DES hoặc 3DES không đáp ứng mức độ an toàn hiện nay. Trong khi đó, nếu sử dụng RSA thì độ an toàn của hệ thống phụ thuộc vào độ dài của khóa, theo NIST thì độ dài hiện nay là 2048 bit, với độ dài bít này thì tốc độ tính toán trong hệ thống ĐHGSCN là không thể đáp ứng trong thời gian ngắn và có những yêu cầu khắt khe (trong phần tiếp theo).

II. NHỮNG RÀNG BUỘC HỆ THỐNG TRONG MẠNG ĐHGSCN

Mạng ĐHGSCN khác với các môi trường mạng thông thường do môi trường hoạt động của nó thường nằm trong các cơ sở hạ tầng quan trọng của quốc gia. Vì vậy, mạng này có một số ràng buộc sau:

- Khả năng tính toán hạn chế: Những thiết bị ở xa như các RTU (Remote Terminal Unit) là một hệ thống nhúng có không gian lưu trữ và khả năng tính toán thấp.
- Tốc độ truyền dữ liệu thấp: Vì hệ thống ĐHGSCN được sử dụng trong thời gian dài, đường truyền trong mạng thường có băng thấp.
- Xử lý thời gian thực: Hệ thống ĐHGSCN cần chính xác. Độ trễ trong quá trình xử lý dữ liệu có thể dẫn đến một số vấn đề nguy hiểm.

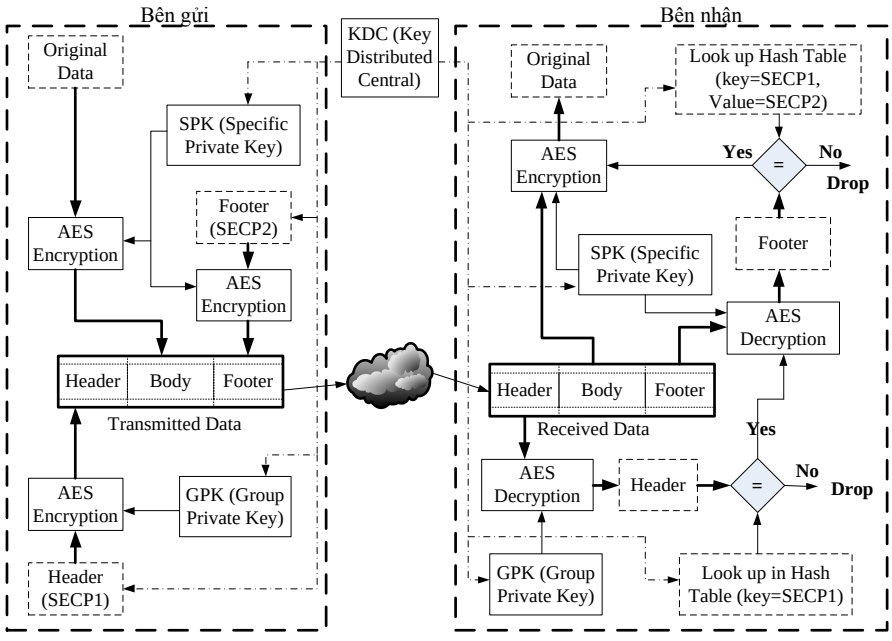
Những ràng buộc của hệ thống ĐHGSCN ở trên làm cho nó khó được áp dụng những công nghệ an toàn đòi hỏi tính toán lớn, vì vậy những ràng buộc đó được xem là cơ sở cho việc áp dụng những cơ chế an toàn.

III. ĐỀ XUẤT GIẢI PHÁP MÃ HÓA XÁC THỰC NHIỀU THAM SỐ AN TOÀN

A. Hai tham số bí mật

Ý tưởng của giải pháp là khi MTU trao đổi thông tin với RTU thì hai bên sẽ chia sẻ trước và giữ hai khóa bí mật, hai tham số bí mật cùng với một bảng băm tại mỗi thiết bị RTU và MTU như sau:

- Khóa bí mật đầu tiên là khóa nhóm (*GPK*: Group Private Key) mà MTU đó liên kết với tất cả các RTU, để truyền thông giữa MTU với tất cả các RTU liên kết với MTU này.
- Khóa thứ hai là khóa riêng (*SPK*: Specific Private Key) để truyền thông giữa MTU với mỗi RTU riêng biệt.
- Hai tham số bí mật phiên (*SECP1* và *SECP2*) giữa MTU và mỗi RTU tạo thành một cặp gửi-nhận.
- Bảng băm chứa danh sách các cặp ***Khóa-Giá trị*** tương ứng với danh sách ***SECP1***-(***SPK***, ***SECP2***), tức là Khóa là *SECP1* thì giá trị là (*SPK*, *SECP2*) tương ứng.



