JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 18, No. 3 : 586~594 Mar. 2014

센서 네트워크 상에서의 저전력 보안 수중 통신을 위한 동작 전압 스케일 기반 암호화에 대한 연구

서화정 · 김호원*

On Dynamic Voltage Scale based Protocol for Low Power Underwater Secure Communication on Sensor Network

Hwa-jeong Seo · Ho-won Kim*

Department of Computer Engineering, Pusan National University, Pusan, Korea

요 약

수중 통신 상에서 가장 중요한 요소는 한정된 전원을 보다 효율적으로 소모하여 운영 가능 시간을 최대화하는데 있다. 보다 효율적인 전압 소모를 위해 적용 가능한 기법으로는 동적 전압 스케일 기법이 있다. 해당 기법은 평상시에는 낮은 주파수로 동작하여 대기 전력을 최소화하며 복잡한 연산을 수행하는 경우에는 빠른 주파수로 계산함으로써 전체 소모되는 전력량을 줄인다. 복잡한 암호화 연산의 경우 빠른 주파수로 연산을 하는 것이 보다 효율적이다. 본 논문에서는 다양한 센서 상에서의 암호화 기법에 동적 전압 스케일 기법을 적용한 결과를 보여 줌으로써 수중 통신 상에서 적합한 저전력 암호화 방안에 대해 살펴본다.

ABSTRACT

Maximizing the operating time by reducing the power consumption is important factor to operate sensor network under water networks. For efficient power consumption, dynamic voltage scaling method is available. This method operates low frequency when there is no workload. In case of abundant workload, high frequency operation completes hard work within short time, reducing power consumption. For this reason, complex cryptography should be computed in high frequency. In this paper, we apply dynamic voltage scaling method to cryptography and show performance evaluation. With this result, we can reduce power consumption for cryptography in under water communication.

키워드 : 수중 통신, 저전력, 보안통신, 동적 전압 스케일링, 임베디드 시스템

Key word : Underwater Communication, Low Power, Dynamic Voltage Scaling, Embedded System

접수일자 : 2013. 12. 02 심사완료일자 : 2013. 12. 27 게재확정일자 : 2014. 01. 14

* **Corresponding Author** Ho-won Kim(howonkim@pusan.ac.kr, Tel:+82-51-510-3927)
Department of Computer Engineering Pusan National University, Pusan, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2014.18.3.586 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

수중 통신 기술은 오염도 모니터링, 심해 조사 및 탐험, 수중 장비 점검과 해양 플랜트와 같은 다양한 기술에 사용되고 있다. 하지만 수중 센서 네트워크를 실용화하기에는 많은 어려움이 따른다. 먼저 전원에 대한 접근이 용이하지 않으며 잦은 전송 오류로 인해 재전송이 자주 발생하게 된다[1]. 또한 무선으로 통신되는 센서 네트워크는 악의적인 노드의 공격에 취약하다. 따라서 수중에서 동작하는 센서 네트워크의 전원에 대한 관리는 지상의 센서 보다 최적화되어야 한다. 전원을 효율적으로 사용하는 방안으로는 Dynamic Voltage Scaling(DVS) 기법이 적합하다[18]. 해당 기법은 대기와 동작 시의 주파수를 동적으로 조절하여 보다 효율적인 전원 소모가 가능하도록 한다.

본 논문에서는 해양 통신 상에서 전원이 부족한 임베디드 장비의 전원을 보다 효율적으로 사용하기 위해 DVS를 암호화 모듈에 적용한 실험결과를 제시한다. 해당 실험은 대표적인 8- 16- 32-비트 임베디드 장비인 ATxmega128A1, MSP430F5529 그리고 PXA271 상에서 대표적인 암호화 모듈인 대칭키, 공개키 암호 그리고 해시에 대해 확인되었으며 해당 결과를 통해 많은 전원이 절약될 수 있음을 확인할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 DVS기법과 암호화 알고리즘, 참고한 암호화 라이브러리 그리고 타겟 보드와 개발 환경을 나타낸다. 3장에서는 제안하는 프로토콜을 나타내며 4장에서는 이에 대한 성능을 평가한다. 5장에서는 해당 논문의 결론을 내린다.

