韓國 컴퓨터情報學會 論文誌
第8卷 第3號, 2003. 9.

2003-8-3-3-2

낮은 계산량을 이용한 효율적인 WTLS 시스템 구현에 관한 연구

정 우 열*

A Study on the Effective WTLS System Implementation using Low-Computation

Woo-Yeol Jeong*

요 약

정보통신과 네트워크의 발전으로 인하여 유/무선망의 통합이 일반화되어가고 있다. 이러한 시점에서 무선환경에서 데이터 통신을 위한 프로토콜로서 WAP이 사용되고 있다. 이러한 WAP에서 안전한 통신을 위하여 개발된 WTLS는 인터넷 프로토콜인 TCP/IP에서 사용되는 TLS를 무선환경에 맞도록 최적화한 것이다. 그러나 WTLS는 WAP 보안문제, 종간 문제, 소비전력 등의 문제점을 가지고 있다. 그러므로 본 논문에서는 WTLS의 단점들을 없애고자 WTLS에 사용되는 암호알고리즘을 제안하였다. 제안된 알고리즘은 단일형태가 아닌 혼합형 알고리즘을 사용하기 때문에 계산상의 복잡도를 줄여 소비전력 및 보안문제를 해결할 수 있다.

Abstract

With information communications and network environments merged wire/wireless networks are generalized. In this viewpoint, WAP is used by communication protocol for the data communication in the field of wireless environment. WTLS developed for the secure communications optimize TLS adapted wireless environment in the TCP/IP internet protocol. But WTLS denote WAP security problem, end-to-end problem, and power consumption, etc. Therefore in this paper we proposed WTLS cryptographic algorithm eliminated WTLS disadvantages. Proposed algorithm solved power consumption, calculated complexity, and security problems because it is not unique but hybrid form.

▸ Keywords : WAP, WTLS, security protocol, high performance

* 한려대학교 멀티미디어정보통신공학과 교수

Ⅰ. 서 론

정보통신의 발달은 다양한 정보의 전송이 필수불가결하며 이러한 정보 전송은 네트워크의 발전을 의미하며 네트워크의 발전은 정보보호기술의 대두를 가져온다. 특히 무선망에서의 인터넷의 사용은 PDA와 같이 인터넷 휴대단말기의 응용서비스 증가를 가져왔다. 이러한 무선 인터넷 단말기의 원활한 사용을 위하여 무선망 프로토콜을 원하게 되었으며 이러한 원인이 배경이 되어 WAP(wireless application protocol)이 등장하게 되었다.

WAP은 WAP 포럼에서 표준화하고 있는 무선 인터넷 환경에서 동작하는 무선망 프로토콜이다. 이러한 WAP의 특징은 무선단말기에서 사용되는 프로토콜이므로 소비전력, 사용 메모리 등과 같은 파라미터에 의하여 유선 인터넷망에서 사용되는 프로토콜과는 다소 차이가 있다[1].

WAP은 무선단말기에 대한 프로토콜이므로 일반적인 프로토콜과 유사하다. 그러나 보안에 관련된 역할은 WTLS(wireless transport layer security)를 사용한다. WTLS는 보안사항에 대하여 무선망에 적합하도록 구성된 프로토콜로서 WAP 단말기와 WAP gateway사이의 보안에 관련된 기능을 수행하게 된다[1][2].

이러한 기능을 수행하게 되는 WTLS는 무선 단말기에 대한 실제적인 무선망 보안을 취급하기 때문에 무선 단말기의 성능과 직결된다. 즉 단말기에서 소비되는 전력, CPU 속도, 전송율 등으로 인하여 WTLS의 효율이 결정된다. 그러므로 본 논문에서는 WTLS의 효율을 증대시키고자 기존 WTLS에 사용되는 암호알고리즘 대신에 혼합형 암호알고리즘을 사용하였다. 혼합형 암호알고리즘이 포함된 WTLS는 기존 WTLS보다 암호화 수행에 걸리는 시간이 단축되었으며 전용 암호프로세서의 사용으로 인하여 시스템 소비전력은 OS 프로세서에 의한 CPU사용의 점유율을 낮출 수 있기 때문에 소비되는 전력측면에서 유리하다.

Ⅱ. WTLS 알고리즘 및 특징

WTLS는 인터넷 프로토콜인 TCP/IP의 보안에 사용하는 TLS(transport layer security)를 무선환경에 맞도록 최적화한 것으로서 TLS가 수행하는 기능을 모두 수행하게 된다. <그림 1>은 WTLS가 수행하는 위치를 보여주고 있다.