Hình 2. Mô hình xác thực hai tham số an toàn

Để gửi một thông điệp từ MTU đến RTU và ngược lại, quá trình xác thực được thực hiện theo thuật toán sau:

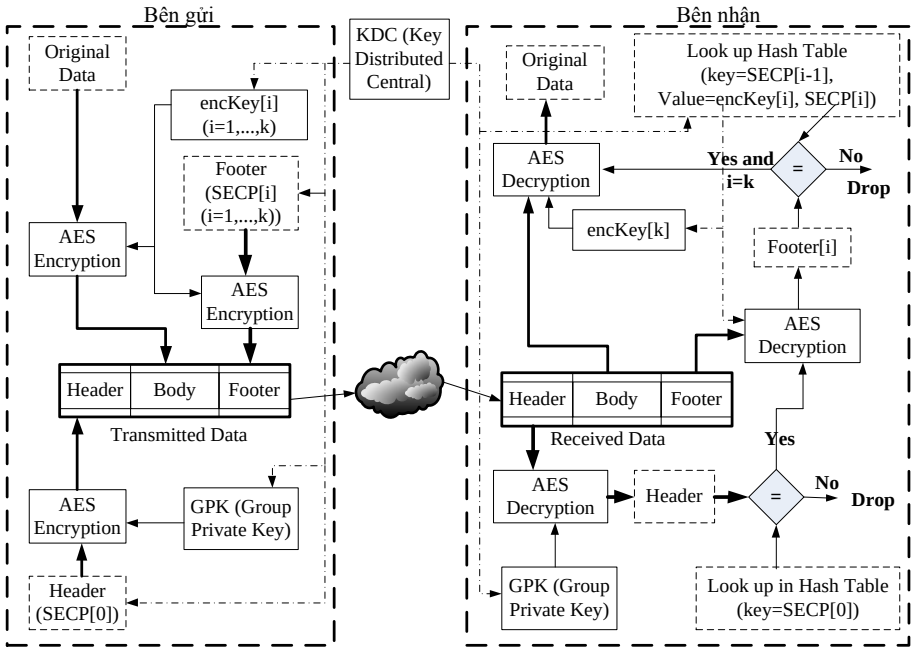
Bên gửi	***Bên nhận***
Khởi tạo, thỏa thuận: *SECP1, SECP2, GPK, SPK*	
Header←SECP1; *encHeader* = Encrytion(Header,GPK); *encBody* = Encryption(message,SPK); Footer ← SECP2; *encFooter* = Encryption(Header,SPK); Msg = *encHeader* + *encBody* + *encFooter*;	Set HashTable()

Msg →	

	Header = Decryption(*encHeader*,GPK);
	If LookHashTable(Header) = True
	  If Decryption(*encFooter*, SPK) = SECP2
	  message = Decryption(*encBody*, SPK)
	  Else Drop();
	Else Drop();

B. Nhiều tham số bí mật

Mục tiêu của phần này là tạo ra mức an toàn hệ thống mạng ĐHGSCN ở những mức khác nhau, được khởi tạo ở mức L1 và tăng lên L2 trong trường hợp gửi nhiều thông điệp quan trong, hoặc phát hiện sự tăng lên về mức độ mối đe dọa, và tiếp tục tăng nó đến mức L10 (nếu cần thiết) trong trường hợp bị tấn công nghiêm trọng. Như phần trước đã trình bày giải pháp xác thực truyền thông giữa hai bên tham gia phụ thuộc vào hai tham số bí mật (*SECP1*, *SECP2*) và hai khóa bí mật (*GPK*, *SPK*).



