Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.3, Jun. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.3.661

무선 환경에서 SSL/TLS를 사용하는 IoT의 에너지 효율성 향상을 위한 기법*

정 진 희,† 조 대 호‡
성균관대학교 전자전기컴퓨터공학과

A Method to Improve Energy Efficiency for IoT Using SSL/TLS on Wireless Network*

Jin Hee Chung,† Tae Ho Cho‡
Department of Information and Communication Engineering,
Sungkyunkwan University

요 약

사물인터넷은 다양한 기기들이 서로 연결되어 효율적인 에너지 소모와 높은 보안을 유지하기 위해 경량의 메시징 프로토콜인 MQTT와 암호화 프로토콜인 SSL/TLS를 사용한다. SSL/TLS의 cipher suite 협상 단계에서 기기에 고정된 cipher suites로부터 선호도가 가장 높은 cipher suite를 선택한다. 선택된 cipher suite는 해당 통신 중에 필수적으로 제공받아야 하는 무결성, 기밀성을 제공하지만 필요 이상으로 높은 강도의 보안성을 제공할 수 있다. 이러한 한계는 에너지를 필요 이상으로 소비하게 만들 수 있으므로 본 논문에서는 SSL/TLS를 사용한 기기들의 에너지 효율성을 향상시키는 퍼지 기반 cipher suite 결정 기법을 제안한다. 실험을 통해 제안 기법은 기존 기법보다 에너지 효율성이 평균 36.03% 향상되었다.

ABSTRACT

The Internet of Things (IoT) is an infrastructure of physical objects that could be connected to the Internet. Most of these are low performance to ensure a reasonable cost for the smart physical objects. Thus, these devices usually use a lightweight messaging protocol: message queue telemetry transport with SSL/TLS. Cipher suites in device are fixed by default and selected based on preference in SSL/TLS. However, the selected cipher suite provides high security level more than expected. This limitation causes energy waste and overhead of devices. In order to counter this problem, we proposed fuzzy logic based cipher suite decision method to improve energy efficiency. Our proposed method saved 36.03% energy.

Keywords: Internet of things, security service, SSL/TLS, IoT security, MQTT, fuzzy logic

I. 서 론

사물인터넷(internet of things)은 다양한 사물들이 인터넷에 연결되는 기반기술이다[1]. 사물인터넷은 사용자들이 유무선 네트워크를 통해 사물들에 직접 접속하고 사물을 제어할 수 있을 뿐만 아니라 다양한 기기에서 수집된 정보를 통해 실시간으로 정확한 날씨를 알려주는 것과 같이 편리하고 지능적인

Received(01. 07. 2016), Modified(1st: 03. 10. 2016, 2nd: 05. 20. 2016), Accepted(06. 08. 2016)
* 이 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2015R1D1A1A01059484)
† 주저자, jinhee91@skku.edu
‡ 교신저자, thcho@skku.edu(Corresponding author)

기능들을 제공한다. 지능적인 기기로 인해 사회가 발전하고 생활의 편리함이 높아진다는 이점이 있지만, 최근 미국에서 감시카메라와 유아 모니터가 도·감청되어 총 700개가 넘는 카메라의 실시간 영상이 인터넷에 유포되는 등 사물인터넷 보안의 문제가 크게 주목받고 있다. 사물인터넷 환경이 보안에 취약한 데는 여러 이유가 있는데 그중 하나는 기기의 성능이 낮은 데 있다. 사물인터넷 기기의 대부분은 사물의 단가를 맞추기 위해 저 성능 저 전력 하드웨어를 사용한다. 그러므로 기기는 성능에 따라 보안성과 에너지 소모를 모두 고려해야 하기 때문에 비교적 보안성이 낮은 방법을 적용할 수밖에 없는 것이다. 이러한 문제를 완화시키기 위해 사물인터넷 기기는 에너지 소모가 낮은 경량의 사물인터넷 표준 메시지전달 프로토콜인 MQTT와 SSL/TLS를 사용한다.

