Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

A Design and Implementation of Cryptographic Processor DNAES Flexibly Internet of Things Network

Sun-Yeob Kim*

Department of Information & Communication Engineering, Namseoul University

ABSTRACT

With the rapid development of the Internet environment, the importance of security for terminals of wireless networks is increasing. In the case of a sensor node, which is often used as a wireless network terminal in the Internet environment, a resource environment such as a memory is poor. Therefore, there is a problem that a memory-intensive security algorithm can not be used. In this paper, we propose the DNAES algorithm considering the security problem when the number of sensors increases because it enables the poor resource environment, low power and high speed processing of sensor nodes. The proposed DNAES encryption algorithm adopts the DN-R technique which reduces the load of important nodes in the wireless network environment. Implementation of the DNAES encryption algorithm was performed using topology of verilog-HDL. The tool used for circuit synthesis was Synopsys Design Analyzer and QUARTUS 12.0. The tools used in the simulation were Synopsys VHDL Debugger, ModelSim 5.8C. Simulation results show that the proposed DNAES encryption algorithm has a 120% increase in throughput compared to the conventional AES algorithm. Therefore, it is considered that the DNAES proposed in this paper is sufficient for the security of the sensor node in the IOT environment.

KEYWORDS: AES, Condition State, High speed, Network management, Sensor network

ARTICLE INFO: Received 4 August 2017, Revised 16 August 2017, Accepted 16 August 2017.

*Corresponding author is with the Department of Information & Communication Engineering, Namseoul University, 91 Daehak-ro Seounghwan-eup Seobuk-gu Cheonan-city Chungnam, 31020, KOREA.

E-mail address: sykim0599@jeongbo.ac.kr

1. 서 론

현재 우리사회는 빠르게 유비쿼터스 환경으로 진입하고 있으며 사물인터넷 시스템도 급격하게 발전되고 있다. 이러한 환경에서 무선 센서 네트워크는 실제의 물리적인 정보를 실시간으로 모니터링하기 위한 수많은 센서 노드들이 사용되고 있다. 이에 따라 센서 노드들의 보안의 필요성이 증대되고 있다[1-3]..

Rijndael 이 제안하여 표준화된 AES 블록알고리즘을 이용하여 센서노드들의 보안성을 향상 시킬 수 있을 것으로 기대하였지만, 센서 노드들이 갖는 열악한 메모리 용량등의 이유로 인하여 AES 알고리즘을 센서 노드에 적용할 수 없다는 문제점이 있다. 그러므로 본 논문에서는 사물인터넷망의 말단을 구성하는 다양한 센서 노드의 보안성을 향상시키기 위하여 기존의 Rijndael이 제안한 블록 알고리즘을 개선한 DNAES (Distributed Network AES)를 제안하였다.

이를 통해 기존의 블록 알고리즘에 비해 처리속도를 보다 향상 시켰으며 RFID와 같은 저용량의 시스템에서 사용할 수 있도록 하여 사물 인터넷망의 단말에서 사용되는 다양한 센서 노드의 보안성을 증대시킬 수 있다.

블록보안 알고리즘은 기본적으로 대칭형 암호알고리즘이지만 본 논문에서 제안한 DNAES는 비대칭형 암호알고리즘의 장점을 포함하도록 하기 위해 분산처리망 기능을 추가하였으며, 그 성능을 다른 암호알고리즘 및 시스템과 비교하였다[4-7].

2. DNAES 암호 알고리즘

2.1 시스템 구조

현재와 같은 네트워크 시대에서는 다양한 불법적인 해킹에 대비하여야 하며, 사물인터넷망의 단말에 위치하는 다양한 센서 노드들 또한 보안성을 증대하여야 한다. 보안증대방안으로는 다양한 방법들에 제안되고 있으나 센서노드들의 자원 제한으로 인하여 암호알고리즘을 그대로 적용할 수 없다.

이에 본 논문에서는 센서노드들이 갖는 열악한 자원환경, 저전력 및 고속처리를 가능하도록 하며, 센서들의 수가 증가했을 때도 보안문제등을 고려하여 DNAES 알고리즘을 제안하였다.