Ⅱ. 관련연구

2.1. 센서 네트워크 상에서의 DVS 기술

센서 네트워크 상에서의 전원을 효율적으로 사용하기 위해서는 MAC 프로토콜[2-4]을 효율적으로 구성하는 기법 혹은 DVS를 통해 동작 주파수를 조절하여 전원을 효율적으로 사용할 수 있다. MAC 프로토콜의 경우 네트워크 단에서의 프로토콜로써 암호화구현과는 거리가 있다. 따라서 DVS를 통해 암호화 과정을 보다 효율적으로 수행하는 방안에 대하여 살펴본다. 가장 먼저 암호화에 대한 DVS가 수행된 논문이다[17]. 여기서는 내장형 컨버터를 이용하여 보다 효율적인 DVS의 구현 및 암호화가 가능함을 보여 주었다. 하지만 보다 실용적인 측면에서 다양한 임베디드 장비와 암호화 프로토콜 상에서의 DVS 구현 결과는 아직까지 보고되지 않았다. 따라서 본 논문에서는 해당 결과에 대한 조사 형식의 결과를 제시하며 이는 저전력으로 전원을 소모하는 암호화가 DVS를 통해 가능함을 확인할 수 있다.

2.2. 암호화 알고리즘

본 장에서는 현재 사용 중인 복호 불가능한 암호화 알고리즘 SHA1, SHA-256과 복호 가능한 대칭키 알고리즘인 AES 그리고 SHA와 함께 전자서명에서 쓰이는 비대칭키 알고리즘인 ECC에 대해 살펴본다.

2.2.1. Cryptographic Hash Function(SHA1, SHA256)

Cryptographic Hash Function은 해시 함수의 일종으로 해시 출력값과 원래의 입력값 사이의 상관 관계를 찾기 어려운 성질을 가지는 것을 말한다. SHA-1은 1994년도에 NIST에 의해 개발된 SHA-0 알고리즘의 개정판으로 두 알고리즘 모두 64-bit의 메시지로부터 160bit의 해시값을 생성한다. 2001년 NIST는 SHA-1을 공표하면서 SHA-2로 불리는 해시 값의 길이가 더 긴 네 개의 변형을 같이 공표 하였는데[7] 그 중 하나가 SHA-256이다. SHA-256은 64-bit 메시지로부터 256bit의 해시값을 생성한다.

2.2.2. Symmetric Cryptography(AES)

AES(Advanced Encryption Standard)는 이전에 표준으로 인정되던 DES를 대신하기 위해 개발된 대칭키 블록 암호화 알고리즘이다. NIST가 새로운 암호화 알고리즘을 공모할 때, Joan Daemen과 Vincent Rijmen이 Rijndeal 암호화 알고리즘을 기반으로 하여 제안한 것이 채택되었고, 2001년 NIST에 의해 공표되었다[10, 11].

2.2.3. Public Key Cryptography(ECC)

ECC(Elliptic curve cryptography는 Neal koblitz[5]와 victor S. Miller[6] 가 독립적으로 제안한 공개키 암호화 알고리즘이다. 타원 곡선상의 군을 형성하는 점들의 집합에서 주어진 점 G가 있을 때 곡선 상의 다른 점 Y는

어떠한 정수 X와 주어진 점 G의 곱으로 표현 될 수 있으며 G와 Y가 주어졌을 때 어떠한 정수 X를 찾는 것이 힘들다는 Discrete Logarithm Problem을 이용하였다. 기존의 공개키 암호화 알고리즘인 RSA에 비해 짧은 키 길이로 대등한 안정도를 가지는 것이 장점이다.

2.3. 암호화 알고리즘

본 장에서는 소프트웨어 적으로 구현된 암호화 라이브러리를 소개한다. Openssl와 Relic은 대표적이고 널리 알려져 사용되는 암호화 라이브러리이다.

2.3.1. Openssl(AES 연산 참고)

OpenSSL은 데이터 통신 네트워크에서 프로토콜로 쓰이는 SSL과 TLS를 구현한 오픈소스 라이브러리이다. 라이브러리 안에는 데이터 통신 네트워크의 기본적인 암호화 기능과 유틸리티 함수 등이 구현되어 있다[8].

2.3.2. Relic(Hash, ECC 연산 참고)

RELIC은 편리함과 융통성을 강조한 현대 암호 구현의 메타-툴킷이다. 특정 암호의 암호화 강도와 구현 알고리즘을 선택해서 빌드 할 수 있기 때문에 암호 툴킷을 효과적이고 유용하게 사용 할 수 있다. TinyPBC가 RELIC 메타-툴킷을 사용한 대표적인 오픈 소스 암호화 라이브러리이다[9].