그러나, 기존의 SSL/TLS를 그대로 저 사양 기기에 적용시키기에는 무리가 있다. SSL/TLS는 핸드셰이크의 첫 번째 단계에서 두 종단 간의 세션에서 사용될 cipher suite가 선호도 순으로 결정된다. 하지만 SSL/TLS를 사용하는 기기 중에는 매우 에너지가 제한적인 센서 같은 사물이 있을 수 있으므로 기기를 고려해서 효율적으로 에너지를 소모해야 한다. 컴퓨터와 같은 고성능 기기와 달리 사물인터넷 기기의 성능은 데이터 전송만 가능한 기기부터 임베디드 프로세싱 능력까지 갖춘 기기까지 성능의 폭이 크기 때문에 기기에 맞게 효율적으로 에너지를 사용하는 것이 중요하다. 또한, 다양한 사물인터넷 기기의 기능과 형태에 맞춰 효율적으로 보안성을 제공하는 것이 필요하다. 예를 들어, 단순한 광고 메시지 전달을 위한 기기와 같은 경우는 통신에 필요한 최소한의 보안성은 만족해야 하지만 필요 이상의 보안성 보장은 과한 에너지 소비와 오버헤드로 인한 기기의 수명 단축 및 에너지 고갈을 야기한다.

본 논문에서는 사물인터넷 기기를 기능과 형태에 따라 네 가지로 구분하여 종류별 보안 유연도를 설정하였다. 그리고 SSL/TLS의 첫 번째 단계에서 설정된 보안 유연도와 퍼지 로직을 통해 보안성을 유지하고 기기의 환경에 적합한 cipher suite를 결정하는 방법을 제안한다.

2장에서 배경을 설명하고 3장에서 제안 기법에 대해 다룬다. 4장에서 실험 결과를 보여주고 5장에서 결론과 향후 계획에 대한 설명으로 마무리한다.

II. 배 경

2.1 MQTT

MQTT는 OASIS에서 지정한 경량의 사물인터넷 표준 메시징 프로토콜이며[2] Fig. 1과 같이 기기를 Broker, Publisher, Subscriber로 구별한다. Publisher와 Subscriber 사이에 Broker가 존재하고 이를 통해 메시지를 교환하는 구조로 이 프로토콜이 운영된다. Publisher는 메시지와 토픽을 발행하여 Broker에게 보내고 Broker는 해당 토픽을 구독한 Subscriber에게 메시지를 전달한다. MQTT는 메시지를 평문으로 전송하기 때문에 SSL/TLS와 같은 보안 프로토콜의 적용이 필요하다.

Fig. 1. MQTT

2.2 SSL/TLS

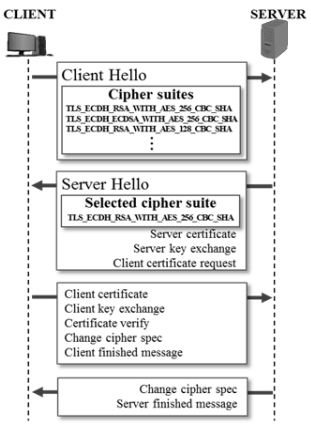

Fig. 2. Handshake process of SSL/TLS

IETF 표준 규약으로써 클라이언트와 서버의 암호화

통신을 위해 전송계층과 응용계층에서 사용된다 [3].

Fig. 2는 SSL/TLS의 핸드셰이크 과정을 보여준다. 첫 번째 단계에서 클라이언트(client)가 서버(server)에게 세션을 열기 위해 Client Hello 메시지를 보내 협상을 시작한다. 클라이언트는 지원할 수 있는 여러 개의 알고리즘 그룹들을 선호도 순으로 정리하여 리스트로 보내는데 이 리스트를 Cipher suites라고 하고 각각을 Cipher suite라고 한다. 서버는 Cipher suites에서 지원할 수 있는 것 중 가장 순위가 높은 Cipher suite를 선택하게 된다. Cipher suite는 키 교환, 인증, 암호화 방식, MAC에 관한 것이며 각각에 대한 알고리즘을 선택하는 것이 아니라 하나의 그룹인 Cipher suite로써 선택된다. 협상이 끝나면 앞서 협상한 cipher suite를 사용하여 인증 및 암호화 통신이 시작된다.