Hình 3. Mô hình mã hóa xác thực nhiều tham số an toàn

Ý tưởng ở đây là khái quát từ giải pháp xác thực hai khóa bí mật, hai tham số bí mật thành $k+1$ khóa bí mật, $k+1$ tham số bí mật thay cho hai khóa bí mật, hai tham số bí mật. Giải pháp được mô tả trong hình 3 được thực hiện theo thuật toán sau:

Bên gửi	***Bên nhận***
Khởi tạo, thỏa thuận: *SecrityLevel >2*, *GPK*, *SECP*[*i*], *encKey*[*i*], *i* = 0…*k-1*, (*k* = *SecurityLevel*)	

Header←*SECP*[0];
encHeader = Encryption(Header,*GPK*);
encBody = Encryption(message,encKey[k]);
For i = 1…*k-1*
  encFooter ← *encFooter* + Encryption(*SECP*[*i*], encKey[*i*]) ;
Msg = *encHeader* + *encBody* + *encFooter*;
	Set HashTable();

Msg →	

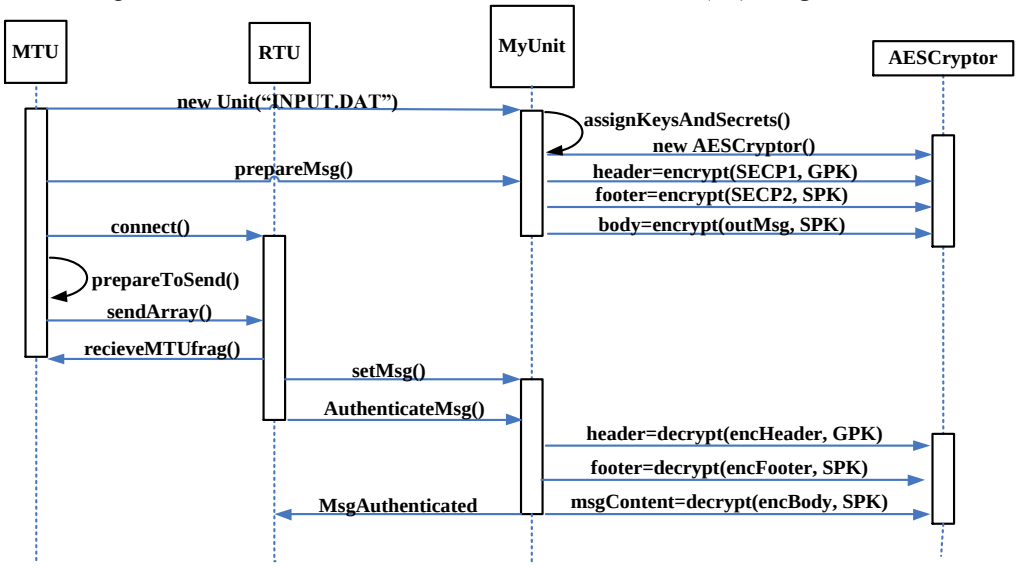
	Header = Decryption(*encHeader*,*GPK*);
	Found = True; *i* = 0;
	If LookHashTable(Header)= True {
	  While (*i* < *k* and Found) {
	  Footer[*i*] = Decryption(*encFooter*[*i*], encKey[*i*]);
	  If LookHashTable(Footer[*i*]) = True
	  Inc(*i*);
	  Else Found = False }
	  If Found
	  message = Decryption(*encBody*, encKey[*i*])
	  Else Drop();}
	Else Drop();