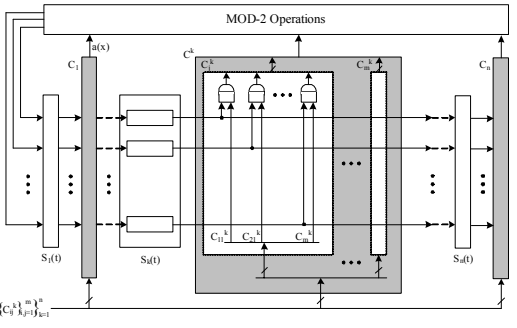

그림 1. 2DSRS 구성
Figure 1. 2DSRS configuration

<그림 1>에 나타난 2DSRS에 대하여 각 이벤트 시간마다, $t \in Z^+$인 상태에서 mn 차원 열 벡터 (column vector) $s(t)$는 식 (1)과 같이 표현된다[4].

$$s(t) = [s_1(t)^T s_2(t)^T \dots s_n(t)^T]^T \quad (1)$$
$$= [s_1^1(t) \dots s_m^1(t) \dots s_1^n(t) \dots s_m^n(t)]^T$$

이때 열 서브벡터 $\{ \boldsymbol{d_j} \}_{j=1}^{n}$는 식 (2)와 같이 표현된다.

$$\boldsymbol{d} = [\boldsymbol{d_1^T}\, \boldsymbol{d_2^T} \dots \boldsymbol{d_n^T}]^T = [d_1^1 \dots d_m^1 \dots d_1^n \dots d_m^n]^T \quad (2)$$

또한 $mn \times mn$ 상태 변환 행렬 Q는 n^2 $m \times m$

귀환행렬 $\{ Q_{ij} \}_{i,j=1}^{n}$으로 구성되어 있다. 만약 에 빈트 시간이 0인 경우, s함수의 다음 상태는 식 (3)과 같이 된다[5].

$$s(t+1) = \begin{bmatrix} Q_{11} & Q_{12} & \cdots & \cdots & Q_{1n} \\ Q_{21} & Q_{22} & \cdots & \cdots & Q_{2n} \\ Q_{31} & Q_{32} & \cdots & \cdots & Q_{3n} \\ \cdots & \cdots & & & \\ Q_{(n-1)1} & & & & \\ Q_{n1} & Q_{n2} & \cdots & & Q_{nn} \end{bmatrix} s(t) = Qs(t) \quad (3)$$

이러한 특징을 이용하여, AES의 iteration 동작 전에 각 상태 변화 시기에 서브벡터 s_i 값을 인가하여 센서 노드의 ID로 s_i를 할당하면 노드들의 숫자와 관계없이 하나의 PN 구조안에 모든 노드들을 포함하며 안전한 망을 구축하게 된다[6].

이와 같은 PRN 분산처리를 수행하기 위하여 사용되는 원시 다항식은 식 (4)와 같이 표현된다[6].

$$PRN_i = x^{16} + x^{13} + x^{12} + x^{11} + x^7 + x^6 + x^5 + x^4 + 1 \quad (4)$$
$$PRN_j = x^{16} + x^{14} + x^{10} + x^9 + x^8 + x^6 + 1$$

DNAES 암호알고리즘은 암호화 및 복호화를 동시에 수행하게 되는데, 둘 중 어떤 작업을 수행할지는 제어신호에 의해 결정된다.

각 라운드마다 그림 2에서 보이는 과정을 거치게되고 데이터 값들은 DN-PRN과 각 라운드에 의하여 별개로 동작하게 된다. 그러므로 라운드가 진행될 때 마다 독립적인 처리를 수행하게 된다. 이러한 네 가지 변환(DN-R : DN PRNG-Round)에 대한 처리는 식 (5)와 같다.