III. 제안 기법

3.1 제안 기법

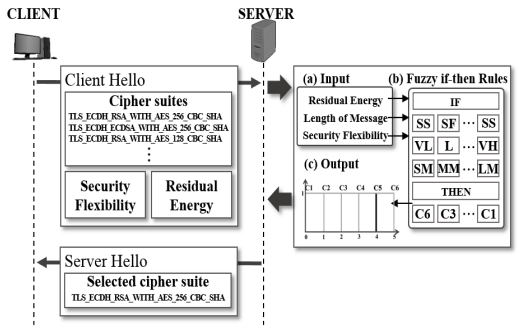

Fig. 3. Process of proposed method

위의 Fig. 3은 제안 기법을 나타낸 그림이다. 핸드셰이크의 첫 번째 단계인 Client Hello 단계에서 기존 기법은 Cipher suites를 보내 서버와 협상하는 데, 제안기법은 Cipher suites와 함께 보안 유연도와 기기의 잔여 에너지 정보를 같이 보낸다. 이 때 보안 유연도는 클라이언트가 해당 연결에 요구하는 보안성의 유연한 정도이다. Fig. 3 (a)와 같이 전송된 두 개의 정보와 메시지 길이가 퍼지의 입력으로 들어가고 입력된 정보와 클라이언트의 상황에 맞게 정의되는 (b)의 퍼지 규칙을 기반으로 결과 값 (c)를 도출해 낸다. 최종적으로 상황에 적합한 cipher suite가 선택된다.

3.2 보안 유연도

보안 유연도는 아래 Table 1과 같은 기준으로 1부터 5까지로 분리된다. 분류의 기준은 IoTFS-0081의 사물인터넷 기능에 따른 분류를 참고하였다[4]. 1에 가까울수록 보안성은 유연해 지고 사물인터넷이 만족해야 할 최소 보안성을 갖추게 되며, 5에 가까울수록 보안성이 엄격해지며 강력한 보안성을 갖추게 된다.

Table 1. Security flexibility

security flexibility	functional classification
1	
≀	communicate indirectly to transmit data
2	
≀	able to interact with other devices and able to read and write data,
3	
≀	able to obtain environment information and convert to digital signal, include sensors and actuators which can communicate with other devices and use gateway.
4	
≀	embedded processors having communication ability including home appliances and smart phone.
5	

3.2.1 제안기법의 최소 보안성

사물인터넷 기기를 위해 에너지 효율성을 높이기 위해서 보안 유연도와 관계없이 최소로 만족하는 보안성은 IETF의 최신 표준 규약인 TLS 1.2 버전에서 권고하는 사항을 준수한다[5]. 대표적으로, 통신의 인증, 기밀성, 무결성을 해칠 수 있다고 알려진 RC4 ,IDEA, DES와 같은 알고리즘은 제외하고 AES 알고리즘의 사용을 권장한다. 또한 1.2 버전에서 사용하는 cipher suites를 사용하여 통신에 사용될 cipher suite를 협상한다.

3.3 퍼지 로직

퍼지 로직의 입력 파라미터는 잔여 에너지(RE) = {VL(very low), L(low), M(middle), H(high), VH(very high)}와 메시지 길이(LM) = {S(short), M(middle), L(long)}, 그리고 보안 유연도(SF) =

{SF(flexible), SS(strict)}이다.

출력 파라미터는 cipher suite(C) = {C1, C2, C3, C4, C5, C6}이다. 각각이 뜻하는 파라미터는 클라이언트와 서버가 동시에 지원하는 cipher suites 중 클라이언트의 선호도로 상위 6개 cipher suite를 메시지 길이 100 bytes 기준 소비전력을 계산하여 그 값의 내림차순으로 정렬한 것이다.

