2019 한국차세대컴퓨팅학회
춘계학술대회

장　소 : 제주 제주한라대학교

일　시 : 2019. 5. 10(금) 12:00 ~ 5. 11(토) 12:00

주최-주관　한국차세대컴퓨팅학회

2019 한국차세대컴퓨팅학회 춘계학술대회

- **대 회 장** : 노병희 교수(아주대학교)

- **조직 위원장** : 문석환 교수(제주한라대학교)
  최 린 교수(고려대학교)

- **학술 위원장** : 김종국 교수[고려대학교]
  한경식 교수(아주대학교)

- **조직 위원**

  김기형 교수(아주대학교)
  김덕환 교수(인하대학교)
  노상욱 교수(가톨릭대학교)
  이상웅 교수(가천대학교)
  신석주 교수(조선대학교)
  한동진 교수(제주한라대학교)

- **학술 위원**

  강진석 박사[프론티스]
  권구락 교수(조선대학교)
  김도형 교수[강원대학교)
  김동호 교수(숭실대학교)
  김정선 교수(한양대학교)
  김중헌 교수(중앙대학교)
  김진환 교수(한성대학교)
  노영태 교수(인하대학교)
  박기웅 교수(세종대학교)
  박병준 교수(광운대학교)
  박운상 교수(서강대학교)
  석준희 교수(고려대학교)
  안정섭 박사(아주대학교)
  오상윤 교수(아주대학교)
  유일선 교수[순천향대학교]
  유성준 교수(세종대학교)
  이문규 교수(인하대학교)
  이우주 교수(명지대학교)
  정형구 교수(경희대학교)
  조성제 교수(단국대학교)

2019 한국차세대컴퓨팅학회 프로그램

2019. 5. 10(금)		
12:00～13:00	등록 : 금호세계교육관 A동 4층 시청각실	
논문발표	Oral Session 1(인공지능/기계학습)	Oral Session 2(인공지능/기계학습)
발표 장소	금호세계교육관 A동 4층 시청각실	금호세계교육관 A동 2층 강의실 3
13:00～14:00	Colorectal Image Classification using Multi-Convolutional Neural Network	혼합현실 환경에서의 실내 위치 정보 시스템 연구 동향 및 분석
	Recurrent-Convolutional Neural Network for Motif Visualization and DNA Transcription Factor Binding Sites Prediction	역문서빈도로 가중된 부속단어를 이용한FastText 워드 임베딩
	실외 환경에서의 이상행동 인식 기술에 대한 제안	기술적지표를 활용한 머신러닝 주가예측 연구
	A Proposal for Synthetic Data Generation to Improve Smart Surveillance in Uncertain Environments	순환신경망을 이용한BLE 실내 위치 추정 향상
14:00～15:20	개회식, 시상식(우수논문)_금호세계교육관 A동 4층 시청각실	
	초청강연 정보통신망 발전과정과 5G(하상용 박사_NIA 글로벌센터)	
	한국차세대컴퓨팅학회 총회&이사회	
논문 발표	Oral Session 3(시스템)	Oral Session 4(시스템)
발표 장소	금호세계교육관 A동 4층 시청각실	금호세계교육관 A동 2층 강의실 3
15:20～16:20	국방 클라우드에 도입 가능한 클라우드 스토리지 기술 분석 및 한계점 제시	지자기 기반 실내 위치 추정에 사용할 수 있는 지자기 벡터 보정법
	효율적인 가상화 시스템 프로파일링을 위한 분석 프레임 요구사항 도출	FPGA BMC 기반 서버 컴퓨팅 시스템 제어를 위한 소프트웨어 개발 및 구현
	소프트웨어 정의 네트워킹환경에서 sFlow와 블룸필터를 활용한 화이트리스트 기반 서비스 거부 공격 완화 시스템	SDN NBI 표준화 동향 분석 및 통합관제를 위한 YANG 데이터 모델제안
	스마트 시티에서의 이상 행동 모니터링 시스템에 대한 제안	스마트 감시를 위한 드론 데이터에서의 객체 감지 기술에 대한 제안
16:20～16:40	Coffee break	