$$\begin{aligned} &DN-R_{(n)-round} \\ &\leqq Inv/SubByte(i)_n + Inv/ShiftDiagonal(i)_n + \\ &\quad Inv/MixColumn(i)_n + AddRoundKey(i)_n \\ &DN-R_{(n-1)-round} \\ &\leqq Inv/SubByte(j)_{n-1} + Inv/ShiftDiagonal(j)_{n-1} + \\ &\quad Inv/MixColumn(j)_{n-1} + AddRoundKey(j)_{n-1} \end{aligned} \quad (5)$$

표준 블록 알고리즘인 AES는 데이터와 키의 길이를 다양한 비트로 변화시키는데, 변화되는 비트에 따라 라운드 수를 결정한다. 따라서 표준 블록 알고리즘인 AES는 데이터 블록의 비트 수에 따라 라운드 수를 결정하므로 데이터 블록 비트 수를 알게 될 경우는 라운드 수를 알 수 있다. 따라서 해킹이 가능해진다.

그러나 본 논문에서 제안한 DNAES는 라운드의 수에 따라 데이터의 내용이 변화하기 때문에 고정된 블록 및 키 크기를 갖는다 할지라도 라운드의 수를 파악 할 수 없다.

DN-R 변환의 첫 번째인 Inv/SubByte 변환은 독립적으로 존재하는 바이트들을 비선형적으로 변형하여 비선형 변형된 바이트 집합을 생성하게 된다. S-box는 Inv/SubByte 변환에 이용되며 역변환이 가능하다. 식 (6)과 같은 affine 변환을 GF(2^8)에 대입가능한 비선형 변환 가능 함수들의 집합들로 구성되어있다.

$$\begin{aligned} [ab]_i = [ab]_i \bigoplus [ab]_{(i+4)\bmod 8} \bigoplus [ab]_{(i+5)\bmod 8} \bigoplus \\ [ab]_{(i+6)\bmod 8} \bigoplus [ab]_{(i+7)\bmod 8} \bigoplus [ac]_i \end{aligned} \quad (6)$$

여기에서 ab는 DN-PRNG의 산출된 데이터 중에서 내부 데이터를 변환해 주는 부분인 s 부분의 비트 블록을 의미하며 $0 \le i \le 7$일 때 $[ab]_i$는 바이트들의 i 번째 해당 비트이고 $[ac]_i$는 특정 ac 바이트 블록의 i 번째 비트를 의미한다.

Inv/ShiftDiagonal 변환은 DN-R 변환의 두 번째 변환으로 데이터의 행 과 열을 기준으로 대각선 방향으로 이루어지며 식 (7)과 같이 표현된다.

$$\begin{aligned} S_a'(03,12,21,30) &= S_a(00,11,22,33) \\ S_b'(13,22,31,00) &= S_b(01,12,23,30) \\ S_c'(23,32,01,10) &= S_c(02,13,20,31) \\ S_d'(33,02,11,20) &= S_d(03,10,21,32) \end{aligned} \quad (7)$$

식 (7)에 표현된 바와 같이 각 데이터 배열에 대하여 대각으로 행과 열이 변환되기 때문에 역방향으로 치환도 가능하며 고속의 연산이 가능하고 랜덤성을 갖기 때문에 보안성도 향상된다.

DN-R 변환의 세 번째인 Inv/MixColumn 변환은 고정된 다항식인 $a(x)$를 곱하기 때문에 새로운 배열이 생성된다.

이 때 식 (7)의 변환식은 곱셈연산을 통해 산출되게 되고, 변환이 완료된 함수 $s'(x)$는 변환되기 전 함수인 $s(x)$에 대하여 $a(x)$를 곱한 모습으로 나타난다. 식 (7)에 나타난 $s'(x) = a(x) \otimes s(x)$ 곱셈모양의 식은 식 (8)의 행렬 식으로 표현할 수 있다.

$$\begin{bmatrix} s'_0 \\ s'_1 \\ s'_2 \\ s'_3 \end{bmatrix} = \begin{bmatrix} 02 & 01 & 03 & 03 \\ 01 & 03 & 03 & 02 \\ 03 & 03 & 02 & 01 \\ 03 & 02 & 01 & 03 \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix} \quad (8)$$

