Kỷ yếu Hội nghị Khoa học Quốc gia lần thứ IX "Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR'9)"; Cần Thơ, ngày 4-5/8/2016
DOI: 10.15625/vap.2016.000100

VỀ MỘT PHƯƠNG PHÁP NÂNG CAO AN TOÀN TRONG MẠNG ĐIỀU HÀNH GIÁM SÁT CÔNG NGHIỆP

Nguyễn Đào Trường[1], Nguyễn Doãn Cường[2], Nguyễn Đức Tâm[1]
[1] Học viện Kỹ thuật mật mã
[2] Viện Công nghệ thông tin, Viện KHCN Quân sự
truongnguyendao@gmail.com, cuongvncntt@yahoo.com, nguyenductamkma@gmail.com

TÓM TẮT— *Bài báo tập trung nghiên cứu các vấn đề an toàn giao thức truyền thông SCADA. Mạng SCADA (Supervisory Control and Data Acquisition) là công nghệ truyền thông để thu thập dữ liệu từ những thiết bị, cơ sở từ xa và gửi các lệnh điều khiển đến các cơ cấu chấp hành. Do nhu cầu kết hệ thống SCADA với mạng doanh nghiệp và internet, vì vậy những bộ phận SCADA là mục tiêu của các cuộc tấn công mạng, thông qua mục tiêu đó mà những kẻ tấn công có thể dễ dàng đánh sập cơ sở hạ tầng quan trọng và nền kinh tế của quốc gia đó. Để bảo vệ mạng SCADA, chúng tôi tập trung vào giao thức truyền thông chưa được thiết kế an toàn. An toàn thông qua giao thức, với mục đích sửa đổi cấu trúc của giao thức nhằm đảm bảo tính toàn vẹn, xác thực và chống phát lại. Trong cấu trúc đề xuất chúng tôi sử dụng hai thuật toán để cải thiện tính bí mật và toàn vẹn của dữ liệu, đánh dấu thời gian để chống phát lại.*

Từ khóa— *SCADA, CRC, an toàn, bí mật, xác thực.*

I. GIỚI THIỆU

SCADA (Supervisory Control and Data Acquisition) là công nghệ truyền thông để thu thập dữ liệu từ những thiết bị, cơ sở từ xa và gửi các tín hiệu điều khiển đến các cơ cấu chấp hành. Mạng SCADA gồm những máy tính và những ứng dụng thực hiện các chức năng quan trọng trong việc cung cấp các dịch vụ và sản phẩm thiết yếu (như xử lý nước thải, phát điện, truyền tải và phân phối). Hệ thống SCADA[18] là những hệ thống nội bộ và các ứng dụng của nó được mở rộng sang các mạng diện rộng theo sự phát triển của công nghệ. Bản thân hệ thống SCADA phần nào được an toàn và giới hạn những vấn đề an ninh. Do nhu cầu của sự kết nối thì ngày nay các hệ thống SCADA được kết nối với mạng công ty và internet, khi đó mạng SCADA không còn là bất khả xâm phạm với các cuộc tấn công. Những hệ thống này được thiết kế chủ yếu tập trung vào các chức năng và hiệu suất và chưa được quan tâm đích đáng đến vấn đề an ninh an toàn.

Khi mà các hệ thống SCADA được kết nối với mạng công ty và internet [1] thì những hiểm họa đối với vấn đề an toàn mạng hiện hữu. Những hiểm họa này là những mối đe dọa đến nền kinh tế của đất nước và đời sống của người dân. Khi những kẻ tấn công xâm nhập và các bộ phận của mạng SCADA thông qua đó có thể phá hủy các cơ sở hạ tầng quan trọng và gây tổn thất cho nền kinh tế của quốc gia đó. Các cuộc tấn công tiềm ẩn những hành động làm cản trở hoặc gián đoạn các dịch vụ tài chính, tắt các hệ thống cung cấp điện năng. Trong khi hệ thống điều khiển truyền thông hiện đại và việc tính toán cung cấp những cơ hội lớn để cải thiện hệ thống cung ứng điện năng đáp ứng nhu cầu tối ưu hiệu suất sản xuất điện và khả năng phục hồi khi gặp sự cố thì chúng cũng làm cho các hệ thống và quá trình vật lý dễ bị tấn công có chủ ý từ bên trong và bên ngoài.

