저전력을 소모하는 난수발생기의 성능 평가

윤정민[1], 김지홍[2], 김진효[3]

요약

휴대전화, PDA와 같은 이동 단말기와 무선 통신의 발전으로 인하여, 이동 단말기를 이용한 전자 메일, 게임, 주식거래 등이 가능하게 되었다. 무선 단말기를 통한 주식거래나 게임 등을 위하여서는 난수발생기(Random Number Generator)의 사용이 필수적이다. 그런데 최근까지의 난수발생기는 우수한 난수성에 중점을 두어 개발되었으며, 이동 단말기에서의 에너지 소비량에 대한 연구는 없었다. 이동 단말기는 무게 및 크기의 한계 때문에 배터리의 용량에 제한이 있게되므로, 되도록 에너지 소비량을 줄여서 주어진 배터리를 오랫동안 사용하기를 원하게 된다. 본 논문에서는 이동 단말기에서 많이 사용되는 여러 난수발생기들을 살펴보고, 저전력 에너지 측정도구인 SES(SNU Energy Scanner)를 이용하여 각 난수발생기의 에너지 소비량을 측정하여 이들을 비교한다. 이를 바탕으로 이동 단말기 환경에서 저전력을 소모하는 난수발생기를 제안하였다.

주요용어: 이동 단말기, 저전력, 난수발생기

제 1 절 서론

최근의 컴퓨터와 통신 기술의 급속한 발달과 더불어, 들고 다닐수 있는 작고 가벼운 이동 단말기들이 놀라운 속도로 증가하고 있다. 이동 단말기들과 무선 통신 기술의 발달에 의하여 휴대 전화기나 PDA등을 통하여 인터넷 쇼핑몰에서 쇼핑을 하거나 계좌 이체 및 전자 메일을 보내고 받는 등의 일은 흔한 일이 되어 버렸다. 많은 사람들이 PDA나 휴대 전화기를 이용하여 전자 메일을 보내고 받거나, 주식매매 등을 한 경험이 있을 것이다. 이러한 과정을 자세히 기억해보면, 그러한 활동의 중간에는 보안을 위하여 인증(authentication)을 받는 단계가 반드시 있었을 것이다. 이러한 인증단계에서, 일반적으로 비밀번호의 안전한 전송을 위하여 암호화 방법을 사용한다. 우리가 알고 있듯이 이러한 암호화 과정에서는 난

[1](151-742) 서울시 관악구 신림9동 산 56-1번지 서울대학교 전기,컴퓨터 공학부
twingo@davinci.snu.ac.kr
[2](151-742) 서울시 관악구 신림9동 산 56-1번지 서울대학교 전기,컴퓨터 공학부
jihong@davinci.snu.ac.kr
[3](690-756) 제주도 제주시 아라1동 1번지 제주대학교 전산통계학과
jinkim@cheju.ac.kr

	장 점	단 점
LCG	연산을 위하여 많은 저장공간을 필요로 하지 않음	발생되는 난수가 짧은 주기를 갖음
	호출시마다 적은 연산이 필요	낮은 차수의 비트에서 난수성이 떨어짐
	빠르게 생성됨	
MSG	기계에 비의존적 (machine independent)	잘못된 a,m의 선택으로 동일한 난수들이 생성될 수 있음
	긴 난수 주기	이전 단계에서 생성된 난수를 저장
	메모리 요구량이 적음	serial correlation이 있을 가능성
SG	MSG보다 serial correlation이 적음	32개의 난수를 저장하기 위하여 여분의 32개의 저장장소가 필요
	난수 순서의 긴 주기성	초기값의 생성 비용이 큼
LFG	lag 변화에 따른 난수 주기성이 좋음	이전 단계에서 생성된 난수들을 저장하기 위한 많은 메모리가 필요
	성능이 좋은 난수발생기	기계 의존적인 난수 생성 속도
SRG	상대적으로 빠른 생성 속도	비트들이 오버랩되어 난수성이 떨어짐
	많은 양의 메모리가 필요하지 않음	
	하드웨어 구현이 쉬움	

표 1.1: <선택된 난수발생기들의 비교>

수발생기가 필요하게 되고, 이러한 난수발생기가 암호화의 중요한 부분을 차지한다. 그러므로 우리가 이동 단말기에서 주식매매, 계좌이체 등의 활동을 하기 위해서 난수발생기의 사용은 불가피하다. 또한 이동 단말기를 이용하여 게임을 하는 경우에도 게임 프로그램에서는 어느 특별한 상황에서 결정을 내리기 위하여 난수발생기를 사용한다. 이렇듯 우리가 의식하지 못하는 사이에 난수발생기는 이동 단말기의 많은 프로그램에서 사용되어 지고 있다. 그런데 이동 단말기에서는 이전보다 훨씬 작고 가벼운 배터리의 크기가 필수적이며, 이렇게 작은 배터리에 의존하는 이동 단말기의 사용시간을 늘리기 위해서는 배터리를 효율적으로 사용하여야 한다. 이를 위하여 이동 단말기에서 많이 사용되는 난수발생기도 전력 소모가 적은 것의 선택이 필요하다.