Inv/MixColumn 변환을 식 (8)을 통하여 수행하면 식 (9)와 같이 x축, y축을 기준으로 $y = x$에 해당하는 대각변환만을 수행하게 된다. 즉, DNAES 암호알고리즘의 대각변환을 수행함에 있어 식 (9)와 같이 대각변환이 구별되어진다.

$$\begin{aligned} y &= -x; \quad Inv/Shift\,Diagonal \\ y &= x; \quad Inv/Mix\,Column \end{aligned} \quad (9)$$

식 (9)에 나타난 바와 같이 전체 대각 변환을 수행하기 위해서는 x방향과 $-x$방향으로 대각 변환을 수행하여야 한다. 식 (9)와 같은 대각변환을 통해 기존 암호알고리즘이 갖는 곱셈연산을 수행해야하는 번거로움과 같은 단점을 줄일 수 있고, 또한 역방향으로 대각 변환을 수행하면 비도가 향상된다[9-10].

DN-R 변환의 마지막 변환인 AddRoundKey 변환은 라운드 키와 DN-PRNG을 이진합 연산을 수행한다. 각 라운드마다 사용되는 키는 키 스케쥴에서 천이상태가 출현할 때마다 별개의 독립된 값을 생성하게 되며, 생선된 값들을 이용하여 식 (10)과 같은 연산을 수행한다.

$$\begin{aligned} &[s'_0, s'_1, s'_2, s'_3] \\ &= [s_0, s_1, s_2, s_3] \bigoplus [PN_{round}] \end{aligned} \quad (10)$$

여기에서 PN_{round}는 DN-PRNG에 대한 라운드 수행 범위를 의미한다. AddRoundKey 변환은 라운드가 수행되는 범위에 따라 연산 횟수는 달라진다. 그렇지만 계산 양은 동일하기 때문에 단순 더하기 기능만을 수행하게 된다[7].

3. DNAES 암호시스템 설계 및 시뮬레이션

본 논문에서 제안된 DNAES 알고리즘의 구현은 verilog-HDL를 사용하였으며 Top-down 형태로 수행하였다. 회로합성에 사용한 tool은 Synopsys Design Analyser와 QUARTUS 12.0을 이용하였다. 또한 시뮬레이션에 사용된 툴은 Synopsys VHDL Debegger, ModelSim 5.8C를 사용하였다.

DN-PRNG 처리부는 제안된 DNAES 암호알고리즘의 핵심부분으로서 실제적인 DNAES 암호알고리즘을 수행하게 되는 부분이다. DN-R 블록은 입력 데이터들과 DNAES 암호알고리즘에서 제시되는 상태조건을 이용하여 조건상태를 생성하게 되며, 생성된 배열들인 $s(t)$는 바이트 치환을 수행하게 된다[11-13].

DNAES 암호시스템 내부의 DN-R 블록은 대각변환이 $y = x, y = -x$방향으로 동시에 수행되는 기능을 수행한다. DN-R 블록은 그림 2에 표현된 블록을 따라 순차적 기능을 수행한다.

AddRoundKey 기능블록은 조건 상태에 따라 기

능을 수행하는 블록이고, 데이터를 바이트로 변환하는 기능은 Inv/SubByte 블록에서 수행된다.

대각변환은 Inv/ShiftDiagonal 블록에서 수행되며 마지막으로 Inv/MixColumn 블록에서 대각변환을 다시 한 번 수행한다[14-15].

DN-R은 SEED를 통해 생성한 랜덤 키 정보를 암호/복호모드에 따라 생성한다.

SEED 포맷과정을 거친 키 정보는 DN-R 블록의 출력이 AddRoundKey 블록의 입력으로 사용된다.

본 논문에서 제안된 DNAES 암호시스템은 입력되는 평문이 128 비트인 경우 암호문도 128 비트를 생성되며, 입력되는 데이터가 평문인 경우 암호문, 입력되는 데이터가 암호문인 경우 암호문을 생성하게 된다.