II. MẠNG ĐIỀU HÀNH GIÁM SÁT CÔNG NGHIỆP

So với các hệ thống công nghệ thông tin (IT) thì hệ thống mạng SCADA có các yêu cầu cao hơn về độ tin cậy, độ trễ và thời gian hoạt động, vì vậy không phải tất cả các giải pháp an toàn mạng IT đều có thể áp dụng vào triển khai cho mạng SCADA. Bí mật, toàn vẹn và sẵn sàng là những mối quan tâm chính trong cả hệ thống IT và SCADA. Sẵn sàng được ưu tiên hàng đầu trong các hệ thống SCADA còn bí mật là mối quan tâm chính trong mạng IT. Cần phải phân tích các mối đe dọa và những lỗ hổng khác nhau ảnh hưởng đến quá trình vận hành của hệ thống SCADA.

Hệ thống SCADA là phần lõi của các hệ thống mạng tự động hóa và mạng công nghiệp tạo nên cơ sở hạ tầng quan trọng quốc gia. Theo truyền thống thì những hệ thống này được triển khai độc lập không có các kết nối ra bên ngoài. Nhưng ngày nay, do nhu cầu kết nối tăng lên từ hệ thống SCADA với mạng công ty và internet (điều khiển từ xa), từ đó cũng để lỗ ra những lỗ hổng từ những mối hiểm họa tấn công mạng. Các bộ phận SCADA[2] được coi là những mục tiêu ưu tiên trong các tấn công mạng thông qua chúng mà các kẻ tấn công có thể dễ dàng đánh sập các cơ sở hạ tầng và nền kinh tế của quốc gia đó. Các cuộc tấn công như vậy có thể ngắt các hệ thống cung cấp điện, làm gián đoạn các dịch vụ tài chính và từ đó cản trở các hoạt động cần thiết của quốc gia.

Bảo vệ hệ thống SCADA để thực hiện các chức năng giám sát và điều khiển các cơ sở hạ tầng tiện ích như điện, khí đốt, nước,… là rất quan trọng liên quan tới an ninh quốc gia. Bất kỳ lỗ hổng nào trong hệ thống này đều có thể gây ra những mối đe dọa nghiêm trọng có thể phá hủy hoặc gián đoạn quá trình hoạt động của chúng. Trong các ứng dụng quan trọng, chiến thuật điều khiển phù hợp sẽ ngăn chặn việc thực thi bất kỳ hành vi độc hại hoặc chưa biết rõ nào. Để bảo vệ hệ thống SCADA, thì quan trọng là phải nắm được những nguy cơ mất an toàn của hệ thống để có thể triển khai các giải pháp bảo mật thích hợp để ngăn chặn các cuộc tấn công mạng.

Việc thiết kế các giao thức trong mạng SCADA[15],[16] truyền thống chưa quan tâm tới an toàn. An toàn hệ thống SCADA thông qua giao thức truyền thông là một giải pháp hợp lý để giải quyết những mối đe dọa vào hệ thống.

Giao thức DNP3 (Distributed Network Protocol Version 3) là giao thức được sử dụng để giao tiếp giữa thiết bị Master và Slave trong các cơ sở hạ tầng quan trọng. An toàn giao thức DNP3 là chủ đề trọng tâm trong bài báo này. DNP3 được thiết kế để tối ưu việc truyền dữ liệu thu thập được và các câu lệnh điều khiển giữa thiết bị master và slave. Nó được thiết kế riêng cho các ứng dụng SCADA, không phù hợp trong môi trường internet. Giao thức DNP3 [10], [12] là một giao thức hiện đại, mở và mạnh mẽ trong môi trường SCADA. DNP3 hoạt động ở tầng thứ 3[5] (tầng ứng dụng trong mô hình EPA) ban đầu được đề xuất bởi IEC (International Electro technical Commission) sau này EPA (Enhanced Performance Architecture) được cải tiến bằng cách thêm vào tầng giả chuyển vận (pseudo transport layer).

A. Tầng ứng dụng

Tầng ứng dụng cung cấp các chức năng chuẩn hóa, định dạng dữ liệu và thủ tục cho việc truyền tải các dữ liệu thu thập được như các giá trị đo, các thuộc tính và các lệnh điều khiển một cách hiệu quả [4]. Các dịch vụ tầng ứng dụng được sử dụng để gửi các thông điệp đến các thiết bị DNP3 và nhận các thông điệp từ các thiết bị DNP3 khác. Một đoạn (fragment) là một khối các octet chứa những thông tin yêu cầu và hồi đáp được truyền giữa thiết bị master và thiết bị bên ngoài. Cấu trúc đoạn ở tầng ứng dụng có hai dạng:

- Đoạn yêu cầu (request fragment)
- Đoạn hồi đáp (response fragment)

Trong đoạn yêu cầu, phần đầu gồm 2 byte: 1 byte là điều khiển ứng dụng, 1 byte là mã hàm chức năng. Trong đoạn hồi đáp, phần đầu gồm 4 byte: 1 byte là điều khiển ứng dụng, 1 byte là mã hàm chức năng, 2 byte chỉ thị bên trong.