논문 발표	Oral Session 5(알고리즘)	Oral Session 6(이동통신/네트워크)
발표 장소	금호세계교육관 A동 4층 시청각실	금호세계교육관 A동 2층 강의실 3
16:40~17:40	EEG Topography 라벨링을 이용한 감정인식 기법	MANET에서Extended-Desync TDMA의 슬롯 사용률 향상을 위한 추가Firing 메시지 전송 및 처리 방법
	UAV 자가진단 기술 개발을 위한 상대적 공간 좌표 측정 기술 조사 연구	소프트웨어 정의 네트워킹 환경에서의 효과적인 지능형 트래픽 분류 기술 적용을 위한 아키텍처 분석
	JRoad: Analysis of Road-Network Graph	IoT 디바이스의 랜덤 키 생성 및 보관방법 연구
	국민소통체계로서의재난관련위기경보개선방안에관한연구	레시피 추천 서비스용 라즈베리파이 기반 음성 인식 시스템 설계 및 구현
2019. 5. 11(토)		
09:30~10:00	등록 : 금호세계교육관 A동 2층 강의실 3	
논문 발표	Poster Session 1(인공지능/기계학습, 시스템)	Poster Session 2(이동통신, 알고리즘, 블록체인)
10:00~11:50	GAN의 활용에 관한 연구 동향 및 분석	사물인터넷 데이터 분석을 위한 기존 머신러닝 기술/연구 분석
	심층강화학습을위한GA-기반행동추상화기법	클라우드 환경을 위한 웹 기반 데이터센터 전용 CFD 시스템 설계
	Alzheimer's disease Identification by Combining VBM, Cortical Thickness and Textural Features of Structural Magnetic Resonance Imaging	소방 VR환경 구축을 위한 HCI기반 필수요소 파악
	강화학습을 이용한 마법유닛 컨트롤 에이전트	유튜브 시간 별 댓글 분석을 통한 안정적인 인플루언서 선정 기준 연구
	LSTM을 이용하여 BEMS을 위한 태양광발전량 예측	LTE기반 위급상황메시지 전송시스템
	스마트폰 사용 데이터를 활용한 사용자 기분 상태 파악 기계학습 및 LSTM모델개발	Real-time Interactive LED Tree-type Food Wastebasket

	딥러닝기반스마트축사사료공급정밀예측기법	Combinatorial Auction Approach to Optimal Resource Sharing in Device-to-Device Communication Underlaying Uplink Cellular Networks
	멀티 스케일 컨볼루션 신경망과 트라이맵 자동생성을 이용한 객체추출	실시간 데이터 이중화를 위한 정책 기반 고속 데이터 전송 기술 개발
	NVIDIA FleX를 이용한 실시간 흙 시뮬레이션	PF-RNG: 초저가 무선 통신 컴퓨팅 환경을 위한 엔트로피수집 모델 제안
	Polyp Segmentation Using a Multi-model Deep Encoder-Decoder Network	SNMP와 NETCONF 프로토콜 및 지원 도구의 특성 분석 비교
	gRPC를 이용하는 웹 프로그램의 벤치마크 도구 개발 및 적용에 관한 연구	HPC 클러스터파일시스템들의성능향상기법분석
	Kubernetes 기반의 응용에서 자원 사용량 측정을 위한 Prometheus의 버전별 부하 테스트	Fully Quantum-Processed Evolutionary Algorithm via Exploitation of Hamiltonian
	오픈데이터중개를위한오픈데이터API 게이트웨이시스템개발	차선 레벨 위치를 검출하는 알고리즘 조사
	Complex Event Processing Rule 적용을 위한 동적 자동화 Rule파일 생성 및 적용 방법	스마트폰기반보행자추측항법을위한3축가속도 센서의축보정
	FPGA 보드 BMC 기반 디바이스 제어 인터페이스 설계 및 구현	블록체인 기반의 온라인 사기 정보 수집 시스템 설계
	컨테이너 기반 자원 관리 효율화를 위한 Mesos 오케스트레이션 방법 개선	Dapp 서비스 분야 현황 및 이더리움 Dapp의 스마트컨트랙트 구조 연구
	A Study on VTuber(Virtual Youtuber) Live Streaming Implementation	제주 풍력통합모니터링을 위한 풍력발전기 연계방법 관한 연구
11:50~12:00	폐회	

PF-RNG: 초저가 컴퓨팅 디바이스의 무선 보안 통신 채널 형성을 위한 엔트로피수집 모델 제안

PF-RNG: Proposal of Entropy Collection Model for Wireless Secure Communication Channel of Ultra Low-Cost Computing Device

조승현, 이광진, 류민수, 진호용, 김영수, 최상훈, 박기웅 †
Seung-Hyeon Cho, Gwang-Jin Lee, Min-Soo Ryu, Ho-Yong Jin, Young-Su Kim, Sang-Hoon Choi, Ki-Woong Park †