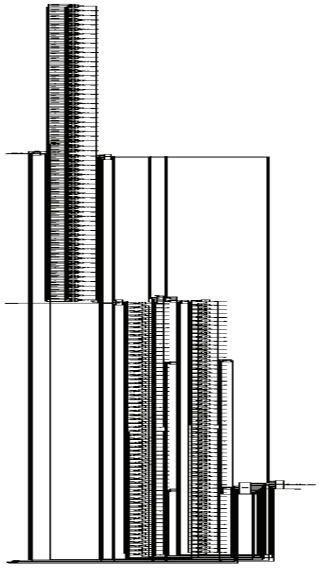

그림 2. DNAES 전체 합성도
Figure. 2 Overall Synthesis of DNAES

DNAES에서는 보다 효과적인 암호화를 위해 키 정보는 암호와화 복호화를 수행하는데는 사용하지 않고 새로운 키 정보를 생성하는 도구로만 사용한다.

<그림 2>는 DNAES 암호시스템의 전체 회로합성도이다. DN-R 블록이 포함된 DNAES 암호시스템은 2DSRS의 범위에 따라 독립적인 의사잡음을 출력하여 암호화를 수행하게 된다.

<표 1>은 기존 대칭형/비대칭형 암호시스템과 제안된 AES-DN 암호시스템을 상호 비교 분석한 표이다.

표 1. DNAES 성능분석표
Table 1. Performance analysis table of DNAES

@50MHz	구 조	라운드수	키 길이 (bits)	데이터 길이 (bits)	처리율 (Mbps)
SEED	Feistel	16	128	128	313.7
AES	SPN	10	128	128/192/256	387.9
Serpent	SPN	32	128	128/192/256	197.3
3DES	Feistel	48	112/168	64	15.6
DNAES	Feistel & SPN	10	128	128/192/256	472.0
RSA	R-L Arch.		128	128	96.0

4. 결 론

사물인터넷의 발전으로 인하여 네트워크 단말에 위치하는 센서노드에 대한 보안이 증대되고 있는 상황에서 네트워크 단말에 위치하는 다양한 센서노드들의 경우 아주 작은 양의 메모리를 갖는 등의 제약 조건이 존재한다. 따라서 급증하는 해킹을 네트워크의 종단에서 차단할 수 있는 암호알고리즘이 필요하다.

본 논문에서 제안된 DNAES 암호시스템은 암/복호화를 수행할 때 필요한 요소는 입력되는 자체 정보뿐이다. 암호알고리즘에서 가장 중요한 요소인 연산시간 및 비도는 제안된 암호알고리즘의 경우 연산을 동시에 수행하기 때문에 기존의 대칭형 블록암호 알고리즘에 비해 120% 증가를 가져왔다.

또한 가장 중요한 분산처리가 가능한 DN 기법을 포함함으로서 PRNG의 성능을 이용하여 비대칭형과 같은 특징을 가질 수 있도록 하였다. 이러한 특징은 분산되며 노드 부하가 큰 산재된 네트워크인 센서 노드환경에 적합하여 복잡한 비대칭형 암호시스템을 사용치 않으면서도 대칭형 특징을 가질 수 있도록 하였다.

그러므로 제안된 새로운 DNAES 암호알고리즘은 센서 노드등과 같은 자원 조건이 열악한 환경을 극복하기에 적합함과 동시에 비대칭형 암호시스템의 대안적인 기능을 수행할 수 있는 암호알고리즘으로 판단된다.

References

[1] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, and D. Whiting, *Improved cryptanalysis of Rijndael*, Seventh Fast Software Encryption Workshop, Springer-Verlag, 2000.

[2] NIST, *AES Algorithm (Rijndael) Information*, http://csrc.nist.gov/archive/aes/rijndael, Jan. 2001.

[3] I. Damaj, M. Itani, H. Diab, *Serpent cryptography on static and dynamic reconfigurable hardware*, aiccsa, pp.680-684, IEEE International Conference on Computer Systems and Applications, 2006.

[4] W. C. Y. Lee, Overview of Cellular *CDMA, IEEE Trans.* Vehicular Tech., Vol. 40, pp. 291-302, May 1991.