B. Tầng giả chuyển vận

Tầng này cho phép chia nhỏ thông điệp. Nó thực hiện chia đoạn dữ liệu dài ở tầng ứng dụng thành các đơn vị dữ liệu có kích thước cố định trong quá trình truyền và ghép chúng lại tại bên nhận.

C. Tầng liên kết dữ liệu

Tầng liên kết dữ liệu truyền dữ liệu trên kênh truyền thông đến thiết bị đích. Tại tầng này thực hiện một số chức năng như đóng gói, gắn địa chỉ đích và nguồn. Nó mã hóa phần dữ liệu chứa dữ liệu được truyền từ tầng giả chuyển vận xuống với phần đầu liên kết dữ liệu có độ dài cố định. Dữ liệu đã mã hóa được truyền trên kênh truyền thông. Khung liên kết dữ liệu DNP3 có khối phần đầu độ dài cố định (10 octet), tiếp theo là các khối dữ liệu tùy chọn. Mỗi khối kết thúc bằng một mã kiểm tra lỗi CRC (Cyclic Redundancy Check) 16 bit. Khung dữ liệu có độ dài 292 octet.

D. Tầng vật lý

Tầng vật lý là tầng làm nhiệm vụ truyền các thông điệp trên các thiết bị truyền thông vật lý.

III. AN TOÀN MẠNG ĐIỀU HÀNH GIÁM SÁT CÔNG NGHIỆP

A. An toàn thiết bị

Thiết bị trong mạng điều hành giám sát công nghiệp đôi khi ở những vị trí rất xa, vì vậy an toàn thiết bị được đặt lên hàng đầu trong quá trình thiết kế và triển khai những thiết bị này.

B. An toàn giao thức

An toàn không được thiết kế trong giao thức DNP3. Giao thức DNP3 không có các kỹ thuật mã hóa và xác thực trong cấu trúc của nó. Kẻ xâm nhập có thể sử dụng các công cụ phân tích giao thức như "Ethereal" hoặc những kỹ thuật đã biết khác để chặn bắt các khung dữ liệu DNP3. Hệ quả là kẻ tấn công bắt các khung dữ liệu không mã hóa (bản rõ) từ một ứng dụng mạng hệ thống SCADA. Bằng cách đó, kẻ tấn công sẽ có được những địa chỉ đích và địa chỉ nguồn của các thiết bị trong hệ thống. Kẻ tấn công có thể sử dụng những khung dữ liệu không được mã hóa chứa những thông tin điều khiển và những thông tin thiết lập hệ thống trong những tấn công tiếp theo vào các thiết bị khác trong hệ thống SCADA hoặc những thiết bị thông minh IED (Intelligent Equipment Device). Những tấn công như vậy có thể tắt các phần mềm MTU, tắt máy tính MTU, hoặc làm cho các RTU ngừng hoạt động. Ngoài ra, kẻ tấn công có thể thay đổi các tham số cài đặt trong IED, bộ điều khiển hoặc toàn bộ hệ thống SCADA, điều đó không những làm cho thiết bị không thể hoạt động khi cần, mà còn gây lỗi bus, lỗi đường truyền, gián đoạn các dịch vụ [13].

Toàn vẹn và xác thực là vô cùng quan trọng trong mạng điều hành giám sát công nghiệp khi mà các thao tác dữ liệu trái phép của đối phương có thể gây ra những hậu quả vô cùng nghiêm trọng. Những tấn công kẻ đứng giữa, phát lại, chối bỏ trực tiếp vào những mạng này trong trường hợp thiếu những nguyên tắc xác thực và toàn vẹn. Do đó, giải pháp an toàn giao thức trong mạng điều hành giám sát công nghiệp là một giải pháp tối ưu. Phần tiếp theo sẽ trình bày về giải pháp đề xuất này.