배터리 사용시간을 늘리는 방법은 크게 두 가지 방법으로 나누어 질 수 있다. 하나는 배터리 자체의 용량을 늘리는 방법이고, 다른 하나는 이동 단말기에서 실행되는 프로그램들의 에너지 소비량을 줄이는 방법이다. 그런데 배터리 용량을 늘리는 기술은 지난 수십년 동안 우리의 요구에 부응할 만큼의 빠른 발전 속도를 보이지 못했다. 그러므로 이동 단말기에서 배터리 사용시간을 늘리기 위해서는 에너지 소비량을 줄이는 연구의 필요성이 최근에 높아졌다.

RNG	LCG	MSG	SG	ALFG	SLFG	MLFG	XLFG	SRG
Energy(nJ)	55.46	321.24	321.68	85.16	85.03	91.13	85.64	39.04

표 2.1: 각 난수발생기의 에너지 소비량

				LFG				
	LCG	MSG	SG	ALFG	SLFG	MLFG	XLFG	SRG
Pearson's χ^2	12.16	11.82	19.47	39.36	12.67	12.33	28.65	16.24
(p-value)	0.7329	0.7563	0.245	0.001*	0.6967	0.721	0.0264*	0.4363
KS	0.0596	0.0438	0.0662	0.0608	0.0467	0.0582	0.0714	0.0367
(p-value)	0.4756	0.838	0.3454	0.4501	0.7754	0.5081	0.2595	0.9504

표 2.2: 난수성 검정 결과

본 논문에서는 여러가지 난수발생기 중에서 잘 알려져 있고 이동 단말기에서의 구현 및 사용이 적합한 난수발생기들을 선택하였다. 이렇게 선택된 난수발생기들은 여러면으로 분석이 잘 되어 있고, 널리 사용되어 지고 있으므로 중요하다고 할 수 있다. 컴퓨터 구현을 위한 난수발생기는 Marsaglia(1985)에서 찾을 수 있는데, 그 당시에는 이동 단말기의 환경이 일반적이지 않았기 때문에 에너지 소비량에 대한 언급은 없었다. 이동 단말기가 일반적인 환경으로 자리잡은 현재의 환경에서는 난수발생기들의 에너지 소비량을 알아볼 필요가 있다고 본다.

제 2 절 선택된 난수발생기들

여러가지 의사(擬似) 난수발생기(pseudo Random Number Generator, 앞으로 본 논문에서는 난수 발생기를 RNG로 표기한다)중에서 많이 쓰이는 5가지를 선택하였고, 이러한 의사 난수발생기중 Linear Congruential Generator, Minimal Standard Generator, Shuffle Generator는 von Neumann이 제안한 다음의 재귀적인(recursive) 알고리즘을 사용한다. (Anderson, 1990, Gentle, 1998, Press, 1993)

$$I_{j+1} = (aI_j + c) \bmod m \tag{2.1}$$

여기에서 I_j, a, c, m은 각각 j번째 생성된 난수, 승수(multiplier), 가수(increment) 그리고 법수(modulus)를 나타낸다. 법수연산(mod)은 0과 $m-1$ 사이의 일양분포를 갖는 숫자를 발생시켜 준다.

그림(2.1)에서 볼 수 있듯이 에너지 소비가 가장 적은 난수발생기는 SRG이다. 이 난수발생기는 LCG보다 약 30% 나 적은 에너지 소비량을 나타낸다. 서로 다른 이항 연산자들을 가지는 LFG들은 거의 서로 비슷한 양의 에너지 소비량을 보인다. 이중에서는 물론 MLFG가