2.4. 타겟 보드와 개발 환경

본 장에서는 구현된 암호화 알고리즘을 동작시키기 위한 개발 환경에 대해서 설명한다. ATxmega128A1, MSP430F5529, PXA271을 사용하여 각각 8-, 16- 32-비트에 맞게 개발 환경을 구축하였다.

2.4.1. ATxmega128A1

ATxmega128A1은 8 비트 AVR 마이크로컨트롤러로써 저전력의 특징을 가진다. 또한 128K 바이트 플래시 메모리를 사용 할 수 있으며 8K 바이트 SRAM을 가진다. 최대동작주파수 32 MHz까지 동작가능하다.

구현된 암호화 알고리즘을 동작시키기 위해 ATmel studio를 사용하였다[12, 13]. ASF가 내장된 소프트에어로써 C/C++ 이나 어셈블리 코드로 쓰여진 응용프로그램을 디버깅 및 개발하는데 사용된다. AVG 뿐만 아니라 ARM Cortex-M 프로세서 또한 지원한다.

2.4.2. MSP430F5529

TI의 MSP430 패밀리의 경우 저전력의 특징을 가지며 기본적으로 저전력 모드를 가지고 있으며 외부 베터리 부착이 가능하다. MSP430F5529의 경우 16 비트 마이크로컨트롤러로써 최대동작 주파수 25MHz까지 동작가능하다. 또한 128K 바이트의 플래시 메모리를 가지며 8K 바이트 SRAM을 가진다[14].

보드 상에서 구현된 코드를 동작시키기 위하여 IAR-Embedded Workbench for MSP를 사용하였다. C/C++ 및 어셈블리코드에 대한 컴파일러와 디버거 툴을 지원한다[15].

2.4.3. PXA271

PXA271 프로세서의 경우 기본적으로 주파수 13MHz로 동작하지만 최대 416Mhz까지 구동이 가능하다. 또한 sleep 모드 및 deep sleep 모드와 같이 많은 저전력 모드를 가지고 있다. SRAM의 경우 256K 바이트 크기를 가지며 4개의 뱅크로 나누어진다. 32 M 바이트 SDRAM 및 플래시 메모리를 가진다[16].

2.4.4. 멀티 미터와 타겟 보드 전력 소모 측정관련

멀티미터는 Agilent 사의 34410A 멀티미터를 이용하여 전류량을 측정한다. 보드에 USB로 전원을 공급하는 대신, 파워서플라이를 이용하여 일정한 전압을 공급하고 보드에 멀티미터를 연결하여 전류 변화량을 측정한다. 전류 변화량은 Computer에서 Exel을 통해 수치화되어 확인이 가능하고 파워서플라이의 공급 전압과 측정된 전류량의 곱을 통해 전력 소모량을 측정한다.

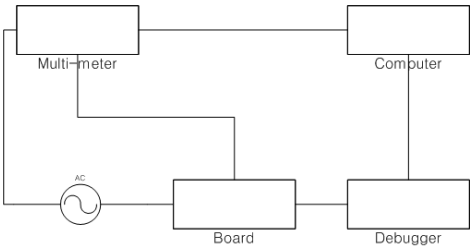

그림 1. 전력 측정 장비 환경 구성도
Fig. 1 Environment for power measuing equipments

Ⅲ. Dynamic Voltage Scale을 통한 암호화 프로토콜 수행 및 실험 절차

본 논문에서는 마이크로프로세서의 동작 주파수를 수행되는 연산에 따라 변경해 가며 사용가능한 기법을 제안한다. 그림 2에서는 고정으로 동작 주파수를 쓰는 방법과 DVS 방법을 이용하여 주파수를 조정해가며 사용하는 방법을 나타내고 있다. 먼저 고정으로 주파수를 사용하게 될 경우 간단한 일을 수행하게 될 때는 짧은 시간 안에 연산이 수행 가능하다. 하지만 암호화와 같은 복잡한 연산 수행을 위해서는 오랜 시간동안 연산을 수행해야 하는 문제점을 가지게 된다. 반면에 높은 동작 주파수로 연산을 수행하게 되면 짧은 시간 안에 연산 결과를 얻을 수 있지만 소모되는 에너지의 양 또한 비례하여 증가하게 된다.

하지만 성능 평가 부분에서 확인할 수 있듯이 전체 에너지 소모량 $J = V \times I \times T$(J: Energy, V: Volt, I: Current, T: Time)은 완전히 동일하게 증가하지 않음을 다양한 플랫폼에서 비교 테스트 해봄으로써 확인할 수 있었다. 따라서 이를 통해 낮은 동작 주파수로 동작하는 보드가 항상 높은 에너지 효율을 보여주지 않으며 오히려 높은 주파수를 사용하게 될 때 좋은 결과를 도출한다. 하지만 높은 동작 주파수를 사용하면 대기하는 기간에도 높은 전류를 사용하게 되므로 비효율적이다. 따라서 본 논문에서는 DVS 기법을 통해 대기 전류를 효율적으로 낮출 수 있다.

