SDR(Software Defined Radio) System 적용을 위한 한국형 암호 알고리즘 (SEED) 구현 및 성능분석

홍성룡[O] 조성호
{jackcom[O], shcho}@casp.hanyang.ac.kr

Sung Yong Hong[O] Sung Ho Cho
Dept. of Information & Communications Hanyang University

요 약

IMT2000다음으로 개방형 구조를 갖는 차세대 통신 시스템(SDR:Software Defined Radio)에 적용할수 있는 정보보안 메커니즘으로 블록암호화 알고리즘인 ' SEED' 를 구현하였다.SDR의 플랫폼은 주로 프로그래머블(Progammable)한 FPGA나 DSP가 주를 이루는데,본 논문은 이러한 SDR 시스템 대상으로 적용할수 있는, 한국형 블록 암호 알고리즘인 ' SEED' 를 DSP,FPGA로 구현하고 성능비교,분석을 통하여 효과적이고 합리적인 SDR 암호화 모듈 구현의 방향을 모색해 보았다.

1. 서 론

정보화 물결과 더불어 산업 및 사회 전반에 걸쳐 정보의 의존성은 점점더 심화되고 있다.특히 인터넷을 기반으로 대량의 정보교환과 통신 서비스는 활발하게 이루어지고 있고 이들간의 정보보호 메커니즘은 정보통신의 신뢰성 있는 정보교환의 근간을 만들어 준다.

최근 많은 연구가 진행되고 있는 개방형 구조를 갖는 차세대 통신 시스템(SDR: Software Defined Radio)의 핵심기술은 DSP나 FPGA 와 같은 프로그래머블 디바이스를 사용함으로써 좀더 많은 유연성과 다양한 어플리케이션을 가능케 해 준다.즉 기능(function)이나 시스템의 스펙(Specifications)의 커다란 변화를 더 이상 요구하지 않게 되었다.이 같은 기술은 가까운 미래에 Wireless의 표준으로 자리 잡히게 될 것이며 관련된 많은 소프트웨어적인 기술을 필요로 하게 될 것이다.보안의 관점에서 보아도 이 같은 유연성은 동일하게 적용이 될 것이다.보안은 지속적인 업그레이드와 관리가 필요한 부분이기 때문에 이는 이와 같은 유연성을 제공해 줄 수 있는 기반구조가 필요하다.이에 SDR 시스템의 플랫폼구조는 가장 좋은 환경이라고 할 수 있다.

따라서 본 연구에서는 이 같은 ' 시스템의 유연성' 관점에서 SDR에 적용가능 암호화 알고리즘을 선택하고 이에 대한 시뮬레이션을 통해서 그 효과와 합리성을 따져 보았다.또한 최근 각광을 받고 있는 SOC 솔루션으로 그 구현 방향을 고려 해 봄으로써 그 구현의 적용방안을 넓혀 보았다.본 연구의 시뮬레이션을 위한 암호화 알고리즘으로는 한국형 암호알고리즘의 표준인 SEED을 선택하여 보안의 측면에서 보다 높은 비도를 가져올수 있으며 DSP와 같은 고속연산의 장점을 가지고 있는 프로그래머블 디바이스를 사용함으로 그 효율성을 극대화 시켰다.사실 종래의 무선환경에서는 이 같은 암호 알고리즘이 차지하는 많은 연산능력(Computation Power)의 필요에 의해 그 구현이 비교적 용이하지가 못했다.주로 통신시스템을 위한 독립장비(Stand-alone)에서는 고 성능을 발휘하는 CPU를 사용함으로써 그 구현의 토대가 이루어 졌지만 이러한 방법은 지속적인 업그레이드와 다양한 어플리케이션의 선택의 범위가 넓은 SDR 시스템에서는 바람직한 방법이라 할 수 없다.이는 많은 전력소비를 가져 오기 때문이다.DSP나 FPGA에 그 구현의 근간을 두고 있는 SDR 에서는 다행이도 이 같은 기존 요구사항들을 해결해 줄 수 있는데 본 연구에서는 이런 SDR 시스템에 적용 가능하도록 한국형 암호 알고리즘 SEED를 다양한 플랫폼환경에서 구현을 하고 성능 비교,분석을 함으로써 그 효과성을 평가 하였다.

2. SDR(Software Defined Radio)

2.1 시스템 구성

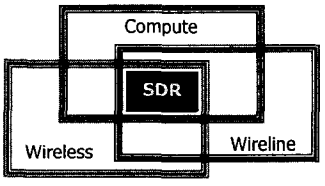

그림 1 SDR(Software Defined Radio)

SDR은 위 그림 1과 같이 소프트웨어로 대체를 함으로써 해외 어느 곳에 있더라도 하나의 단말기로 2G와 3G는 물론 xDSL, CDMA, GSM, UMTS, cdma2000, 무선LAN, 블루투스, 위성통신 등 다양한 통신망을 넘나들며 통신을 하는 개방형 구조의 차세대 통신 시스템이라고 할 수 있다.