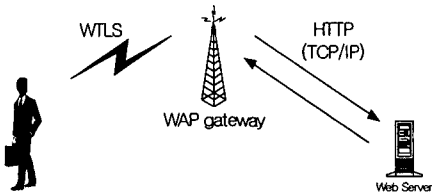

그림 1. WAP 프로토콜
Fig. 1 WAP protocol

WTLS는 <그림 1>과 같이 WAP gateway와 무선 단말기사이에 존재하는 프로토콜이다. 일반적으로 WAP에서의 보안은 WTLS와 SSL/TLS가 사용되며 WAP gateway에서 서로 다른 프로토콜 스택 변환이 발생한다. 이때 WAP 게이트웨이에서 프로토콜 변환을 위해 송신자의 데이터를 복호화하여 수신자의 프로토콜로 다시 암호화하게 되는데 이때 원래의 평문이 노출될 가능성이 있다. 이러한 노출가능성은 WTLS와 SSL/TLS와는 무관하게 동작하므로 WAP 프로토콜의 단점으로 동작하게 된다[3][5].

일반적으로 유선망과 무선망에서의 보안은 SSL/TLS와 WTLS가 담당하게 되는데 이때 WTLS는 TLS를 기본으로 업그레이드 된 것이므로 기본적인 기능은 동일하다. 그러나 무선망에 대한 보안을 담당하게 되는 WTLS는 TLS가 가지지 못한 기능이 몇 가지 보충되어 있다.

WTLS는 WDP(wireless datagram protocol)에서 datagram transport를 지원하기 때문에 datagram의 중복, 분실, 데이터 순서의 뒤바뀜 등을 체크할 수 있도록 sequence number를 record layer의 header에 explicit field로 사용한다. 또한 WTLS는 무선망에서 사용되는 프로토콜이므로 idle time이 유선망에 비하여 매우 길다. 또한 전송속도 및 한정된 채널로 인하여 전송 데이터량을 최소로 해야 한다.

WTLS의 가장 큰 단점중의 하나는 단말기의 프로세서 및 인터페이스 전력소비문제이다. 그러므로 사용하는 알고리즘에 제약이 따른다. 그러므로 연산량이 많거나 메모리를 많이 사용해야하는 암호알고리즘은 WTLS 프로토콜을 사용해야하는 시스템에는 부적합하다는 것이다. 그러나 비도측면에서 보면 보안에 매우 좋지 못한 경우이다.

WTLS는 〈그림 2〉와 같은 구조를 가지고 있으며 상위에는 Handshake, Change Cipherspec., Alert, Application data 프로토콜로 구성되어 있으며 이러한 프로토콜들은 하위의 Record layer 프로토콜을 거치게 된다.

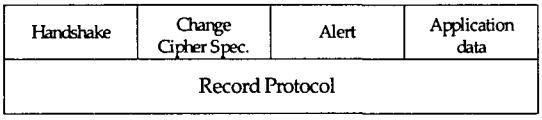

그림 2. WTLS 구조
Fig. 2 WTLS architecture

Record layer에서 사용되는 알고리즘들은 서버와 클라이언트의 결정에 의하여 security parameter로 유지된다. Handshake에서는 서버와 클라이언트가 Record layer에서 사용할 암호 알고리즘을 포함한 security parameter를 설정하게 된다.

WTLS는 session과 connection에서 state를 유지해야하는 stateful 프로토콜이다. 이때 실제적인 통신이 이루어지는 단위는 connection이며 여러 개의 connection이 모여 하나의 session을 구성하게 된다. state는 pending state와 current state로 나뉘어져 있고 각 state는 read state와 write state의 세부 state로 분류된다. pending state는 서버와 클라이언트에 의하여 결정된 암호알고리즘과 키 블록을 임시 저장해 놓는 state이고 record layer에서 실제 데이터가 처리될 때 항상 current state의 알고리즘과 키를 사용한다.

〈그림 3〉은 WTLS에 대한 state를 나타내고 있다. handshake 프로토콜 상에서 암호알고리즘을 포함한 security parameter의 세부 항목이 설정되면 설정된 내용은 record layer로 전달되어 키 블록을 생성하는 동시에 pending state에 저장된다.