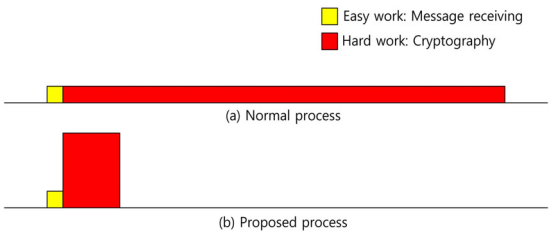

그림 2. 동작 방법 비교
Fig. 2 Comparison of working process

표 1에서는 센서가 가지는 상태에 따른 전력 소모를 나타낸다. 실험과정에서 우리는 대기 전력도 동작 주파수에 큰 영향을 받음을 확인하였다. 따라서 sleep 상태에서 동작 주파수를 최저로 유지하여 불필요하게 소모되는 전력을 줄여야 함을 확인할 수 있다.

표 1. 센서의 상태 비교
Table. 1 Status comparison on sensor

상태	전력소모
Sleep	낮음
Working	높음

표 2에서는 본 논문에서 수행한 DVS 기법에 대한 pseudo 코드를 나타내고 있다. 해당 코드는 자신에게 인터럽트가 발생하는 경우 해당 일을 끝내고 다시 sleep 모드로 변경되는 형식으로 동작한다. 만약 simple work에 대한 인터럽트가 발생하게 된다면 낮은 주파수로 동작을 하게 되며 만약 hard work가 들어오게 될 경우 주파수를 연산 수행기간동안 높여서 수행하게 된다. 여기서 simple work와 hard work를 나누는 기준은 클럭사이클로 봤을 때 1,000 이하로 동작하는 프로세서는 simple work로 생각한다. 그 이유는 동작 주파수를 변경하게 될 경우에도 보드 상에서는 세팅으로 인한 오버헤드가 작업 전후로 발생하기 때문이다. 해당 오버헤드가 약 1,000 이 되므로 이를 넘어서지 않는 경우를 simple work로 정의한다.

표 2. 본 논문에서 실험한 DVS 알고리즘
Table. 2 DVS algorithm in this paper

```
1. While(1) {
2. sleep
3. if(interrupt) {
4. if(simple work) {
5. do simple work }
6. else if(hard work) {
7. frequency modulation to high
8.  do hard work
9. frequency modulation to low } } }
```

Ⅳ. 성능 평가

4.1. ATxmega128A1

표 3에서는 동작 주파수에 따른 소모 전류가 다르게 나타남을 확인할 수 있다. 주파수가 높아질수록 대기 전류와 워킹 전류가 높아짐을 확인할 수 있다.

표 3. 동작 주파수에 따른 소모 전류 (mA), 타겟보드: ATxmega 128A1
Table. 3 Current consumption (mA) for dynamic frequency, Target board: ATxmega128A1

Status	주파수 (MHz)		
	1	12	32
Ready	34.06	34.75	35.91
Work	36.11	46.54	55.75

표 4, 5에서는 주파수에 따른 암호화 시간과 그에 따른 전력소모를 나타내고 있다. 여기서 동작 주파수가 짧은 경우에 더 많은 전력이 소모됨을 확인할 수 있다. 그 이유는 동작 전류는 줄어들지만 동작하는 시간이 더욱 많이 증가하게 된다. 따라서 전체 소모하는 전력은 주파수가 낮을수록 높아지게 된다. 그림 3-5에서는 ATxmega128 보드에서 주파수를 조정해 가며 암호화 연산을 수행한 결과를 나타낸다. 주파수가 낮으면 낮은 전류로 동작하지만 전체 수행 시간이 늘어나게 되어 전력소모가 많아짐을 확인할 수 있다.

