IoT 환경에 적합한 경량 DTLS 프로토콜 구성 방법

안수현* 김광조*

*KAIST 정보보호대학원

A Method of lightweight DTLS protocol for IoT

SooHyun Ahn* Kwangjo Kim*

*Graduate school of information security, KAIST.

요 약

최근 사물인터넷 (IoT: Internet of Things)의 등장으로 인하여 점점 IoT의 역할이 중요해지고 있지만 이에 대한 보안은 아직 미비한 수준이라 할 수 있다. IoT 디바이스에 프로토콜로 고려되고 있는 Host Identity Protocol (HIP)이나 Datagram Transport Layer Security (DTLS) 프로토콜은 보안적인 측면이나 성능적인 측면에서 아직 IoT 환경에 적용되기에는 보완되어야 할 점이 많은 것이 현실이다. 특히, HIP 프로토콜은 아직 프로토콜에 대한 개발이 진행 중에 있어 DTLS에 비해 호환성이 떨어진다. 따라서, 이 논문에서는 IoT 환경을 위해 제시되고 있는 DTLS에 경량 암호와 인증프로토콜을 도입한 DTLS+를 제안한다.

I. 서론

iPhone, Android phone으로 대변되는 스마트폰에 등장과 함께 무선네트워크에 대한 관심이 높아짐으로 인해 공공기관, 학교, 회사, 가정 심지어 도심 속 거리까지 무선 AP, 무선 LAN 등 무선 환경에 쉽게 접속가능하게 해주는 장치들이 설치됨에 따라 이제는 유선 네트워크 환경뿐만이 아니라 무선 네트워크 환경도 점점 일반 사람들에게 영향을 미칠 수 있는 중요한 부분이 되어가고 있다. 이러한 무선 네트워크의 발전과 함께 소위 사물인터넷이라 불리 우는 IoT가 등장하게 되었고 이에 대한 의존도와 역할이 점점 증가하고 있다. 하지만, IoT에 역할이 중요해지고 있는 것에 반해 이에 대한 보안은 아직 미비한 것이 현실이다. 최근 이러한 사실을 반영하듯이 IoT를 이용한 개인정보 유출 및 스팸 메일 발송 등 IoT의 취약점을 악용하는 공격이 점점 증가하고 있는 추세이다. 이에 따라 IoT 환경에 보안성을 제공해 줄 수 있는 프로토콜로 HIP와 DTLS가 제안되고 있다[1,2,3]. 하지만 아직 이 두 프로토콜이 IoT에 적용되기에는 보안 및 성능적인 측면에서 보완되어야 할 점이 많이 있다. 따라서 본 논문에서는 IoT를 위해 제시된 두 프로토콜 중 하나인 DTLS에 경량 암호와 Quantum Resistance를 가진 DTLS+를 제안하고자 한다.

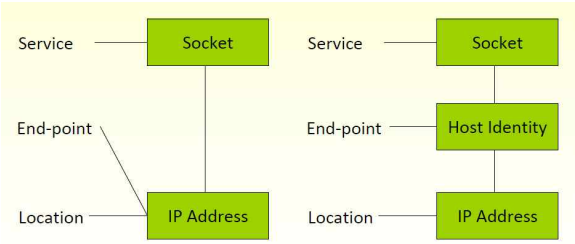
본 논문의 구성은 다음과 같다. 논문의 2장에서는 HIP와 DTLS에 대해서 알아보며 3장에서는 DTLS를 향상시키는 방법을 제시하고 이에 대해 설명하며 4장에서는 제시된 방법을 분석한다. 마지막으로 5장에서는 이에 대한 결론을 맺는다.

II. 배경 지식

2.1 HIP

HIP[4]는 IETF에서 1999년부터 개발되어 온 인터네트워킹 구조와 프로토콜 모음으로서, IP와 전송 계층 사이에 이름공간을 추가함으로써 원래의 인터넷 구조를 개선시킨 것이다. 이 새

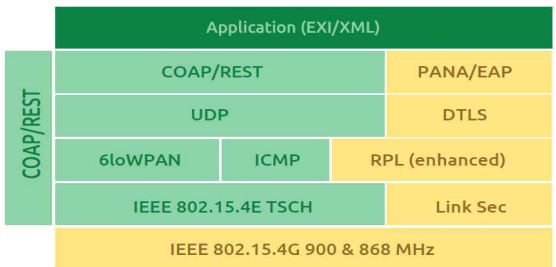
로운 구조는 공개키 기반의 ID를 사용하여 ID와 위치표시자를 구분하며, 기존의 인터넷과 호환성을 제공한다.[5] 이러한 기능을 제공함으로써 통신 중인 단말이 이동하거나 다른 링크로 통신을 재개하더라도 세션이 끊기지 않게 된다. 이렇게 새로운 이름공간과 프로토콜 계층을 추가함으로써 이동성, 보안성, 익명성을 제공한다.