IV. TRIỂN KHAI GIẢI PHÁP ĐỀ XUẤT TRONG MÔI TRƯỜNG MẠNG ĐHGSCN MÔ PHỎNG

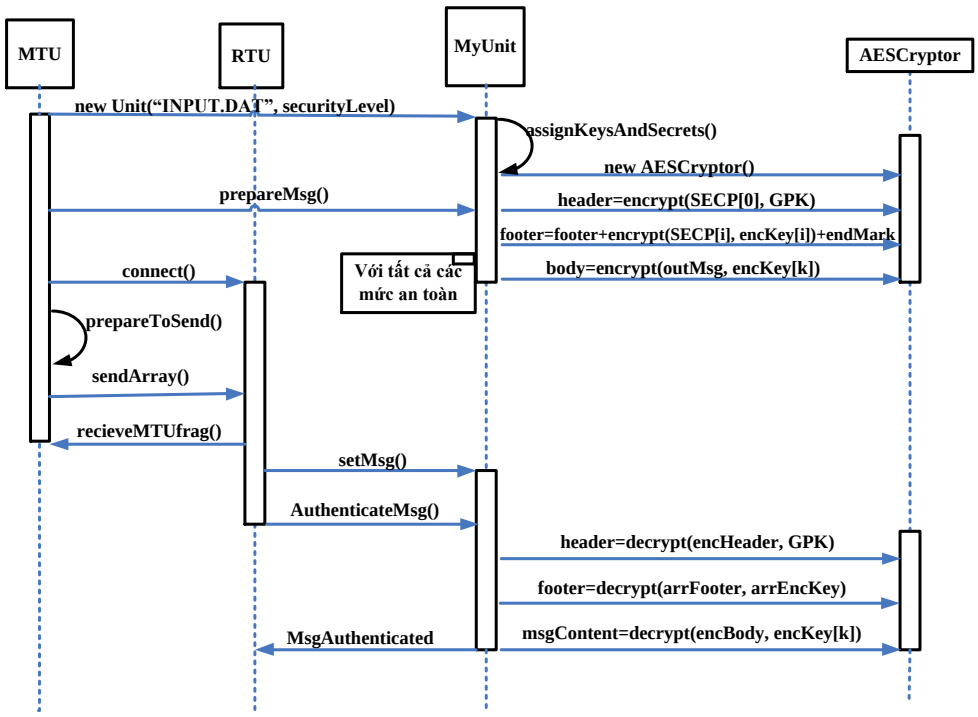
A. Mô hình thực nghiệm mô phỏng

Việc thử nghiệm được thực hiện trên hai máy trong hệ thống ĐHGSCN giả lập, một máy coi như MTU, còn máy kia coi như RTU. Máy MTU là một máy tính chạy Windows 7 bộ vi xử lý Intel Core i5 Dual Core 2,4GHz*2,4GHz, RAM 4GB và máy còn lại chạy Windows 7 bộ vi xử lý Intel Core i5 2,4GHz, RAM 2GB đóng vai trò là RTU. Hai máy này được nối mạng với nhau qua 2 Switch Planet và 02 Router Cisco.

Quá trình truyền thông an toàn giữa MTU và RTU với các mức an toàn gồm mã hóa xác thực với hai tham số an toàn được thể hiện như trong hình 4 và mã hóa xác thực với nhiều tham số an toàn (≥3) trong hình 5.



Hình 4. Quá trình mã hóa xác thực hai tham số an toàn với giao thức DNP3 mô phỏng