표 4. 주파수(MHz)에 따른 암호화 시간 소모(ms), 동작 전압: 3.3 V, 타겟보드: ATxmega128A1
Table. 4 Time consumption for encryption depending on frequency, Target board: ATxmega128A1, voltage: 3.3 V

Scheme		1	12	32
		Time (ms)		
SHA-1		5	4	1.823
SHA256		60	10	3.24
AES		4.5	0.4	0.189
secp 160r1	SM	9,700	2,070	460
	Multi-SM	30,700	5,600	1,200

표 5. 주파수(MHz)에 따른 암호화 전력소모(mJ), 동작 전압: 3.3 V, 타겟보드: ATxmega128A1
Table. 5 Energy consumption for encryption depending on frequency, Target board: ATxmega128A1, voltage: 3.3 V

Scheme		1	12	32
		Energy Consumption (mJ)		
SHA1		0.59499	0.615648	0.3429
SHA256		7.13988	1.53912	0.599
AES		0.535491	0.061565	0.0356
secp 160r1	SM	1492.946	425.38692	85.084
	Multi-SM	4725.098	863.4463	221.958

즉 그래프와 x축의 넓이가 전력소모를 나타내는데 운영 주파수가 낮을수록 소모되는 전력이 많음을 확인할 수 있다.

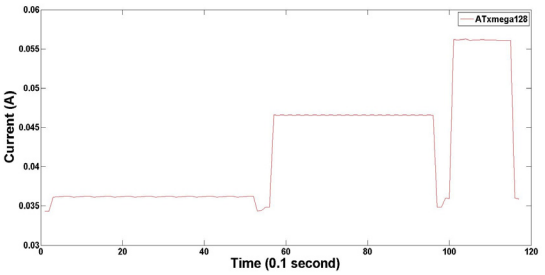

그림 3. ATxmega128에서 SHA1 1000번 수행
Fig. 3 Computing SHA1 on ATxmega128, 1000 times

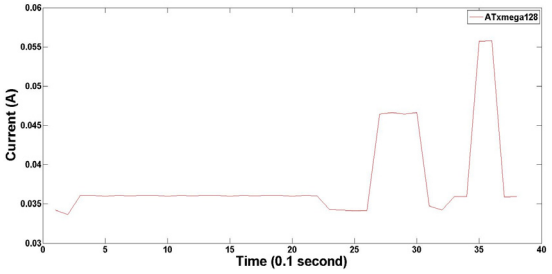

그림 4. ATxmega128에서 SHA256 40번 수행
Fig. 4 Computing SHA256 on ATxmega128, 40 times

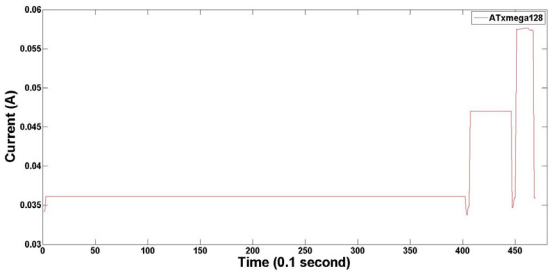

그림 5. ATxmega128에서 AES 10000번 수행
Fig. 5 Computing AES on ATxmega128, 10000 times

표 6에서는 가장 복잡한 연산인 ECC의 스칼라 곱셈을 3번 취했을 때 단일 동작 주파수를 쓰는 경우와 다중 동작 주파수를 쓰는 경우를 나누어 나타내고 있다. 전체적인 효율이 높은 주파수를 쓰는 경우 낮은 주파수로 대기를 하는 것이 높은 주파수를 단일로 쓰는 경우에

비해 성능이 좋게 나타남을 확인할 수 있다. 여기서 비교 벡터로 사용한 결과는 단일 동작 주파수이다.

표 6. 주파수(MHz)에 따른 성능 개선, 실험 시나리오: 1분간 3번의 스칼라 곱셈 수행하며 이 외의 시간에는 대기 모드로 동작
Table. 6 Performance enhancement depending on frequency

Scheme	1	12	32
	Energy (mJ)		
Pre	6940	7122	7200
Our	6940	6999	6842
$\frac{Our}{\mathrm{Pre}}(\%)$	100	98.27	95.02

4.2. MSP430

표 7에서는 MSP403 보드의 경우를 나타낸다. 여기서도 주파수가 높아짐에 따라 대기와 워킹 전류가 증가함을 확인할 수 있다.

표 7. 동작 주파수에 따른 소모 전류(mA), 타겟보드: MSP430
Table. 7 Current consumption (mA) for dynamic frequency, Target board: MSP430

Status	주파수 (MHz)		
	8	12	25
Ready	7.84	8.2946	9.439
Work	10.815	12.543	18.003

표 8, 9에서는 주파수에 따른 시간과 전력 소모를 나타낸다. 여기서도 주파수가 높을수록 적은 전력을 소모함을 확인할 수 있다.