보안의 측면에서 이 SDR 시스템을 Black Side와 Red Side로 구분을 짓는데 암호화된 부분들을 Black side라 하고 그렇지 않은 정보가 노출된 부분들을 Red side라고 한다.이를 INFORSEC 요소라 하는데 이 단은 암호화 뿐만 아니라,그것과 관련된,전체적인 정보의 조합도 필요하다.단말기의 인증시에도 INFOSEC단에서 처리해야 할 인증의 개수나, 계산량 등을 고려해서 그 수용성을 판단 하도웨어를 선택해야 한다.[1]

그림 2는 프로그래머블 디지털 radio로써 Black, Red 영역의 명확한 경계를 보여준다.

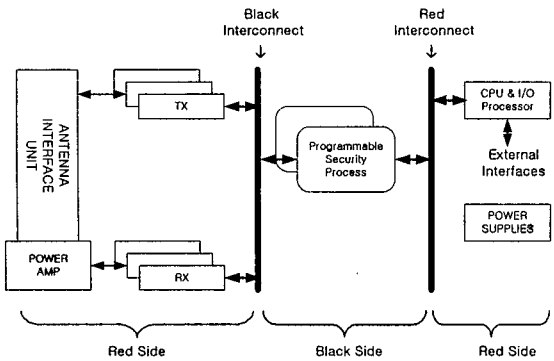

그림 2 Black/Red 영역

3. Security Algorithm

3.1 Digital Encryption

Radio Communication의 주요한 필요조건은 원래의 정보(Information)를 상대방으로 하여금 인지할수 없도록 Digital 로 변환하여 데이터를 변형하고 이를 인증된 사용자에게만 제공할수 있어야 한다.그림 3은 아주 개념적인 Digital encryption의 원리를 간략하게 보여주고 있다.

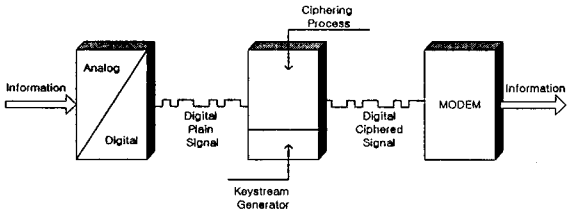

그림 3 The Principle of digital encryption

3.2 Security of Existing Wireless Systems

기존 무선환경에서 사용되는 Security는 표-1과 같이 요약 될수 있다.무선환경에서의 보안핵심 요소는 Data Encryption과 authentication(인증)이라 할수 있다.

표 1 Security of Existing Wireless Systems

Item	Algorithm
User authentication	Hash function,block ciphers
authentication of Network operator/Service Provider encryption of user data	Same above (frequently not implemented) stream cipher(scrambling)
encryption of control channel	stream cipher (frequently not implemented)
hiding User ID	temporary ID

3.3 Block Ciphers

블록 암호 알고리즘은 대부분 Feistel 구조로 설계된다.(예: DES,FEAL,LOKI,Blowfish,Twofish,SEED 등).Feistel 구조란 각각 t 비트인 L_0, R_0 블록으로 이루어진 2t비트 평문 블록(L_0, R_0)이 r 라운드($r \geq 1$)를 거쳐 암호문 (L_r, R_r)으로 변환되는 반복구조를 말한다.즉, 평문 블록이 여러 라운드를 거쳐 암호화 되는 과정이다.

3.4 한국형 표준 암호 알고리즘 SEED

DES는 공표된 이래로 암호강도에 비해 키 길이가 너무 작다는 비판이 있어 왔다.이러한 DES를 안전하게 사용하기 위해서는 키 길이와 키 선택이 중요한데, 키 전수 탐색 방법(Brute-force)이나 차분해독법(DC:differential cryptanalysis),선형 해독법(LC:linear cryptanalysis)등의 공격으로부터 안전하려면 키 길이가 112비트 이상 늘려야 한다.따라서 한국형 암호 알고리즘인 128비트 Key를 사용하는 SEED는 기존 DES보다 좀더 높은 보안강도를 보여준다.또한 SEED 는 무엇보다도 한국형 암호 알고리즘의 표준이라는데 그 의미를 둘 수 있다.

다음 그림 4는 SEED알고리즘의 전체 블록도이다.

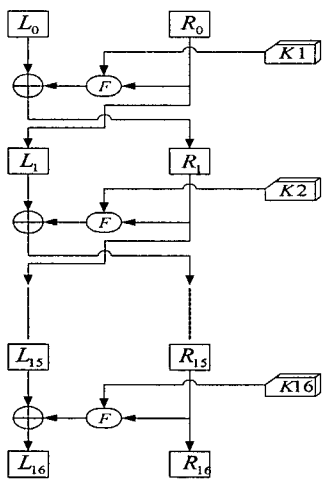

그림 4 SEED 전체 구조도

비록 SEED가 DES와 같은 구조로 알고리즘이 유사하나 DES가 XOR연산과 Permutation연산만을 사용하여 H/W구현상의 속도 향상을 가지는 반면 Adder와 G함수의 잦은 사용으로 전체적인 성능의 향상을 기대해 볼수 있다.