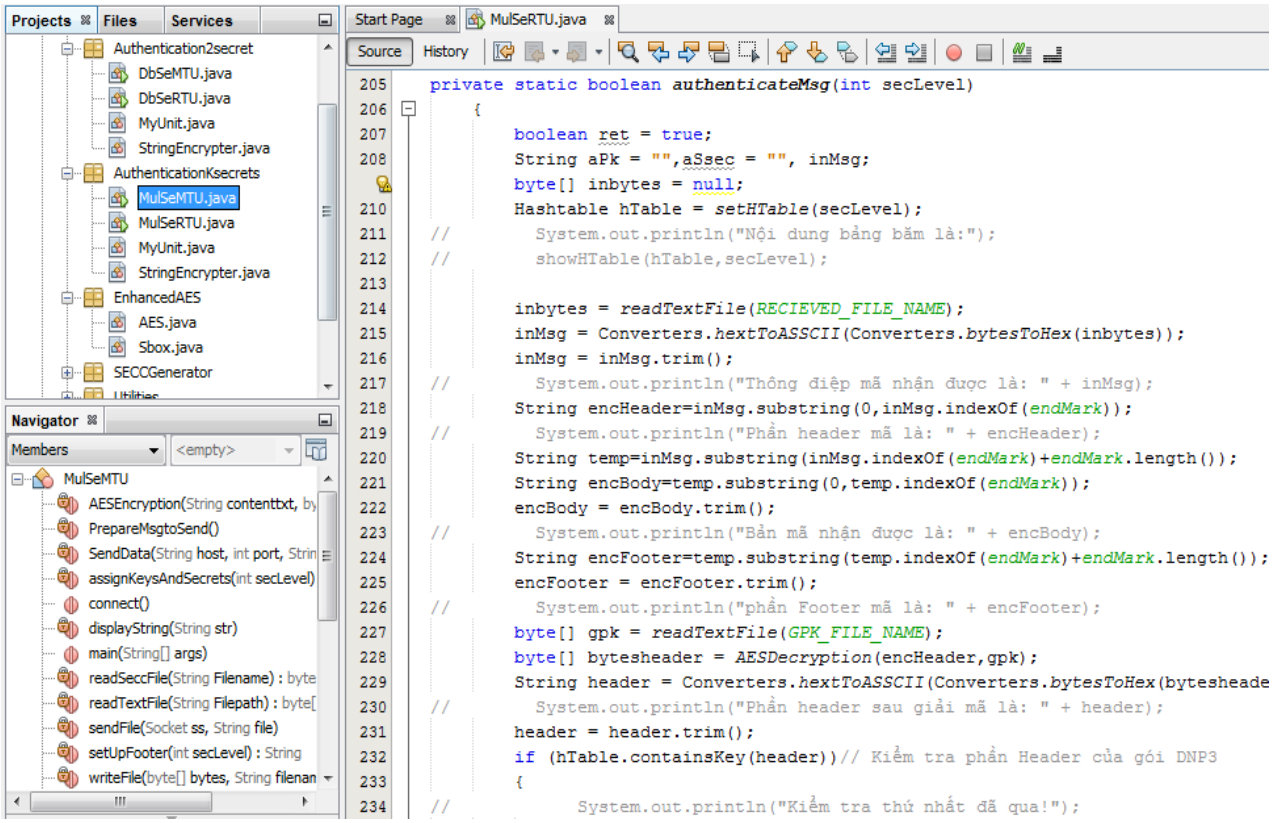


Hình 5. Quá trình mã hóa xác thực nhiều tham số an toàn với giao thức DNP3 mô phỏng

B. Các môđun mã hóa xác thực nhiều tham số an toàn

Các môđun mã hóa xác thực nhiều tham số an toàn được thực hiện bằng mô phỏng trên công cụ Java, mô tả quá trình đóng gói, mã hóa, xác thực gói tin DNP3.

Chương trình gồm: Lớp **EnhancedAES** là lớp tạo ra các hàm mã hóa và giải mã sử dụng thuật toán AES; Lớp **Authentication2secret** là lớp tạo ra quá trình truyền thông giữa MTU và RTU xác thực bằng hai tham số an toàn; Lớp **AuthenticationKsecrets** là lớp truyền thông an toàn nhiều mức an toàn tương ứng với nhiều tham số an toàn giữa MTU và RTU.



Hình 6. Cấu trúc các môđun xác thực nhiều tham số an toàn

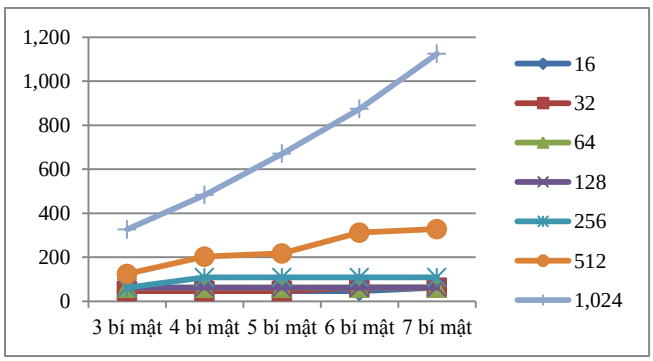
C. Một số kết quả thử nghiệm

Các thử nghiệm được thực hiện và thống kê thời gian thực hiện giữa xác thực nhiều tham số bí mật, SSL/TLS. Thực nghiệm được thực hiện truyền một file text đơn giản có kích thước 16B trên máy đóng vai trò MTU truyền sang máy khác đóng vai trò RTU. Các khóa bí mật được sử dụng để mã hóa và giải mã bằng AES[9] có kích thước là 16, 24 và 32 MB tương ứng với AES-128, 192, 256.

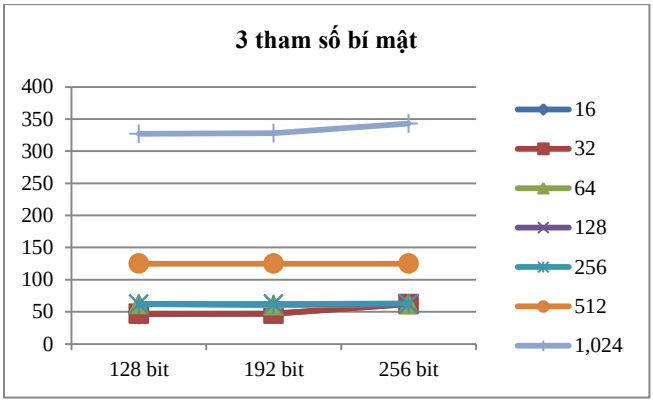
Các file chứa tham số bí mật có kích thước thay đổi từ 16B đến 1KB để làm các bí mật *SECP*[*i*] (*i* =0,...,*k*-1). Các kết quả được phân theo các hình thức sau: Thông điệp DNP3 được triển khai xác thực bằng SSL/TLS sử dụng RSA làm thuật toán trao đổi khóa công khai, SSL/TLS sử dụng Diffie-Hellman để phân phối khóa và DNP3 với xác thực các tham số bí mật sử dụng AES. Các kết quả chi tiết được thể hiện trong bảng 1 và các hình 7, 8, 9, 10.