표 8. 주파수(MHz)에 따른 암호화 시간 소모(ms), 동작 전압: 3.3 V, 타겟보드: MSP430
Table. 8 Time consumption for encryption depending on frequency, Target board: MSP430, voltage: 3.3 V

Scheme		8	12	25
		Time (ms)		
SHA-1		5	3.4	1.002
SHA256		12.4	8.3	3.921
AES		0.45	0.3	0.119
secp 160r1	SM	580	400	159
	Multi-SM	1650	1116.7	600

표 9. 주파수(MHz)에 따른 암호화 전력소모(mJ), 동작 전압: 3.3 V, 타겟보드: MSP430
Table. 9 Energy consumption for encryption depending on frequency, Target board: MSP430, voltage: 3.3 V

Scheme		8	12	25
		Energy Consumption (mJ)		
SHA1		0.178448	0.140732	0.162321
SHA256		0.44255	0.343553	0.311196
AES		4.56885	3.0459	1.9278
secp 160r1	SM	37.323	28.05	25.757
	Multi-SM	106.1775	78.30625	97.198

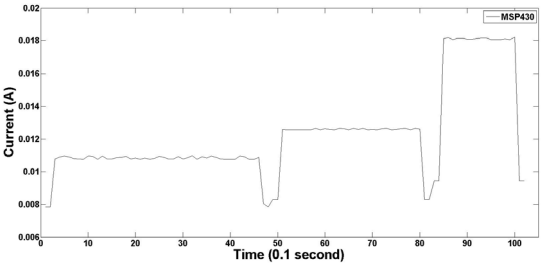

그림 6. MSP430에서 SHA1 1000번 수행
Fig. 6 Computing SHA1 on MSP430, 1000 times

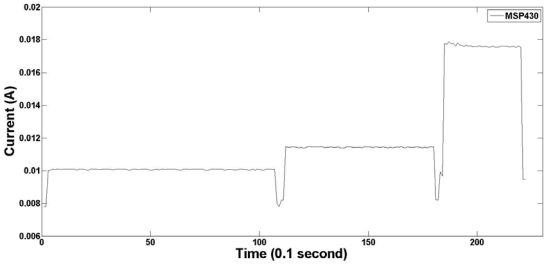

그림 7. MSP430에서 SHA256 1000번 수행
Fig. 7 Computing SHA256 on MSP430, 1000 times

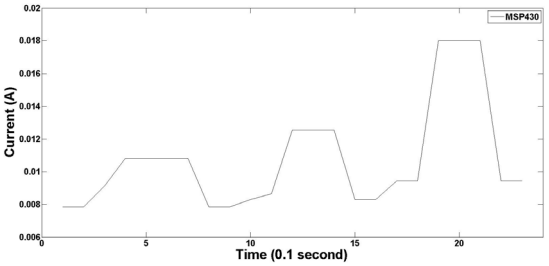

그림 8. MSP430에서 AES 1000번 수행
Fig. 8 Computing AES on MSP430, 1000 times

그림 6-8에서는 MSP430 상에서 암호화의 전력 소모를 나타낸다.

표 10에서와 같이 DVS 기법을 적용하였을 때 성능이 좋아짐을 확인할 수 있다.

표 10. 주파수(MHz)에 따른 성능 개선, 실험 시나리오: 1분간 10번의 스칼라 곱셈 수행하며 이 외의 시간에는 대기 모드로 동작
Table. 10 Performance enhancement depending on frequency

Scheme	8	12	25
	Energy (mJ)		
Pre	1609.262	1698.41	1913.857
Our	1609.262	1614.4	1605.645
$\frac{Our}{Pre}$(%)	100	95.05	83.89

4.3. Imote2

표 11에서는 Imote2 상에서의 동작 주파수에 따른 전류를 나타내고 있다. 여기서도 다른 노드들과 동일한 결과가 나타남을 확인할 수 있다.

표 11. 동작 주파수에 따른 소모 전류(mA), 타겟보드: Imote2
Table. 11 Current consumption(mA) for dynamic frequency, Target board: Imote2

Status	주파수 (MHz)					
	13	104	208	312	416	512
Ready	31.9	52.7	76.1	91.8	102.6	117.6
Work	32.9	59.1	89.7	110.1	124.1	142.4

표 12, 13에서는 다른 센서들과 동일하게 소모되는 시간과 전력량이 높은 주파수일수록 줄어듦을 확인할 수 있다.