C. Giải pháp an toàn đề xuất

Trong phần này xem xét các khía cạnh an toàn truyền thông của giao thức DNP3 trong mạng SCADA. Chúng tôi tập trung vào cải tiến an toàn giao thức DNP3 để giảm thiểu mối đe dọa trong hệ thống SCADA. Chủ yếu tập trung vào phân bố lại các byte trong giao thức, với những phân bố lại đó chúng tôi sử dụng các thuật toán như CRC cải tiến,

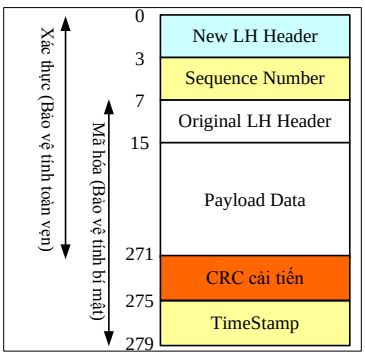
mật mã AES (Advanced Encryption Standard), đánh dấu thời gian (TS – TimeStamp) và chữ ký số để đảm bảo các khía cạnh an toàn. Giao thức DNP3 truyền thống chỉ sử dụng CRC để phát hiện lỗi trong quá trình truyền [9], [11]. Chúng tôi đề xuất hai hình thức an toàn sau:

- Mã hóa gói tin DNP3.
- Cải tiến cấu trúc bên trong giao thức DNP3.

Sử dụng 34 byte ngoài 272 byte PDU (Protocol Data Unit) liên kết DNP3 để cho mục đích an toàn và toàn vẹn. Chúng tôi phân phối lại các byte này để tăng cường phạm vi dữ liệu và an toàn cho giao thức DNP3 bằng sự sắp xếp lại như sau:

- New LH Header (4 byte)
- Key Sequence Number (4 byte)
- Original LH Header (8 byte)
- Payload Data (256 byte)
- CRC cải tiến (4 byte)
- TimeStamp (4 byte).

Trong giải pháp đề xuất của chúng tôi, thông điệp được bảo vệ bằng mật mã AES cải tiến [17] và giải thuật CRC cải tiến để xác thực, đánh dấu thời gian (TimeStamp) chống phát lại, như trong Hình 1.



Hình 1. Cấu trúc gói tin giao thức DNP3 đề xuất (MoDNP3)

Trong giao thức đề xuất (MoDNP3), thông điệp được bảo vệ bằng:

- Thuật toán mã hóa/ giải mã AES: AES cung cấp tính bí mật bằng cách mã hóa dữ liệu.
- Thuật toán CRC cải tiến để xác thực dữ liệu trong giao thức: CRC cải tiến giúp giúp xác thực dữ liệu ở cả bên gửi và bên nhận. Trong CRC cải tiến, sử dụng 4 byte trong giao thức MoDNP3.
- Đánh dấu thời gian (TimeStamp): sử dụng giao thức NTP (Network Time Protocol)[7] để đánh dấu thời gian, sử dụng 4 byte.

1. Thuật toán mã hóa AES cải tiến

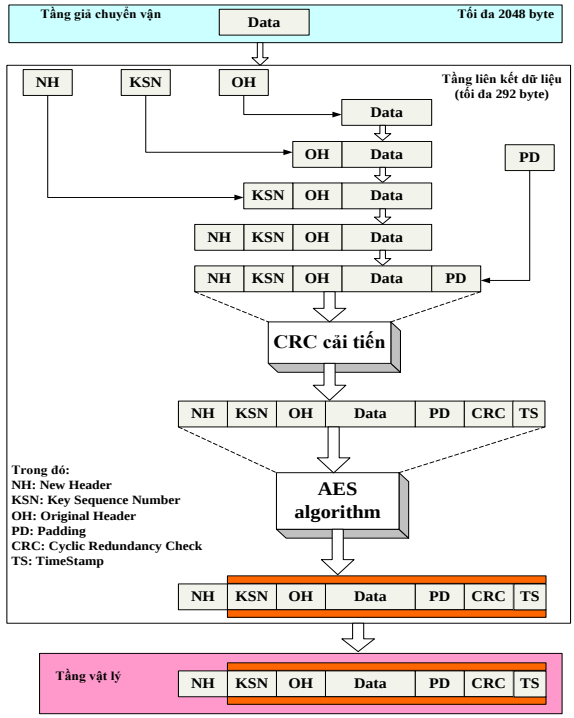
AES cải tiến [17] là mã khối đối xứng có độ dài khóa thay đổi (128, 192, 256). Nó được Rijndael đề xuất năm 2001. Thuật toán AES gồm hai phần: Phần mở rộng khóa phục vụ cho các vòng mã và phần mã hóa. Trong phần mở rộng khóa, khóa đầu vào có thể là 128, 192 hoặc 256 bit. Quá trình mã hóa dữ liệu gồm 10, 12, 14 vòng thực hiện mã hóa tương ứng với các độ dài khóa 128, 192, 256.