[그림 1] HIP가 추가된 프로토콜 스택

2.2 DTLS

DTLS[6]는 Transport layer의 TCP 프로토콜에 보안성을 제공해주는 TLS (Transport Layer Security) 프로토콜을 UDP에 적용가능하게 해주는 UDP를 위한 보안 프로토콜이라 할 수 있다. 그러므로 UDP기반의 애플리케이션들은 이 DTLS를 사용함으로써 도청, 간섭, 메시지 변조 등 네트워크상에서 발생할 수 있는 공격들을 막을 수 있다. 특히나 UDP를 사용하는 IoT에 보안성을 추가해 줄 수 있는 프로토콜로 제시되고 있다. [그림 2]는 무선 디바이스 상에서의 프로토콜 구조를 나타내고 있다. 그림에서 볼 수 있듯이 UDP를 사용하기 때문에 DTLS를 사용하는 것을 볼 수 있다. 이러한 점은 IoT 환경에서도 적용이 된다고 할 수 있다.



[그림 2] 무선 디바이스 상에서의 프로토콜 구조

III. 제안 기법

먼저 HIP와 DTLS상에서의 보안 문제점을 설명하고 다음으로 본 논문에서 제시하고자 하는 DTLS+에 대하여 기술하고자 한다.

3.1 HIP와 DTLS에서의 보안 문제점

HIP와 DTLS가 IoT 환경에서 사용하기 위해 제시되고 있지만 두 프로토콜에서 보안문제가 보고되고 있다. 먼저 HIP에서는 서버와 클라이언트가 보안채널로 통신을 한다고 해도 변조된 클라이언트라면 보안채널을 통해 공격이 가능하며[7], 서버 관리자가 모든 권리를 가지고 있기 때문에 만약 서버가 변조 되면 HIP를 사용하는 시스템 전체가 취약해지는 문제점이 있다. 또한 이 외에도 HIP 디자인상의 문제, 구현상의 문제 등 여러 가지 취약점이 보고되고 있다.

DTLS는 TLS를 기반으로 설계된 프로토콜이기 때문에 보통 TLS를 사용하기 위해 OpenSSL을 사용하는 것처럼 DTLS를 사용하고자 하는 유저들은 OpenSSL을 사용한다. 그러므로 OpenSSL상에서의 취약점도 그대로 DTLS에서도 나타나게 된다. 특히나 최근 2014년에 Heartbleed 취약점, Recursion flaw 취약점, Invalid fragment 취약점[8] 등 많은 취약점이 보고되고 있고 이러한 취약점은 고스란히 DTLS를 기반으로 한 IoT 디바이스에 적용되므로 쉽게 공격에 대상이 될 수 있다.

3.2 경량 암호 알고리즘

DTLS에서 사용되는 대표적인 암호 알고리즘은 AES 알고리즘이라고 할 수 있다. 하지만 이 AES 알고리즘은 자원이 제한적인 IoT 디바이스에 사용하기에는 비용과 성능 면에서는 부적합하다고 할 수 있다. 최근에 제시된 LEA[9] 알고리즘은 AES 보다 빠른 연산속도를 가지지만 일부 보고서에서는 IoT 환경에 적용은 지속적인 검토가 요구된다고 보고 있다. 그러므로 본 논문에서는 DTLS에서 ChangeCipherSpec의 암호 알고리즘중 하나로 기존의 경량 암호 알고리즘으로 제안된 PRINCE 알고리즘[10] 및 개량된 Extended PRINCE[11]를 사용할 것을 제안한다. PRINCE는 다른 알고리즘에 비해 하드웨어 최적화가 잘 되어 있는 알고리즘이라고 할 수 있다. PRINCE를 하드웨어로 구현 시 AES-128보다 면적 부분에서 최대 16.35배 정도의 면적을 덜 차지하며 전력 부분에서는 최대 84.8배 정도

전력을 덜 소비한다. PRINCE는 다른 암호 알고리즘인 PRESENT, LED에 대해서도 마찬가지로 면적과 전력 면에서 우수한 성능을 보여주고 있다. 이러한 부분에서 PRINCE는 IoT 디바이스에 사용하기에 알맞은 경량 알고리즘이라고 할 수 있다.