표 12. 주파수(MHz)에 따른 암호화 시간 소모(ms), 동작 전압: 4.5 V, 타겟보드: Imote2
Table. 12 Time consumption for encryption depending on frequency, Target board: Imote2, voltage: 4.5 V

Scheme		13	104	208	312	416
		Time (ms)				
SHA-1		1.5	0.172	0.087	0.06	0.045
SHA256		1.75	0.215	0.105	0.075	0.05
AES		0.19	0.024	0.012	0.008	0.005
secp 160r1	SM	628	82	41	31	28
	Multi-SM	1890	245	120	90	75

표 13. 주파수(MHz)에 따른 암호화 전력소모(mJ), 동작 전압: 4.5 V, 타겟보드: Imote2
Table. 13 Energy consumption for encryption depending on frequency, Target board: Imote2, voltage: 4.5 V

Scheme		13	104	208	312	416
		Energy Consumption (mJ)				
SHA1		0.222	0.045	0.035	0.029	0.025
SHA256		0.259	0.056	0.042	0.037	0.028
AES		0.028	0.006	0.004	0.004	0.003
secp 160r1	SM	93.33	21.70	16.42	15.42	15.95
	Multi-SM	280.6	64.83	48.07	44.77	42.73

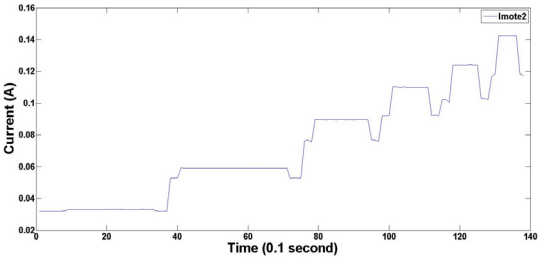

그림 9. Imote2에서 SHA1 2000번 수행
Fig. 9 Computing SHA1 on Imote2, 2000 times

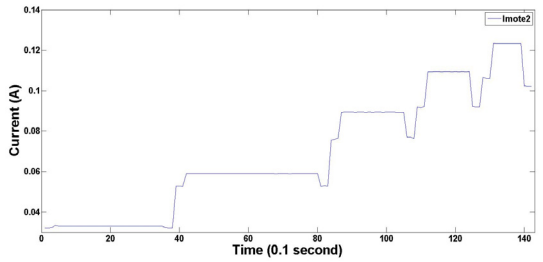

그림 10. Imote2에서 SHA256 2000번 수행
Fig. 10 Computing SHA256 on Imote2, 2000 times

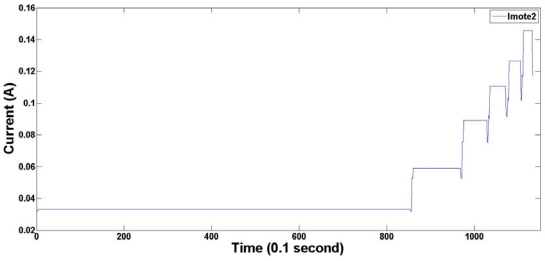

그림 11. Imote2에서 AES 500,000번 수행
Fig. 11 Computing AES on Imote2, 500,000 times

그림 9-12에서는 여러 동작 주파수에 따른 전류 소모를 나타낸다. 주파수가 증가할수록 소비되는 전류가 늘어나지만 동작 시간이 줄어듦을 확인할 수 있다.

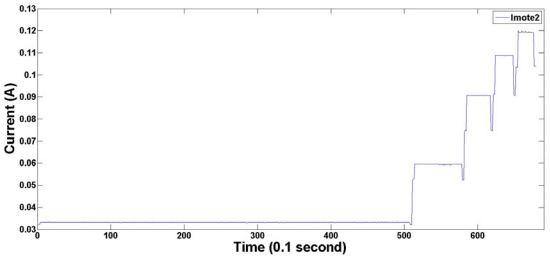

그림 12. Imote2에서 ECC 160비트 스칼라 곱셈 100번 수행
Fig. 12 Computing ECC 160-bit scalar multiplication on Imote2, 100 times

표 14에서는 다중 동작 주파수를 사용할 때 성능이 개선됨을 확인할 수 있다.