Trong kịch bản của chúng tôi, số thứ tự khóa KSN (Key Sequence Number), phần đầu gốc, dữ liệu, CRC cải tiến và đánh dấu thời gian (TimeStamp) được mã hóa bằng thuật toán AES cải tiến như thể hiện trong Hình 2. Tổng 272 byte được cho qua thuật toán mã hóa AES, là mã khối đối xứng, mỗi khối có độ dài 128 bit. Khóa mã của AES có độ dài 128, 192, 256 bit. Nó là một thuật toán mã hóa đủ mạnh với các giao thức sử dụng trong mạng SCADA.

2. Thuật toán CRC cải tiến

CRC giúp cho việc xác thực dữ liệu ở cả bên gửi và bên nhận. Trong CRC cải tiến, sử dụng 4 byte. Trong CRC sử dụng một đa thức sinh để chia thông điệp để tìm ra phần dư gọi là CRC[3], [8]. Để có CRC r bit ta cần đa thức sinh phải có bậc *r*. Để tìm đa thức phần dư bên gửi bổ sung thêm *r* bit '0' vào thông điệp *m* bit và chia đa thức gồm $m + r$ bit đó cho đa thức sinh. Dữ liệu được truyền gồm *m* bit thông điệp gốc, tiếp theo là *r* bit CRC. Phương pháp CRC[6], [14] thực hiện trên thông điệp như đa thức trên trường *GF*(2). Tại bên nhận, người nhận sử dụng chung đa thức sinh đó để chia thông điệp nhận được. Nếu đa thức phần dư tìm được sau khi chia thông điệp nhận được đó bằng 0 thì thông điệp không có lỗi, ngược lại là có lỗi.

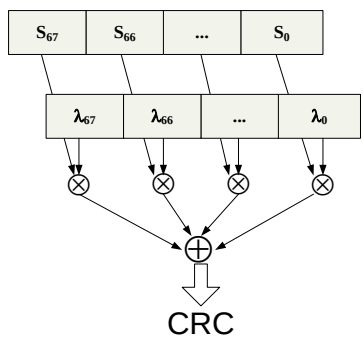
Trong giao thức MoDNP3, thông điệp ban đầu có thể biểu diễn dưới dạng đa thức: $P(x) = a_{N-1}x^{N-1} + a_{N-2}x^{N-2} + \cdots + a_1x^1 + a_0$, biểu diễn dưới dạng nhị phân là $[a_{N-1}a_{N-2} \ldots a_1a_0]$, a_{N-1} là bit có trọng số cao nhất, n_0 là bit có trọng số thấp nhất.



Hình 2. Cấu trúc bên trong của MoDNP3

Trong việc tính CRC, luôn luôn kết hợp với đa thức sinh $G(x)$ có bậc M, $G(x)$ được biểu diễn dưới dạng đa thức $G(x) = g_M x^M + g_{M-1}x^{M-1} + \cdots + g_0$, dạng nhị phân $[g_M g_{M-1} \ldots g_0]$.

Trong thuật toán CRC cải tiến, chia thông điệp ban đầu gồm N bit $[a_{N-1}a_{N-2} \ldots a_0]$ thành n đoạn, mỗi đoạn có M bit. Không mất tính tổng quát, $N = nM$, với N là số bit của thông điệp ban đầu, M là số bít của mỗi đoạn, n là số nguyên dương. Trong giao thức MoDNP3, thông điệp gồm 272 byte được chia thành 68 đoạn (S_0, S_1, … S_{67}), mỗi đoạn 4 byte, như được thể hiện trong Hình 3.



Hình 3. CRC cải tiến

Trong đó, $S_i(x) = a_{(i+1)M-1}x^{M-1} + \cdots + a_{iM}$.

Thông điệp gốc sẽ là: $P(x) = \mathrm{S}_{n-1}x^{N-1} + \mathrm{S}_{n-2}x^{N-2} + \cdots + \mathrm{S}_0$ (1). Và $S_i(x)$ là đoạn thứ i của thông điệp gốc.

Với thông điệp gốc là $P(x)$ và đa thức sinh $G(x)$, chúng ta có thể tính CRC bằng cách bổ sung M bit *0* sau bit có trọng số thấp nhất và chia thông điệp sau khi đã bổ sung cho đa thức G(x). Kết quả là: $CRC[P(x)] = (P(x)x^M)\ mod\ G(x)$ ... (2). Từ (2) và tính chất đồng dư, việc tính trên các đoạn thông điệp đã chia (1) như sau: $CRC[P(x)] = S_{n-1}(x)^{nM}\ mod\ G(x) + \cdots + S_0 x^M\ mod\ G(x)$. Ở đây, $S_i(x)\ mod\ G(x) = S_i(x)$.