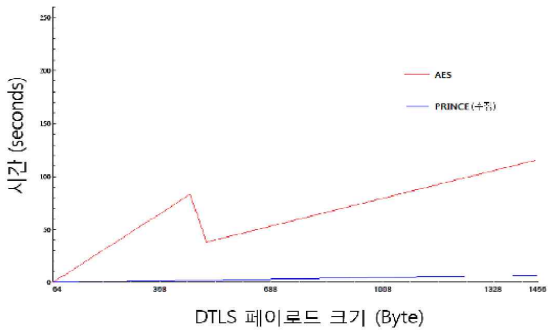
3.3 Quantum Resistance

DTLS를 이용한 IoT 환경에서는 handshake 과정을 이용하여 상호인증을 할 수 있는데 이때 사용되는 알고리즘으로는 RSA, Diffie-Hellman, Elliptic Curve Diffie-Hellman 같은 공개키 암호 시스템이 사용된다. 하지만 이러한 공개키 암호 시스템은 양자 컴퓨터 공격에 대해 안전하지 못하다. 그러므로 양자 컴퓨터에 대한 안전성을 보장하기 위해 DTLS에 양자 컴퓨터 내성이라고 할 수 있는 Quantum Resistance 특징을 가진 인증 프로토콜을 추가해야 한다. 이를 위해 본연구실에서 연구된 양자 컴퓨터 공격에 견딜 수 있는 LPN (Learning Parity with Noise) 기반의 O-FRAP (Optimistic Forward secure RFID Authentication Protocol)를 DoS 공격에 방어 할 수 있도록 발전시킨 O-FRAP^{+} [12]나 본 연구실에서 연구하고 있는 Ring-LPN 문제 기반의 Lapin*[13]를 사용한다. O-FRAP^{+}는 인증 프로토콜로 자원이 제한적인 RFID 시스템에서 사용할 수 있도록 제안된 프로토콜이며 이 프로토콜은 상대적으로 낮은 연산량을 가지고 있어 다른 인증 프로토콜에 비해 경량화 된 프로토콜이라 할 수 있다. O-FRAP^{+}는 LPN을 기반으로 하므로 Quantum Resistance를 가진다. 또한 본 연구실에서 연구 중인 Ring-LPN 기반의 Lapin*는 O-FRAP^{+}처럼 경량 암호 인증 프로토콜이며 이 또한 양자 컴퓨터 공격에 대비할 수 있는 프로토콜이므로 Quantum Resistance를 가지게 되어 미래의 양자 컴퓨터 공격에 대비할 수 있다.

IV. 분석

[표 1] 은 본 논문에서 제시된 DTLS+와 기존의 IoT를 위한 프로토콜로 제시된 HIP와 DTLS를 비교한 표이다. [표 1] 을 통해 기존의 DTLS의 특징은 유지하면서 인증 암호화가 수정되고 Quantum Resistance가 추가된 것을 확인 할 수 있다. 이에 대한 분석 결과는 아래와 같다.

첫 번째로 DTLS의 암호화 프로토콜로 PRINCE 알고리즘이나 개량된 알고리즘인 Extended PRINCE를 사용함으로써 기존의 AES 알고리즘과 다른 암호 알고리즘이 가지지 못한 면적과 전력 측면에서 이점을 가졌다는 것이다. 또한, [14]에서 PRINCE가 AES보다 블록 처리 속도에서 약 17배정도 빠른 것으로 분석된다. [그림 3] 은 이러한 결과를 바탕으로 AES와 PRINCE를 DTLS 페이로드 크기가 증가함에 따라 암호화 되는데 걸리는 시간을 비교한 그림이다.



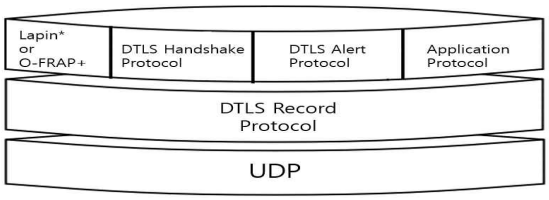
[그림 3] AES와 PRINCE 암호화 시간 비교

[그림 3] 을 통해 PRINCE가 비록 추정치이긴 하지만 AES보다 더 빠르게 암호화를 할 수 있음을 기존의 결과를 바탕으로 유추할 수 있다. 이렇게 PRINCE는 저전력 저면적에 사용할 수 있고 암호화 속도 역시 빠르므로 자원이 제한되어 있는 IoT 환경의 매우 적합한 알고리즘이라고 할 수 있다.