SEED가 가지는 G함수는 그림 5와 같고 이는 간략하게 확장 SS-Box들을 이용해서 다음과 같이 기술될 수 있다.

$$Z = SS_3(X_3) \oplus SS_2(X_2) \oplus SS_1(X_1) \oplus SS_0(X_0)$$

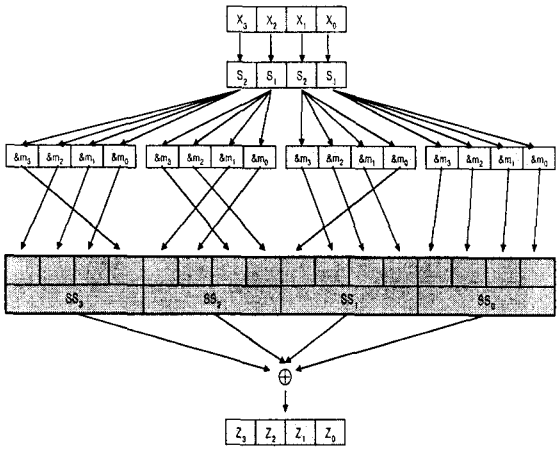

그림 5 SEED의 G함수

SEED의 라운드 키 생성과정은 128비트 암호키를 64비트씩 좌우로 나누어 이들을 교대로 8비트씩 좌/우로 회전이동한 후,결과의 4워드들에 대한 간단한 산술연산과 G함수를 적용하여 라운드 키를 생성한다.

즉,주어진 128비트 암호키 K=A‖B‖C‖D를 32비트 레지스터 A,B,C,D로 나눈다.각 라운드 i에 사용되는 라운드 키 $K_i = (K_{i,0}; K_{i,1})$는 다음과 같이 생성한다.

$$for(i = 1; i <= 16; i++)$$
$$\{$$
$$K_{i,0} \leftarrow G(A + C - KC_i);$$
$$K_{i,1} \leftarrow G(B - D + KC_i);$$
$$if(i\%2 == 1)\ A \| B \leftarrow (A \| B)^{>>8}$$
$$else\ \ C \| D \leftarrow (C \| D)^{<<8}$$
$$\}$$

4. 실험결과 및 고찰

표 2는 서로다른 플랫폼에서의 성능에 대한 비교를 보여준다. 또한 표 3은 각각 DSP와 FPGA,NIOS프로세서를 이용하여 시뮬레이션을 한 결과이다.

이는 DSP나 FPGA 의 저전력 소비와 유연성을 바탕으로 그 설계의 근간을 이룬다.고속연산과 쉽게 재 구성할 수 있는 잇점을 제공해 줌으로 SDR 시스템의 보안 메커니즘 구현의 한 부분을 구성할 수 있다.

표 2 구현을 위한 플랫폼 비교

Device	suitability for calculation	Power consumption	Flexbility
Pentinum III 800	fair	fair	excellent
FPGA	excellent	excellent	fair
DSP	good	good	excellent

표 3 다양한 플랫폼에서의 성능비교

Platform	Speed (msec/operation)	
	encryption	decryption
Pentinum III 800	0.23	10.2
FPGA	0.013	0.112
DSP	1.2	10.5
SOC(NIOS)	2.3	4.3

5. 결론

SDR Security시스템을 위한 대칭키암호 알고리즘인 한국형 표준 암호알고리즘 SEED를 적용하고 유연성을 평가하고자 SDR 핵심 솔루션인 DSP와 FPGA로 각각 그 구현과 성능평가를 기준으로 분석하였다.DSP는 유연성면에서 FPGA보다 우수하지만 처리속도면에서는 다소 그렇치 못함을 알수 있다.이러한 Trade-off는 적용 Application에 따라서 선택되어질수 있고 선택성을 가변적으로 설정함으로써 그 적용의 범위를 넓힐수 있다.또한 최근 SOC기술의 발달로 ASIC 타입이나 HDL 기반의 라이브러리 형태로 프로세서가 구성되고 사용자 로직이 더해지는 SOC 솔루션은 이런 유연성과 빠른 연산의 적정한 구현 방안이 될 것이다.

참고문헌

[1]Joseph Mitola 3 ' SOFTWARE RADIO ARCHITECTURE Object-Oriented Approaches to Wireless Systems Engineering' A Wiley-Interscience Publication,pp.221 2000

[2]' 128비트 블록암호 알고리즘 표준' 한국정보통신 기술협회(TTA),9,1999

[3] R.Stephen Preissig ' Data Encryption Standard (DES) Implementation on the TMS320C6000'