저장된 pending state는 change cipher spec. 프로토콜에 의하여 current state로 옮겨진다. current state로 옮겨지면 pending state는 NULL 상태로 초기화된다. 이때 change cipher spec. 메시지를 보내면 pending write state가 current write state로 바뀌고 change cipher spec. 메시지를 받게 되면 pending read state가 current read state로 바뀐다.

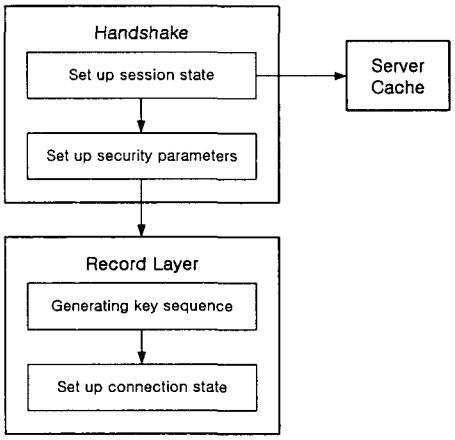

그림 3. WTLS state
Fig. 3 WTLS state

이와 같은 동작을 수행하는 WTLS는 별도의 압축알고리즘을 사용하지 않고 NULL 알고리즘만을 지원한다. WTLS는 key block에서 sequence number를 별도로 세팅되는 것이 아니고 PRF(pseudo-random function)의 입력에 포함되어 있다. 이와 동시에 WTLS의 key block은 handshake 과정에서 설정된 key refresh에 따라서 일정주기마다 새로운 데이터 블록을 생성하게 된다[6].

key block이 key refresh마다 새롭게 업데이트 되는 것과 같이 datagram transport를 지원하는 WTLS에서 IV 역시 각 record 마다 새롭게 설정된다.

〈그림 4〉는 WTLS의 record layer와 헤더 포맷을 보여준다.

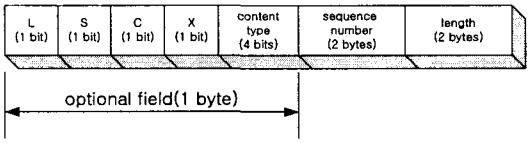

그림 4. WTLS record layer 포맷
Fig. 4 WTLS record layer format

'L'비트는 length field indicator로서 '1'인 경우 length field를 포함하고 있음을 알려준다. 그러므로 수신자가 전송 데이터의 길이를 알고 있거나 전송 데이터의 마지막 record일 경우에는 '0'이 된다. 그러나 그렇지 않은

경우, 즉 전송 데이터들이 연접된 경우에는 반드시 length field가 포함되어 있어야 한다. 'S' 비트는 sequence number field indicator로 사용되는 비트이다. 이때 S의 값이 '1'일 경우 sequence number field를 포함하고 있음을 알 수 있다. 'C' 비트는 cipher spec. indicator로서 current cipher spec.을 나타낼 때 사용된다. 'X' 비트는 reserved이며 나머지 4비트는 content type을 나타낸다.

III. 저전압, 저복잡도를 가지는 WTLS

무선단말기에서 사용되는 WTLS에 대한 저전압 및 계산상의 저복잡도는 단말기 수명과 직결되는 문제이다. 그러므로 WTLS를 구현할 때 저전압 및 계산상의 간소화는 시스템 효율을 결정짓는 중요한 파라미터가 된다.

WTLS는 TLS에서 사용되던 RSA, DH를 사용하지 않고 저 복잡도 및 저전압을 위하여 ECDH 알고리즘 및 RSAx를 사용한다. 그러나 ECDH 역시 대칭형 암호알고리즘에 비하여 계산상의 복잡도가 매우 높다.

그러므로 본 논문에서는 대칭형 암호알고리즘을 적용한 혼합형 암호알고리즘을 사용하여 WTLS에 적용하였다.