두 번째로 Quantum Resistance를 추가함으로써 미래에 발생할 수 있는 양자컴퓨터에 대한 공격에도 대비한 것이다. [그림 4] 는 O-FRAP^{+}/Lapin*가 추가된 DTLS의 구조를 나타낸 것이다. 기존의 인증 방법으로 사용된 handshake는 유지하면서 고유의 인증방식을 추가하고 여기에 HIP와 기존의 DTLS에는 존재하지 않는 특징으로 양자 컴퓨터 공격에 견딜 수 있는 Quantum Resistance를 추가하였다고 할 수 있다. 이처럼 기존의 프로토콜이 갖지 못한 Quantum Resistance 특징이 추가됨으로써 장기간 보안성을 보장한다. 또한 두 프로토콜 모두 초기에 자원제한적인 디바이스를 겨냥하여 만들어진 혹은 연구되고 있기 때문에 IoT 환경에 알맞은 프로토콜이 될 것이라 생각된다.

구 분		HIP	DTLS	**DTLS+**
보안성	인증 암호화	X	AES-{GCM,CCM}	**PRINCE/ Extended PRINCE**
	상호 인증 여부	O	O	**O**
	공개키 암호 사용 여부	O	O	**O**
	대칭키 암호 사용 여부	O	O	**O**
	Quantum Resistance	X	X	**O**
	키 공유 방식	Diffie-Hellman	PKI	**PKI**
호환성	IoT 네트워크 적용	어려움	쉬움	**쉬움**

[표 1] DTLS+와 HIP, DTLS 비교



[그림 4] O-FRAP+/Lapin*가 추가된 DTLS

V.결론

본 논문에서는 IoT 환경을 위한 DTLS의 향상 방법에 대해 제안하고 있다. 비록 제안된 기법들은 아직 구현되지 않은 상황이라 제안된 기법들이 얼마나 효율성을 가질 수 있는지 확인을 하기는 어려우나 경량 암호 및 인증 프로토콜이므로 성능 면에서 개선효과가 있을 것이라 생각된다.

향후 연구에서는 이 논문에서 제안된 기법들을 실제로 구현하고 기존 DTLS보다 얼마나 개선되었고 IoT 환경에 적합한지 판단하는 연구가 필요하다.

[참고문헌]

[1] Oscar Garcia-Morchon et al. “Securing the IP-based Internet of Things with HIP and DTLS” ACM WiSec 2013. April 17-19, 2013, Budapest, Hungary

[2] Hummen, R., Wirtz, H., Ziegeldorf, J. H., Hiller, J., &Wehrle, K. (2013). Tailoring end-to-end IP security protocols to the Internet of Things. In ICNP (pp. 1-10).

[3] Hummen R. Shafagh, H, Raza, S., Voigt, T., &Wehrle, K. (2014). Delegation-based Authentication and Authorization for the IP-based Internet of Things. In IEEE SECON.

[4] RFC 4347, http://tools.ietf.org/html/rfc6347

[5] Pekka Nikander, Andrei Gurtov, and Thomas R. Henderson, “Host Identity Protocol (HIP): Connectivity,Mobility, Multi-homing, Security, and Privacy over IPv4 and IPv6 Networks,” IEEE Communication Survey & Tutorial, 2010, 4

[6] RFC 4423, http://tools.ietf.org/html/rfc4423

[7] Sääskilahti Juha, and Mikko Särelä. "Risk analysis of host identity protocol: using risk identification method based on value chain dynamics toolkit." Proceedings of the Fourth European Conference on Software Architecture: Companion Volume. ACM, 2010.

[8] CVE List, https://cve.mitre.org

[9] Lee Donggeon, et al. "Efficient Hardware Implementation of the Lightweight Block Encryption Algorithm LEA." Sensors 14.1 (2014): 975-994.

[10] Julia Borghoff, *et al,* “PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications”, Advances in Cryptology - ASIACRYPT2012, Springer, pp.208-225, 2012.

[11] HakJu Kim and Kwangjo Kim, “Toward an Inverse-free Lightweight Encryption Scheme for IoT,” 2014 Conference on Information Security&Cryptography, Dec. 6, 2014

[12] Dang Nguyen Duc and Kwangjo Kim, "Defending RFID Authentication Protocols against DoS Attacks", Computer Communications, Vol. 34, No. 2, pp.384-390, 2011.

[13] 최락용, 김광조, “IoT 환경에서의 Ring-LPN을 이용한 경량 인증 방법”, 2014년 한국정보보호학회 동계학술대회, 2014년 12월 6일

[14] Doröz, Yarkin, et al. "Toward Practical Homomorphic Evaluation of Block Ciphers Using Prince." IACR Cryptology ePrint Archive 2014 (2014): 233.