Bảng 1. Thời gian thực thi của một số mô hình xác thực an toàn

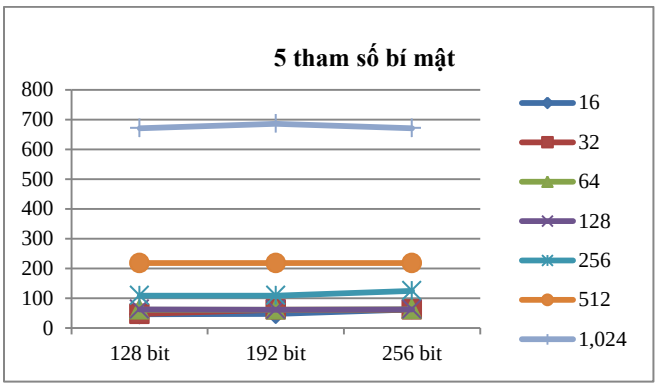
Mô hình xác thực thử nghiệm với DNP3 mô phỏng		*Thời gian trễ trung bình (ms)*
Mô hình đề xuất	**Kích thước tham số bí mật <4096 bit**	**<400**
	Kích thước tham số bí mật >4096 bit	**>400**
SSL/TLS với RSA		2663
SSL/TLS với Diffie-Hellman		2497.6



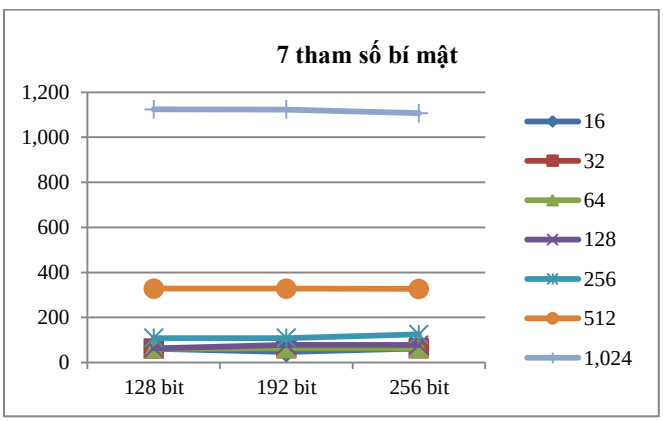
Hình 7. Thời gian truyền thông của các mức an toàn khác nhau với độ dài tham số an toàn từ 16 đến 1024 byte (tương đương từ 128 bit đến 8192 bit)



Hình 8. Thời gian truyền thông ba tham số an toàn với các khóa AES và độ dài tham số an toàn khác nhau



Hình 9. Thời gian truyền thông năm tham số an toàn với các khóa AES và độ dài tham số an toàn khác nhau



Hình 10. Thời gian truyền thông bảy tham số an toàn với các khóa AES và độ dài tham số an toàn khác nhau

V. SO SÁNH GIẢI PHÁP ĐỀ XUẤT VỚI CÁC KIẾN TRÚC KHÁC

A. Giải pháp đề xuất với SSL

Giải pháp đề xuất làm tăng mức độ an toàn, như đã trình bày trong phần III.A và III.B, rõ ràng phương pháp mã hóa nhiều khóa và xác thực sử dụng nhiều tham số an toàn không sử dụng mật mã khóa công khai như SSL, bởi vì việc sử dụng những ánh xạ một chiều để mã hóa dữ liệu đòi hỏi tính toán rất cao, sẽ làm suy hao đáng kể hiệu suất. Vì vậy, giải pháp đề xuất có hiệu suất cao hơn SSL và rất an toàn trong thời gian như nhau.