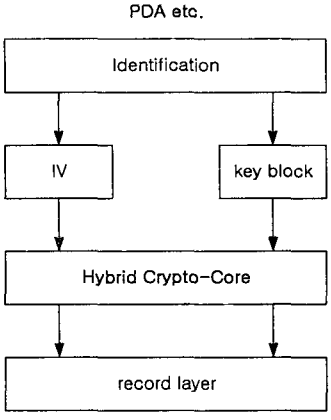

그림 5. 제안된 WTLS 암호시스템
Fig. 5 Proposed WTLS crypto-system

〈그림 5〉는 기존 WTLS에 제안된 혼합형 암호방식을 적용한 단말기 암호시스템으로서 무선단말기가 기본적으로 가지고 있는 ID를 이용하여 IV와 key block을 생성하고 생성된 IV 및 key block을 이용하여 hybrid crypto-core의 입력으로 사용한다.

$$ID \rightarrow IV_n \rightarrow Initial\_seed \rightarrow PRF(PRN) \rightarrow Initial\_key\_block \rightarrow key\_block_n(IV_n) \quad \cdots\cdots (1)$$

식 (1)에서 ID와 Initial_seed, Initial_key_block을 이용하여 sequence number를 생성한다. 이때 ID는 Initial_seed와 Initial_key_block을 생성하는 기본재료로 사용된다.

PRF(PRN)과 $key_block_n(IV_n)$은 혼합형 암호시스템의 입력으로 사용된다.

기존 TLS 또는 WTLS는 IV에 대한 생성방법 및 사용을 XOR을 이용하여 record마다 새롭게 갱신하였다. 이와 같은 방법을 적용하기 위하여 PRF(PRN)과 $key_block_n(IV_n)$을 스트림 형태로 표현하면 식 (2)와 같다.

여기에서 PRF(PRN)에 대한 초기 데이터는 $P=\{p_0, p_1, \cdots, p_{62}, p_{63}\}$, key block에 대한 데이터 $K=\{k_0, k_1, \cdots, k_{62}, k_{63}\}$ 이다.

$$record\ event <= P(MSB) \oplus K(MSB) \text{ and } P(LSB) \odot K(LSB) \quad \cdots\cdots (2)$$

기존 WTLS가 RSAx 또는 ECDH 암호알고리즘을 사용하는 이유는 상대방에 대한 인증기능 때문이다. 그러므로 본 논문에서 인증에 관련된 기능은 ID에 의한 특정포맷을 이용하여 인증 데이터를 생성한다.

식 (3)은 record가 변화될 때마다 새로운 인증데이터를 생성하고 생성된 인증데이터를 식 (2)에서 발생되는 암호문과 합하는 기능을 수행한다.

$$record\ event\ and\ Auth. = P(MSB) \oplus K(MSB) \text{ and } P(LSB) \odot K(LSB) \text{ and } Auth. \quad \cdots\cdots\cdots\cdots (3)$$

여기에서 and는 &와 같이 단순 결합을 의미하며 ⊕는 비트들끼리의 XOR, ⊙는 비트들끼리의 XNOR 연산을 의미한다.

식 (3)에서와 같이 XOR, XNOR의 연산이 bit by bit 연산을 기본으로 수행하기 때문에 각 스트림들에 대한 연산은 가중치(weight)가 없는 단순 2진 데이터 연산이다. 이러한 단순연산의 결과 산출되어지는 데이터 스트림은 사용목적에 따라 별도의 포맷을 수행하게된다. 즉 데이터 암호용으로는 XOR, XNOR연산의 결과값을 사용하며 인증용으로는 Auth.의 값을 사용하게 된다.

〈그림 6〉은 채널상에서 제안된 혼합형 암호시스템에 대한 프로토콜이다. 암호를 수행하는 부분은 블록 암호알고리즘을 사용하며 인증용으로는 스트림방식인 PRF를 사용하도록 하였다. 이때 사용되는 PRF의 초기값과 블록 암호시스템에서의 초기값은 ID 포맷팅에 의한 값을 사용하도록 함으로서 역변환 및 인증기능이 수월하도록 하였다.

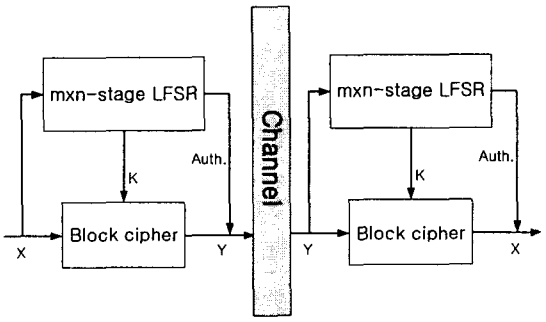

그림 6. 제안된 WTLS 혼합형 암호시스템
Fig. 6 Proposed WTLS hybrid crypto-system

Ⅳ. 대칭형 기반 WTLS 암호시스템 설계

대칭형 기반 WTLS 암호시스템은 ID에 의한 데이터 포맷팅 과정을 수행하는 부분과 PRF 및 블록 암호부분으로 분류된다.