$S_i(x)x^{(i+1)M}\ mod\ G(x) = S_i(x)\ mod\ G(x)x^{(i+1)M}\ mod\ G(x)$, với i = 0, 1, 2, …, n-1. Với bậc của đa thức $S_i(x)$ trong mỗi đoạn nhỏ hơn M. Xác định hệ số λ, $\lambda_i = x^{(i+1)M}$ mod G(x) với i = 0,1,2, …, n-1.

Sau đó tính CRC như sau: $CRC[P(x)] = S_{n-1} \otimes \lambda_{n-1} \oplus \ldots \oplus S_0 \otimes \lambda_0$.

Sử dụng đa thức sinh $G(x)$ để tính λ. Để tính các thành phần của λ, chúng ta có:

$\lambda_0 = x^M$ mod $G(x) = \{g_{M-1} + g_{M-2} + \ldots + g_0\}$

$\lambda_1 = x^{2M}$ mod $G(x) = \{\lambda_0 \otimes \lambda_0\}$

…..

$\lambda_n = x^{nM} \bmod G(x) = \lambda_0^n$.

Kết quả ta có ($\lambda_0, \lambda_1, \ldots, \lambda_n$), sau đó tính CRC như sau: $CRC(P(x)) = S_{n-1} \otimes \lambda_{n-1} \oplus \ldots \oplus S_0 \otimes \lambda_0$.

Phép toán $\otimes$, $\oplus$ trong các biểu thức trên là phép nhân và phép cộng trên trường $GF(2)$ (Galois Field).

Thuật toán CRC cải tiến được mô tả như sau:

B1. Thông điệp N bit, chia thành n đoạn $[S_{n-1}S_{n-2}\ldots S_1S_0]$ và mỗi đoạn có kích thước M bit ($N = nM$).

B2. Khởi tạo đa thức sinh $G(x)$ với bậc M đồng thời tính các hệ số λ (như đã trình bày ở trên).

B3. Nhân n-cặp trên trường $GF(2)$ đồng thời và sau đó thực hiện phép XOR thu được CRC.

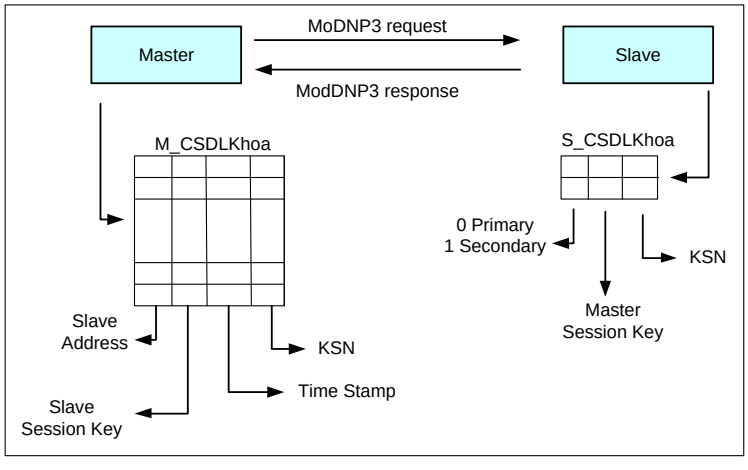
Thông điệp ban đầu sẽ được chia thành 68 đoạn, mỗi đoạn 4 byte. Những đoạn này sẽ sử dụng thuật toán CRC để tạo ra xác thực thông điệp. Trong Hình 3 mô tả CRC cải tiến. Trong thuật toán CRC được sử dụng để đảm bảo tính toàn vẹn của thông điệp trong giao thức SCADA. Ở đây 4 byte được sử dụng trong CRC trong 20 byte và những byte còn lại phục vụ trong tương lai. Do đó giao thức này sẽ được xác thực và toàn vẹn bằng cách sử dụng thuật toán mã AES cải tiến và CRC cải tiến như đã trình bày ở trên. Với giải pháp này chúng tôi sắp xếp lại các byte của giao thức DNP3 để đảm bảo tính bí mật, toàn vẹn và xác thực. Trong giao thức này chúng tôi đã thay đổi một số cách sắp xếp thông tin trong giao thức để đảm bảo tính an toàn của giao thức. Phần mở đầu LH ban đầu và dữ liệu Payload được mã hóa bằng thuật toán AES để đảm bảo tính bí mật của thông điệp. 4 byte phần CRC đề xuất của chúng tôi được sử dụng để xác thực thông điệp. 4 byte đánh dấu thời gian được sử dụng để chống tấn công phát lại trong SCADA.