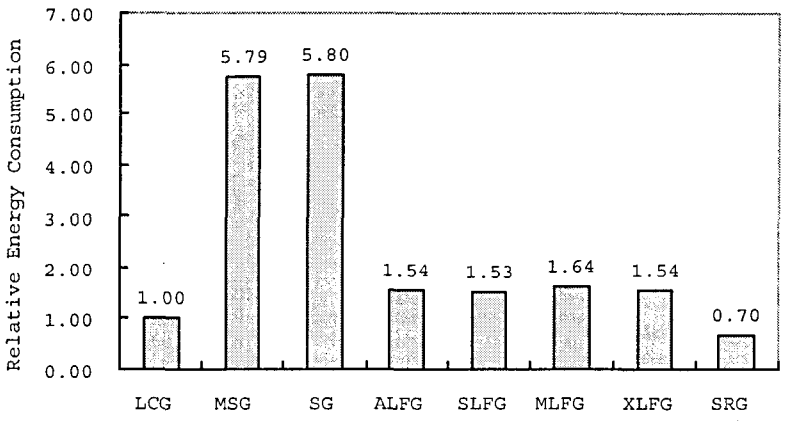

그림 2.1: 각 난수발생기의 상대적 에너지 소비량

곱하기 연산을 이용하므로 가장 많은 에너지 소비량을 나타내고 있다. MSG와 SG는 LCG에 비하여 거의 6배나 많은 에너지 소비량을 보이고 있다. 이것은 MSG와 SG에서는 곱하기 연산이 많은 부분을 차지하고 있기 때문이다. 앞에서도 언급하였지만 곱하기 연산은 다른 연산에 비하여 전력 소모가 상당히 많은 연산이기 때문이다.

그리고 본 논문에서 결과가 실리지는 않았지만 식 (2.1)에 사용된 상수 c값의 변화에 따른 에너지 소비량도 조사하였다. 그러나 값에 의한 에너지 소비량의 차이가 그리 크지가 않고 일정한 규칙성도 없었다. 즉 에너지 소비량의 측면에서 상수 c는 크게 영향을 미치지 않는다는 결론이다.

제 3 절 결론

이동 단말기에서 사용하는 대다수의 프로그램들은 LCG를 사용하고 있다. 이는 LCG가 ANSI C 표준이기 때문에, 난수발생기가 필요한 경우 C 언어의 표준 라이브러리에 있는 LCG를 이용한 `rand()`함수를 소프트웨어 개발자들이 관행적으로 사용하기 때문이다. 그러나 표 (4.2)의 결과를 보면 SRG가 다른 난수발생기들보다 적은 전력 소모를 보임을 알 수 있으므로, PDA나 휴대폰과 같이 에너지 소비량이 매우 중요한 이동 단말기의 프로그램에서는 **LCG를 사용하기 보다는 SRG를 사용함으로 인하여 30% 정도의 에너지 절약** 효과를 볼 수 있으며, **전력소모량이 큰 MSG와 SG의 사용은 피해야 한다.** 그러나 이동 단말기에서 사용되는 프로그램이라 하더라도 암호화와 같이 에너지 소비량 뿐만 아니라 난수성도 매우 중요한 요인으로 작용하는 경우에는 **난수성이 의심되는 ALFG와 XLFG의 사**

용은 피해야 한다.

참고 문헌

[1] Anderson, S.(1990), "Random number generators on vector supercomputers and other advanced architecture," *SIAM Review.* **32**(2):221-251.

[2] ARM Ltd., *ARM7 Thumb Family.* `http://www.arm.com/armtech/ARM7_Thumb`.

[3] Gentle, J.(1998), *Random number generation and Monte Carlo methods.* Springer-Verlag, New York.

[4] Knuth, D.(1981), *The Art of Computer Programming: Seminumerical Algorithms.* Addison-Wesley. volume 2, pages 1-93.

[5] Laramie, P.(1999), "Instruction level power analysis and low power design methodology of a microprocessor," Master's thesis, Electrical Engineering and Computer Science, University of California at Berkeley. pages 38-57.

[6] L'Ecuyer, P.(1988), "Efficient and portable combined random number generators," *Communications of the ACM.* **31**(6):742-774.

[7] Marsaglia, G.(1985), "A current view of random number generators," *Computer Sciences and Statistics: 16th Symposium on the Interface.*(edited by L. Billard), North Holland, Amsterdam. pages 3-10.

[8] Park, S. and Miller, K.(1988), "Random number generators: good ones are hard to find," *Communications of the ACM.* **31**(10):1192-1201.

[9] Press, W., Teukolsky, S., Vetterling, W., and Flannery, B.(1993), *Numerical Recipes in C : The Art of Scientific Computing.* Cambridge University Press. second edition. pages 274-300.

[10] Schrage, L.(1979), "A more portable fortran random number generator," *ACM Transactions on Mathematical Software.* **5**(2):132-138.

[11] Shin, D., Shim, H., Joo, Y., Yun, H., Kim, J. and Chang, N.(2002), "Energy-monitoring tool for low-power embedded programs," *IEEE Design and Test of Computers.* **19**(4):7-17.

[12] Tiwari, V., Malik, S. and Wolfe, A.(1994), "Power analysis of embedded software: a first step towards software power minimization," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems.* **2**(4):437-445.

[13] 윤정민(2002), 난수 발생 프로그램. `http://davinci.snu.ac.kr/jungmin/random`.