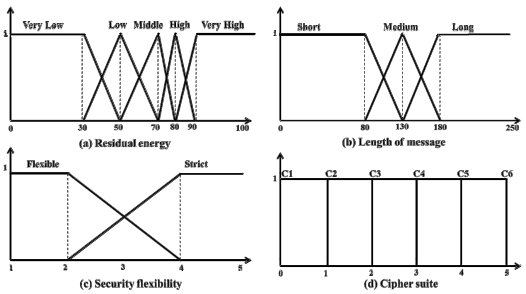

Fig. 4. Fuzzy membership function

Fig. 4의 (a), (b), (c)는 제안된 퍼지 로직 시스템의 입력 값 세 가지(RE, LM, SF)의 멤버십 함수이고 (d)는 출력(Cipher suite) 멤버십 함수이다. 퍼지 로직 시스템의 멤버십 함수는 사물인터넷 기기의 조건을 고려하여 결정되었다. 효율적으로 설계하기 위해서 데이터를 퍼지 멤버십 함수의 튜닝 전략[6]을 이용하여 조정하였고, 이 데이터를 기반으로 멤버십 함수를 설정하였다. 퍼지 로직 시스템 방법의 추론은 맘다니 모델의 합성방법[7]을 사용하고 역 퍼지화 방법으로는 무게 중심 법을 사용한다.

- (a) 잔여 에너지: 기기에 남은 에너지를 백분율로 계산되어 입력되는 값이다. 소비 에너지를 줄이고 기기의 수명을 늘리기 위해서 사용된다.
- (b) 메시지 길이: 협상되는 cipher suite의 구성요소 중 통신하는 동안 많은 에너지를 소비하는 것은 암호화 과정이다. 그러므로 메시지 길이에 대해 고려해야 소비 에너지를 줄일 수 있다. MQTT에서 허용하는 최대 메시지 길이인 250MB보다 작은 값이 들어간다.
- (c) 보안 유연도: 사물인터넷 기기의 기능에 따른 보안성의 유연한 정도이다. 최소의 보안성을 유지하면서 기기 특성에 따라 보안을 강화하기 위해서 사용된다.

3.4 퍼지 규칙

Table 2. Cipher suite evaluation score

C \ score	E	P	T	$\frac{E}{T}-\frac{P}{T}$=ES
C1	1	6	7	-0.71429
C2	2	5	7	-0.42857
C3	3	2	5	0.2
C4	4	3	7	0.142857
C5	5	4	9	0.111111
C6	6	1	7	0.714286
C7	X	X	X	X

Table 3. The rule of selecting a cipher suite

residual energy	selected cipher suite	
very high	the highest preference cipher suite	
high	security flexibility	
	strict	a cipher suite which has the highest preference
	flexible	a cipher suite which has the smallest absolute value of ES
middle	strict	
	flexible	if the cipher suites (only for cipher suites which have positive ES number) is rearranged in order of increasing, the first, second and third cipher suites are selected when message length is S, M, L
low	if the cipher suites (only for cipher suites which have positive ES number) is rearranged in order of decreasing, the first, second and third cipher suites are selected when message length is L, M, S	
very low	the highest ES valued cipher suite	

퍼지 규칙을 정하는 과정을 설명하기 위해 Table 5의 cipher suites를 사용하여 Table 2에 규칙 정의 과정을 보였다. Table 2와 같이 각각의 cipher suite(C)마다 점수를 산정하였다. E는 소비전력을 뜻하고 P는 선호도, T는 총점을 뜻한다. Cipher suites에서 제안기법의 최소 보안성을 만족하지 못할 경우 C7과 같이 고려대상에서 제외시킨다. 그 이외의 cipher suite는 소비전력이 적을수록, 선호도가 높을수록 큰 점수를 얻는다. 산정된 점수를 기반으로 최종 평가점수 ES(Evaluation Score)를 계산한다. ES값이 음수면 비교적 선호도는 높고 소비전력이 큰 경우이며 양수일 경우 비교적 소비전력이 적고 선호도가 낮은 경우를 뜻한다. 또한, 소비전력

과 선호도의 상대적 격차는 ES의 절댓값으로 알 수 있다. 최종 평가점수는 Table 3과 같이 잔여에너지(RE)와 메시지 길이, 보안 유연도를 기준으로 cipher suite를 선택하는 데 사용된다. 정해진 규칙의 일부분은 Table 4와 같다.