3. Đánh dấu thời gian

Đánh dấu thời gian được bên nhận sử dụng kết hợp với khe thời gian nội bộ để kiểm tra tính mới của gói tin vừa nhận. Giải pháp này sử dụng một số tuần tự 4 byte đơn giản và được cung cấp cho tất cả các thiết bị DNP3 với những khe thời gian có kích thước hữu hạn để xác minh tính mới của gói tin. Do đó, giải pháp này không những thuận tiện mà còn hoàn toàn an toàn. Việc triển khai thực tế sử dụng các đánh dấu thời gian NTP (Network Time Protocol)[7] phù hợp trong việc đánh giá tính mới của gói tin với độ chính xác cao. Tất nhiên, việc thực hiện các đánh dấu thời gian NTP yêu cầu một máy chủ NTP trong kiến trúc SCADA để cung cấp một xung nhịp đồng bộ đáng tin cậy cho tất cả các thiết bị tham gia truyền thông. Tại bên nhận, sau khi giải mã thông điệp thì thiết bị Slave phải đối chiếu đánh dấu thời gian này với thời gian trong khóa phiên (trong phần 4.), nếu hai thời gian này khớp nhau thì mới tiếp tục thực hiện hành động trong thông điệp, ngược lại thì Slave bỏ qua hành động yêu cầu này vì có thể là một tấn công phát lại.

4. Quản lý khóa trong MoDNP3

Việc quản lý khóa trong MoDNP cần đơn giản phù hợp với môi trường mạng SCADA. Được thực hiện trong quá trình cấu hình thiết bị Primary Master, Secondary Master và các thiết bị Slave để thiết lập kết nối khởi tạo giữa chúng;



Hình 4. Truyền thông trong SCADA/MoDNP3

Thiết bị Master tạo và quản lý một cơ sở dữ liệu khóa an toàn "M_CSDLKhoa" cho các khóa phiên dùng chung với các Slave (Hình 4). Cơ sở dữ liệu này bao gồm 4 trường: Địa chỉ Slave được sử dụng như một chỉ số khóa, khóa phiên dùng chung, đánh dấu thời gian để giới hạn việc sử dụng khóa dùng chung trong thời gian định trước và số thứ tự khóa. Thiết bị Master gọi hàm "M_TaoKhoa" để tạo ra một khóa phiên duy nhất khi mà khóa phiên cũ đã hết hạn. Hàm "M_BosungKhoa" để thêm một khóa phiên mới vào cơ sở dữ liệu khóa.

Thiết bị Slave phải duy trì hai khóa phiên, một khóa để truyền thông với thiết bị Primary Master, khóa còn lại để truyền thông với thiết bị Secondary Master (Hình 4). Cơ sở dữ liệu này có 3 trường và 2 bản ghi: (0, Khóa phiên thiết bị Master chính (Primary Master Session Key) và 1, Khóa phiên thiết bị Master thứ hai (Secondary Master Session Key), Số thứ tự khóa (Key Sequence Number)). Hàm "S_ BosungKhoa" để cập nhật khóa phiên mới vào cơ sở dữ liệu khóa và hàm "S_BosungSTTKhoa" để cập nhật số thứ tự khóa KSN vào cơ sở dữ liệu khóa.

IV. KẾT LUẬN

Khi hệ thống mạng điều hành giám sát công nghiệp bị xâm nhập trái phép, kẻ tấn công có thể từ đó phá hủy những công trình quan trọng của quốc gia. Những hiểm họa từ những mạng này là rất lớn, nó ảnh hưởng đến an ninh của đất nước, ảnh hưởng tới tính mạng của người dân. Trong bài báo này, chúng tôi nghiên cứu vấn đề an toàn giao thức truyền thông trong mạng điều hành giám sát công nghiệp. Để bảo vệ các mạng SCADA, chúng tôi hướng tới những giao thức mà khi xây dựng chúng ban đầu chưa có những thuộc tính an toàn. Với mục đích thay đổi cấu trúc bên trong của các giao thức đó để tạo ra giao thức toàn vẹn, xác thực hơn, chống tấn công phát lại. Trong cấu trúc giao thức đề xuất, sử dụng hai thuật toán được để cải tiến khả năng an toàn và toàn vẹn của phần Payload. Chúng tôi đã sử dụng 4 byte cho CRC cải tiến, 4 byte đánh dấu thời gian và còn lại 12 byte trong cấu trúc để cho những cải tiến trong tương lai. Mục đích là tăng tính an toàn của giao thức trước những hiểm họa trên mạng điều hành giám sát công nghiệp.