[5] Mitsuru Matsui, *Linear cryptanalysis method for DES cipher*, In Tor Helleseth, editor, Advances in Cryptology-Eurocrypt'93, Vol. 765 of Leture Notes in Computer Science, Springer-Verlag, Berlin, pp. 386-397, 1994

[6] Microelectronic Systems Laboratory, *Implementation of DES algorithm using FPGA technology*, http://www.alagger.com/des-vhdl/ report.pdf, 2002.

[7] NIST, *Draft FIPS for the AES*, http://csrc.nist.gov/publications/drafts.html, Feb. 2001.

[8] R. D. Silverman, *A cost-based Security analysis of symmetric asymmetric Key lengths*, Bulletin 13, RSA Lab., 2000.

[9] Chang-Whan Kim, *Ubiquitous environments in the information protection technology*, http://www.eic.re.kr, Nov. 2008.

[10] *DES and 3DES cores*, http://www.heliontech.com/des.htm, Jan 2014.

[11] *SEED block cryptographic algorithm*, https://www.kisa.or.kr/public/library/report_View.jsp?regno=011433&pageIndex=1&searchType=&searchKeyword=seed, Nov. 2006

[12] Kaisa Nyberg and Lars R. Knudsen, *Provable security against a differential attack*, Journal of Cryptology, Vol. 8, No. 1, pp. 27-37, 1995.

[13] R. D. Silverman, *A cost-based security analysis of symmetric asymmetric key lengths*, Bulletin 13, RSA Lab., 2000.

[14] NIST, Draft FIPS for the AES, http://csrc.nist.gov/publications/drafts.html, Feb. 2001.

[15] R. D. Silverman, A cost-based Security analysis of symmetric asymmetric Key lengths, Bulletin 13, RSA Lab., 2000.

사물인터넷 네트워크 환경에 적용가능한 암호프로세서 DNAES의 설계 및 구현

김선엽

남서울대학교 정보통신공학과

요 약

사물 인터넷 환경의 급속한 발전에 의해서 무선네트워크의 단말에 대한 보안의 중요성이 증대되고 있

다. 사물인터넷 환경의 무선 네트워크 단말로 많이 사용되는 센서 노드의 경우에는 메모리등의 자원환경이 열악하다. 따라서 메모리를 많이 사용하는 보안알고리즘을 사용할 수 없다는 문제점을 지니고 있다. 이에 본 논문에서는 센서노드들이 갖는 열악한 자원환경, 저전력 및 고속처리를 가능하도록 하며, 센서들의 수가 증가했을 때도 보안문제등을 고려하여 DNAES 알고리즘을 제안하였다. 제안된 DNAES 암호알고리즘은 무선 네트워크 환경에서 중요한 노드의 부하를 줄여주는 DN-R 기법을 채용하였다. DNAES 암호알고리즘의 구현은 verilog-HDL를 사용하였으며 Top-down 형태로 수행하였다. 회로합성에 사용한 tool은 Synopsys Design Analyser와 QUARTUS 12.0을 이용하였다. 또한 시뮬레이션에 사용된 툴은 Synopsys VHDL Debegger, ModelSim 5.8C를 사용하였다. 시뮬레이션 결과, 제안된 DNAES 암호알고리즘은 기존 AES에 비해 120%의 처리율 증가를 보였다. 따라서 현재 급증하는 사물인터넷 환경의 센서노드의 보안을 위한 알고리즘으로 충분할 것으로 판단된다.

감사의 글

이 논문은 2016년도 남서울대학교 학술연구비 지원에 의해 연구되었음.

Sun-Yeob Kim received the bachelor's degree in the Department of Electronic Engineering from the Wonkwang University in 1995. He received the M.S. degree and the Ph.D. degree in the Department of Electronic Engineering from Wonkwang University in 1995 and 2001, respectively. From 2001 to 2006, he was a researcher at HanKook Precision & Electronics Co,. LTD. He has been a professor in the Department of Computer Engineering at JiSik University since 2006. His current research interests include embedded system, micro controller systems, cryptographic algoritm. He is a life member of the KKITS.
E-mail address: sykim0599@nsu.ac.kr