〈그림 7〉은 실제적인 데이터들에 대한 암호화를 수행하는 부분으로서 블록암호시스템으로 구성되어 있다. 입력은 64 비트가 기본 크기이며 128 비트로 동작할 수 있도록 외부 인터페이스 부분에서 조절이 가능하도록 하였다.

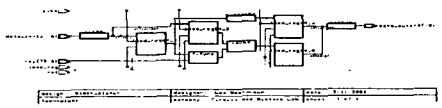

그림 7. 데이터 암호블록
Fig. 7 Data crypto-block

〈그림 8〉은 데이터 암호블록에 대한 모의실험 결과를 나타내고 있다.

이때 입력데이터는 "0123456789ABCDEF0123456789ABCDEF"이며 키값은 "00104408 80FF10014418 81FF" 이다. 암호화된 데이터는 "AA808D8D82080FAD7072FF55D0587775"이다.

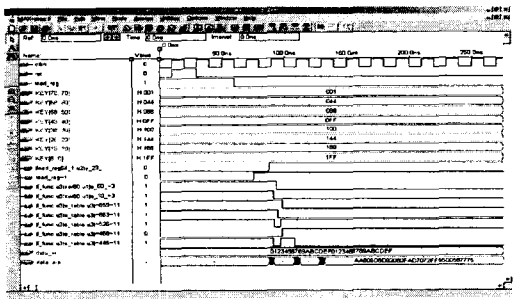

그림 8. 데이터 암호블록 모의실험 결과
Fig. 8 Simulation of data crypto-block

Ⅴ. 결론

무선단말기의 보안유지를 위하여 사용되는 WTLS는 인터넷 표준인 TLS를 무선채널에 적합하도록 변형한 프로토콜이다.

WTLS는 무선단말기의 기종에 상관없이 WAP를 지원할 수 있도록 데이터그램 전송을 지원하지만 무선채널환경의 열악함으로 인하여 커다란 효율증대는 어렵다. 그러므로 본 논문에서는 비대칭형 암호알고리즘에 기반을 둔 WTLS가 아닌 대칭형 기반 WTLS 시스템을 제안하였다.

대칭형 암호알고리즘의 장점인 처리속도, 단순한 계산 등은 WTLS의 저전력 및 계산량의 복잡도등을 개선할 수 있으며 이로 인하여 보다 높은 비도 제공 및 대용량의 데이터들을 실시간으로 전송할 수 있다는 장점을 가진다. 또한 WTLS의 하드웨어 구현은 무선채널 상에서 제약조건이었던 메모리 크기, 전력소비, 전송대역폭, 전송속도 등을 향상시킬 수 있으며 무선 단말기들에 대하여 적용이 용이하다는 장점을 가진다.

그러므로 제안된 하드웨어 대칭형 기반 WTLS 시스템은 대용량 및 실시간 처리가 무선인터넷 환경 속에서 가능하도록 해법을 제시할 것으로 사료된다.

참고문헌

[1] O. Goldreich, "Two Remarks Concerning the Goldwasser-Micali-Rivest Signature Scheme", In Proceeding CRYPTO'86, Lecture Notes in Computer Science No. 263, Springer-verlag, 1987, pp. 104-110

[2] O. Goldreich, L. A. Levin, "A Hard-core Predicate for All One-Way Functions", Proceedings of the 21st ACM Symposium on Theory of Computing, 1989, pp. 25-32

[3] S. Goldwasser, S. Micali, R. L. Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen Message Attack", SIAMJ. On Computing, Vol. 17, No. 2, 1988, pp. 281-308

[4] R. Lmpagliazzo, M. Naor, "Efficient cryptographic schemes probably as secure as subset sum", In 30th Annual Symposium on Foundations of Computer Science, IEEE. 1989. pp. 236-241

[5] R. J. McEliece, "A Public-key Cryptosystem based on Algebraic Coding Theory", DSN Progress Report 42-44, Jet Propulsion laboratory

[6] M. Naor, M. yung, "Universal One-Way Hash Functions and their Cryptographic Applications", In Proceedin· 21st ACM Symposium on Theory on Computing, 1989, pp. 33-43

저 자 소 개

정 우 열

1995. 3 ~ 현재 한려대학교 멀티미디어정보통신공학과 교수