Table 4. Fuzzy if-then rules

rule No.	input			output
	SF	RE	LM	C
2	SS	M	SM	C5
6	SS	L	MM	C3
17	SF	M	SM	C5
29	SF	VH	LM	C1

IV. 실험 결과

4.1 초기 파라미터

소비 에너지 비교 실험을 위해 총 2000회의 실험을 하였고, 실험 한 회당 기기의 잔여 에너지와 메시지 길이가 랜덤으로 생성된다. 보안 유연도는 1부터 5까지의 입력이 랜덤으로 결정된다. cipher suite의 선호도는 Open SSL의 최신버전인 1.0.2의 선호도를 참고했다. 클라이언트와 서버가 공동으로 지원하는 cipher suites는 Table 5로 정의한다.

Table 5. Output cipher suite parameters

No.	cipher suite
C1	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
C2	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
C3	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
C4	TLS_DH_RSA_WITH_AES_128_CBC_SHA
C5	TLS_RSA_WITH_AES_256_CBC_SHA
C6	TLS_RSA_WITH_AES_128_CBC_SHA
C7	TLS_RSA_WITH_RC4_128_SHA

SSL/TLS와 제안 기법이 선택한 cipher suite의 소비 에너지는 [8, 9]의 데이터를 참고하여 계산되었다. 대표적으로 SHA는 바이트당 0.75 μJ, AES_256_CBC는 바이트당 2.29 μJ를 소비한다. 실험에 사용된 기기는 Compaq iPAQ 3670 pocket PC이며 206MHz의 CPU 클록 속도와 64MB의 RAM을 가지고 있다. 키 교환에서 사용된 DH는 512 bits의 키를 가지며 ECDH는 163 bits, 인증의 RSA는 1024 bits, ECDSA는 163 btis의 키를 가지는 알고리즘이 사용되었다.