TÀI LIỆU THAM KHẢO

[1] Anupam Saxena, Om Pal, Zia Saquib, Dhiren Patel, "Customized PKI for SCADA Systems Network", Int. J. of Advanced Networking and Applications. 282. Volume: 01, Issue: 05, Pages: 282-289 , 2010.

[2] Athar Mahboob, Junaid Zubairi, "Intrusion Avoidance for SCADA Security in Industrial Plants", Collaborative Technologies and Systems, 2010.

[3] David C. Feldmeier, "Fast Software Implementation of Error Detection code", IEEE/ACM Transactions on networking, December 1995.

[4] Distributed Network Protocol (DNP3), IEEE Standard for Electric Power Systems Communications 2012.

[5] DNP3 Application Note AN2003-001, http://www.dnp.org.

[6] D. V. Sarwate, "Computation of Cyclic Redundancy Checks via Table Lookup", Communications of the ACM, vol. 31, no. 8 1988.

[7] D. L. Mills. Internet time synchronization: The network time protocol. IEEE Transactions on Communications, 39(10):1482–1493, October 1991.

[8] H. Michael Ji, Earl Killian, "Fast Parallel CRC Algorithm and Implementation on a Configurable Processor", IEEE 2002 vol3.

[9] M. Bellare, P. Rogaway, "Entity authentication and Key distribution", in Advances in cryptology-CRYPTO 93, Leture notes in computer Science, Springer 1994.

[10] Munir Majdalawieh, Francesco Parisi- Presicce, Duminda Wijesekera (2006), "DNPSec Distributed Network Protocol Version 3 (DNP3)", Security Framework Advances in Computer, Information and Systems Sciences and Engineering 2006.

[11] P. Rogaway, M. Bellare, J. Black, "OCB A block –cipher mode of operation for efficient authenticated", ACM Trans. Inf. Syst. Secure 2006.

[12] Robert Dawson, "Secure Communication for Critical Infrastructure Control System", University of Queensland 1997.

[13] Safeguarding IEDs, Substations, and SCADA Systems Against Electronic Intrusions by Paul Oman, Edmund O. Schweitzer, III, and Jeff Roberts - Schweitzer Engineering Laboratories, Inc. Pullman, WA USA.

[14] Sanjay M.Joshi, Pradeep K. Dubey, Marc A. Kalpan, "A new parallel algorithm for CRC Generation, Communication", ICC IEEE International Conference 2000.

[15] S. Bhagaria, S B Prabhakar, Z Saquib, "Flexi-DNP3: Flexible distributed network protocol version 3(DNP3) for SCADA security",Recent Trends in Information System 2011.

[16] S Saiwan, P Jain, Z Saquib, D Patel, "Cryptography key Management for SCADA System An Architectural Framework", Advances in Computing Control, & Telecommunication 2011.

[17] V. Sumathy & C. Navaneethan, "Enhanced algorithm for strong encryption", International Journal of Advances in Engineering & Technology, Sept 2012.

[18] Zia Saquib, D. Patel, R. Rajrajan, "A configurable and efficient key management scheme for SCADA" International Journal of Research and Reviews 2011.

A NEW METHOD FOR ENHANCING SECURITY ON NETWORKED INDUSTRIAL SUPERVISORY AND CONTROL SYSTEM

Nguyen Dao Truong, Nguyen Doan Cuong, Nguyen Duc Tam

ABSTRACT*— This paper investigates security issues of SCADA communication protocol. SCADA stands for Supervisory Control and Data Acquisition, a communication technology which collects data from distant facilities and sends control signals to actuators. Due to the need to connect SCADA systems with corporate networks and the Internet, so SCADA components are considered to be profoundly privileged targets for cyber attacks through which hackers can easily demolish the nation's critical infrastructure and economy. In order to protect the SCADA networks, we focus on the protocols as they were not designed with inherent security features. Security system through protocol hardening is the main focus of this paper. The goal is to modify the structure of such protocols to provide more integrity and authentication. In the proposed structure, two algorithms are used to enhance the security and integrity of the payload and using timestamp againt replay on the network.*