표 14. 주파수(MHz)에 따른 성능 개선, 실험 시나리오: 1분간 10번의 스칼라 곱셈 수행하며 이 외의 시간에는 대기 모드로 동작
Table. 14 Performance enhancement depending on frequency

Scheme	13	104	208	312	416
	Energy (mJ)				
Pre	8644.1	14251.	20570	24812.	27731.
Our	8644.1	8712.2	8718.3	8722.7	8731.8
$\frac{Our}{\mathrm{Pre}}(\%)$	100	61.1	42.3	35.1	31.5

V. 결 론

본 논문에서는 센서 네트워크 상에서 복잡한 연산인 암호화 기법에 DVS기법을 적용한 결과를 여러 임베디드 장비에서 상에서 동작시키고 이에 따른 실제 전력을 측정하였다. 이를 통해 주파수가 높을수록 복잡한 연산을 빠르게 계산하기 때문에 오히려 전력 소모가 줄어드는 사실과 동작 주파수에 따라 대기 전류가 달라 낮은 주파수로 대기를 하는 것이 이득이라는 점을 바탕으로 동적 전압 스케일 기법이 센서네트워크 상에서의 암호화 과정에도 효율적으로 적용이 가능함을 확인할 수 있었다. 해당 프로토콜은 에너지가 한정적인 수중 통신과 같은 환경에서 소모되는 전력량을 효율적으로 줄인다. 실험을 통해 DVS은 암호화 연산을 해저 통신 환경 상에서 효율적인 전원 관리가 가능함을 확인 할 수 있었다.

감사의 글

본 논문은 지식경제부 산업융합원천기술개발사업으로 지원된 연구결과입니다(No.10043907).

REFERENCES

[1] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, “Wireless sensor network survey,” *Computer Networks*, 52 , pp. 2292 – 2330, 2008

[2] Ye, Wei, John Heidemann, and Deborah Estrin. "An energy-efficient MAC protocol for wireless sensor networks." In *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 3, pp. 1567-1576, 2002

[3] Polastre, Joseph, Jason Hill, and David Culler. "Versatile low power media access for wireless sensor networks." In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pp. 95-107, 2004

[4] M.C. Vuran, I.F. Akyildiz, “Spatial correlation-based collaborative medium access control in wireless sensor networks,” *IEEE/ACM Transactions on Networking 14,* 316 – 329, 2006

[5] Koblitz, N. "Elliptic curve cryptosystems". Mathematics of Computation 48, pp. 203 – 209, 1987

[6] Miller, V. "Use of elliptic curves in cryptography". CRYPTO 85, pp. 417 – 426, 1985

[7] NIST, “FIPS 180-1” (supereded by FIPS 180-2). See also NIST’s Secure Hasing site.

[8] OpenSSL Homepage for AES : http://www.openssl.org, 2014

[9] Relic Homepage for TinyPBC : https://code.google.com/p/relic-toolkit/, 2014

[10] J. Daemen, V. Rijmen, "AES Proposal: Rijndael", 1999

[11] National Institute of Standards and Technology (NIST),

"FIPS 197: Advanced Encryption Standard (AES)", 2001
[12] Information of ATxmega128A1, Available at http://www.atmel.com/devices/atxmega128a1.aspx, 2013
[13] Information of ATxmel Studio, Available at http://www.atmel.com/Microsite/atmel_studio6/default.aspx, 2013
[14] Information of MSP430F5529, Available at http://www.ti.com/product/msp430f5529, 2013
[15] Information of IAR-Embedded Workbench for MSP, Available at http://www.iar.com/, 2013
[16] Information of PXA271, Available at http://www.datasheetarchive.com/PXA271-datasheet.html, 2013
[17] Goodman, James, Abram P. Dancy, and Anantha P. Chandrakasan. "An energy/security scalable encryption processor using an embedded variable voltage DC/DC converter." Solid-State Circuits, IEEE Journal of 33, no. 11, pp. 1799-1809, 1998
[18] Dynamic voltage scaling, available in: http://en.wikipedia.org/wiki/Dynamic_voltage_scaling, 2013

서화정(Hwa-jeong Seo)

2010년 2월: 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월: 부산대학교 컴퓨터공학과 석사 졸업
2012년 3월 ~ 현재: 부산대학교 컴퓨터공학과 박사과정
※관심분야 : 정보보호, 암호화 구현, IoT

김호원(Ho-won Kim)

1993년 2월: 경북대학교 전자공학과 학사 졸업
1995년 2월: 포항공과대학교 전자전기공학과 석사 졸업
1999년 2월: 포항공과대학교 전자전기공학과 박사 졸업
2008년 2월: 한국전자통신연구원 정보보호연구단 선임연구원/팀장
2008년 3월~현재: 부산대학교 정보컴퓨터공학부 부교수
※관심분야 : 스마트그리드 보안, RFID/USN 정보보호 기술, PKC 암호, VLSI 설계, embedded system 보안, IoT