4.2 결과

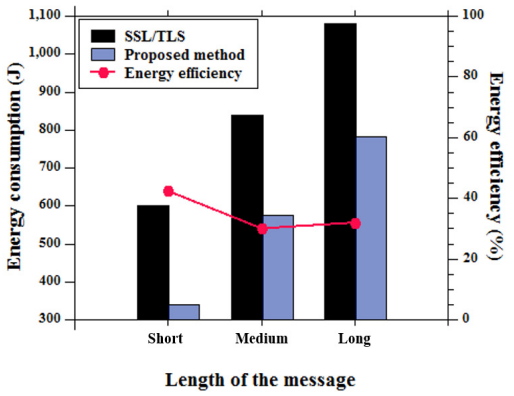

Fig. 5. Energy consumption and efficiency

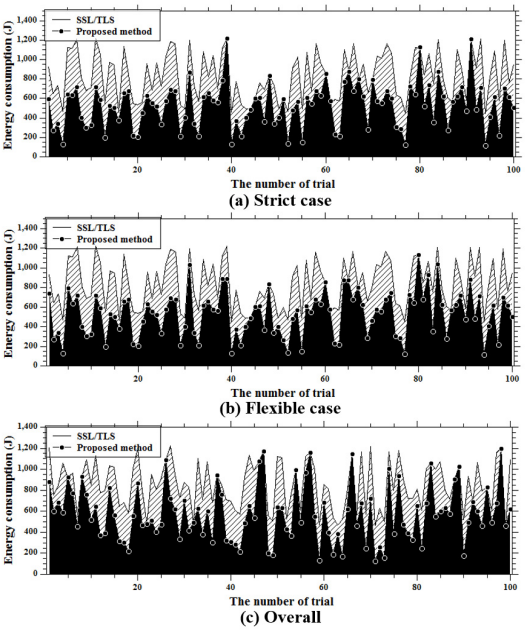

Fig. 6. Energy consumption and efficiency

클라이언트와 서버의 공동 지원 cipher suites 중에서 기존 기법은 가장 높은 선호도를 갖는 C1이 선택된다. 모든 경우에서 기존 기법보다 같거나 적은 에너지를 소비했고, 보안 유연도, 메시지 길이, 잔여 에너지가 랜덤이었을 때 평균 36.03% 에너지 감소율을 보였다. Fig. 5는 메시지 길이별 평균 소비 에너지의 차이와 에너지 효율성을 보여준다. 메시지 길이가 short일 때 42.43%, medium은 30.13%,

long은 32.06%의 에너지 효율을 보였다. Fig. 6은 보안 유연도별 소비에너지를 보여준다. 엄격할 경우 평균 35.33%의 에너지 효율성을 보였고(a), 유연한 경우 36.93% 향상을 보였다(b). 보안 유연도, 메시지 길이, 잔여에너지가 랜덤이었을 때 제안기법의 전체 에너지 효율성은 평균 36.03% 향상 되었다(c).

V. 결론 및 향후 연구

MQTT를 사용하는 사물인터넷은 보안을 강화하기 위해 SSL/TLS를 사용할 수 있다. 본 논문은 MQTT를 사용하는 사물인터넷 기기가 SSL/TLS로 보안을 강화했을 때 에너지 효율성 향상을 위해서 퍼지 로직 시스템 기반의 cipher suite 결정 기법을 제안한다. 실험 결과는 제안기법으로 평균 36.03%의 에너지 효율성이 높아진 것을 보여준다. 향후 연구로는 퍼지의 멤버십 함수를 최적화를 할 예정이다.

References

[1] K. Zhao and L. Ge, "A survey on the internet of things security," in *Computational Intelligence and Security (CIS), 2013 9th International Conference on, 2013,* pp. 663-667, 2013.

[2] A. Banks and R. Gupta, "MQTT Version 3.1. 1," *OASIS Standard,* 2014.

[3] E. Rescorla, *SSL and TLS: Designing and Building Secure Systems.* Addison-Wesley Reading, 2001.

[4] IoT Forum, "The Classification and Security Requirements based on IoT Device Capabilities," IoTFS-0081, 12.1, 2015.

[5] T. Dierks, "The transport layer security (TLS) protocol version 1.2," 2008.

[6] J. Yen and R. Langari, *Fuzzy Logic: Intelligence, Control, and Information.* Prentice-Hall, Inc., 1998.

[7] R. Babuška, "Fuzzy Systems, Modeling and Identification," *Delft University of Technology, Department of Electrical Engineering Control Laboratory, Mekelweg,* vol. 4, 1996.

[8] N. R. Potlapally, S. Ravi, A. Raghunathan and N. K. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," *Mobile Computing, IEEE Transactions on,* vol. 5, pp. 128-143, 2006.

[9] R. Karri and P. Mishra, "Minimizing energy consumption of secure wireless session with QoS constraints," in *Communications, 2002. ICC 2002. IEEE International Conference on,* 2002, pp. 2053-2057, 2002.

〈저자소개〉

정 진 희 (Jin Hee Chung) 학생회원
2015년 2월: 단국대학교 컴퓨터과학과 공학사
2015년 3월~현재: 성균관대학교 전자전기컴퓨터공학과 석사과정
〈관심분야〉 사물인터넷, 정보보호

조 대 호 (Tae Ho Cho) 정회원
1983년 2월: 성균관대학교 전자공학과 공학사
1987년 2월: University of Alabama 전자공학과 공학석사
1987년 2월: University of Arizona 전자 및 컴퓨터공학과 공학박사
1995년~현재: 성균관대학교 정보통신공학부 교수
〈관심분야〉 무선 센서 네트워크, 모델링 시뮬레이션, 지능 시스템, 모델링 방법론, 네트워크 보안 시뮬레이션, 전사적 자원 관리