B. Giải pháp đề xuất với chữ ký số

Cũng như mã hóa khóa công khai, kiến trúc chữ ký số sử dụng khóa công khai và khóa bí mật. Trong kiến trúc xác thực này có một bản tóm lược hàm băm chứa đánh dấu thời gian và thông điệp đó được gửi đi hoặc là một phần của nó. Bên gửi sử dụng khóa bí mật của họ để mã hóa bản tóm lược này và gửi thông điệp đó cùng với bản tóm lược đã mã hóa sang bên nhận. Bên nhận sử dụng khóa công khai để giải mã bản tóm lược đó và tính bản tóm lược trong thông điệp của nó sử dụng đánh dấu thời gian và giải mã thông điệp đã nhận và so sánh hai bản tóm lược này để quyết định việc xác thực bên gửi [8]. So với kiến trúc chữ ký số thì giải pháp đề xuất an toàn hơn vì chúng phụ thuộc vào việc xác nhận ít nhất hai tham số bí mật chứ không phải chỉ một và chính thông điệp cũng được mã hóa không như

trong trường hợp chữ ký số bản rõ gửi đi mà không được mã hóa. Kiến trúc đề xuất cũng nhẹ hơn kiến trúc chữ ký số vì nó không sử dụng mã hóa khóa công khai.

VI. KẾT LUẬN

Bằng giải pháp mã hóa xác thực đề xuất chúng tôi nhận thấy đây là một giải pháp khá phù hợp trong môi trường mạng đòi hỏi tính toán nhanh, với những tài nguyên tính toán của các thiết bị trong hệ thống hạn chế. Đồng thời với đánh giá về thời gian trễ khi thực hiện với giải pháp đề xuất hoàn toàn có thể đáp ứng được với những mạng có yêu cầu khắt khe về thời gian thực thi. Bên cạnh đó giải pháp đề xuất hoàn toàn chống lại được các tấn công cơ bản trong mạng như DoS và tấn công giả mạo. Bởi vì đây là những tấn công rất nguy hiểm và phổ biến trong mạng điều hành giám sát công nghiệp.

TÀI LIỆU THAM KHẢO

[1] C. W. Ten, C. C. Liu, G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems", Power Systems, IEEE Transactions on, vol.23, no. 4, pp. 1836-1846, 2008.

[2] G. Dondossola, J. Szanto, M. Masera, et al. "Effects of intentional threats to power substation control systems". International journal of critical infrastructures, vol.4, no. 1, pp. 129-143, 2008.

[3] G. Hayes, K. El-Khatib. "Securing modbus transactions using hash-based message authentication codes and stream transmission control protocol". Communications and Information Technology (ICCIT), 2013 Third International Conference on. IEEE, pp. 179-184, 2013.

[4] Z. H. Pang, G. P. Liu, "Design and implementation of secure networked predictive control systems under deception attacks", Control Systems Technology, IEEE Transactions on, vol. 20, no. 5, pp. 1334-1342, 2012.

[5] A. Kahate, "Cryptography and network security". Tata McGraw-Hill Education, 2013.

[6] NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), 2015.

[7] Donghyun Choi, Hakman Kim, Dongho Won, and Seungjoo Kim, "Advanced Key Management Architecture for Secure SCADA Communication," To be published on IEEE Transactions on power delivery, 2009.

[8] Hieb, J. L., Graham, J. H., & Patel, S. C. Cyber Security Enhancements for SCADA and DCS Systems. Critical Infrastructure Protection: Issues and Solutions, Springer, 2007.

[9] J. Daemen and V. Rijmen, "The Design of Rijndael: AES-The Advanced Encryption Standard." Springer-Verlag, 2002.

A METHOD OF SECURE AND EFFECTIVE AUTHENTICATED ENCRYPTION IN INDUSTRIAL CONTROL AND MONITOR NETWORK

Nguyen Dao Truong

ABSTRACT: *Industrial control and monitor networks are widely used in the national important infrastructures. The inactivity of this network could have serious consequences for the country. Because protocols used in the communications network of this system often do not have good security solutions. The paper proposes a secure encryption solution with varying degrees of assurance to ensure secure and efficient communication across the entire system. The proposed solution uses the Advanced Encryption Standard (AES) encryption algorithm, which combines the secret parameters that both parties agree on to create a multi-level protection barrier. With the proposed solution, it is capable of combating attacks in industrial control and monitor networks such as DoS attacks, fake attacks.*