세종대학교 정보보호학과
me@shc.me, {leekjin97, onsoim, majinga2007, 34t3rnull, csh0052}@gmail.com, woongbak@sejong.ac.kr†

요 약

무선 통신 환경에서 요구되는 대다수의 암호화 기법은 무작위성에 기반하여 설계되어 있기 때문에 안전한 통신 환경을 위해서는 신뢰할 수 있는 RNG를 확보하는 것이 매우 중요한 요소 중 하나이다. 그러나 웨어러블 컴퓨팅, 사물인터넷 등의 초저가 무선 통신 컴퓨팅 환경에서는 설계의 단순화와 가격 절감으로 인해 신뢰도가 높은 RNG를 확보하는데 어려움이 있었다. 이에 본 논문에서는 COTS 무선 통신 모듈을 활용하여 엔트로피를 수집하며, 패리티 피드백을 통해 수집한 엔트로피의 신뢰도를 판단할 수 있는 Parity-Feedback 모델을 제안하여 가격 절감 요소를 유지하며 신뢰할 수 있는 RNG 확보 방안을 제안한다.

1. 서론

웨어러블 컴퓨팅, 사물인터넷 등의 차세대 컴퓨팅에서 활용되는 컴퓨팅 장치는 최소한의 성능으로 필요한 기능만 갖추어 생산 단가를 낮추는 소형화와 경량화를 추구하고 있다[1]. 이를 통해 보다 높은 보급률과 낮은 접근성을 제공하여 실생활에 유익을 도모하고 있다. 이러한 흐름 속에서 사물인터넷은 사용자의 일상에 보다 더 가까운 곳에 위치하게 되었으며, 필연적으로 수집되는 정보에 대한 관리와 안전한 통신 방법에 대해서도 중요성이 크게 부각되고 있다. 수요에 따라 다양한 보안 기법에 대한 연구가 활발히 진행되어 왔으며, 암호화를 비롯한 대다수의 보안 기법은 신뢰할 수 있는 Random Number Generator(RNG)를 기반으로 동작하게 된다. 따라서 신뢰할 수 있는 RNG를 확보하는 것이 초저가 무선 통신 컴퓨팅 환경을 위한 주요 과제이며 이를 위한 활발한 연구와 구현이 진행되어 왔다. 그러나 이러한 구현은 초저가 컴퓨팅 디바이스에 적용하기에 많은 한계가 존재하였으며, 요구하는 신뢰성을 충족시키지 못하는 어려움이 있었다. 이에 본 논문에서는 통신을 기반으로 하는 장비에는 공통적으로 안테나가 있다는 것에 착안하여 초소형 차세대컴퓨팅 환경에서 존재하는 요구사항과 제약 사항을 충족하는 엔트로피 확보 방법과 발생 가능한 공격으로부터 유효성을 확인할 수 있는 모델을 제안하고자 한다.

2장에서는 기존의 RNG 구현 방법과 초소형 차세대 컴퓨팅 환경에서 발생 가능한 문제점과 한계를 다룬다. 3장에서는 무선 통신을 활용한 엔트로피 수집 방법과 발생 가능한 문제점에 대해 다루며, 마지막으로 4장에서는 발생 가능한 문제점을 개선할 수 있는 모델에 대해 제안을 한다.

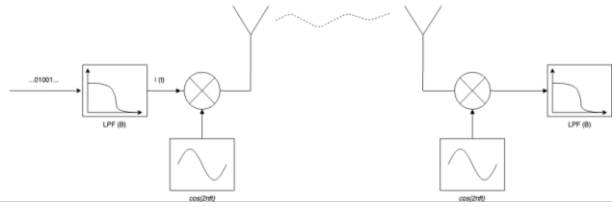
2. 기존의 RNG 구현 방법과 한계

난수생성기를 구현하는 방법으로는 크게 물리적 방법과 논리적 기반으로 구분 지을 수 있다. 그중 논리적 기반의 난수생성기로는 현대의 CPU에서 발생하는 glitter의 무작위성을 통해 엔트로피를 수집하며 이는 Google의 Zicorn OS 에서도 사용하는 등 이미 실용화가 되어 있다. 그러나 이러한 CPU의 glitter 현상은 명령 파이프라인, 저전력 설계를 위한 클럭 스케일링 등의 요인으로 발생하기 때문에 상대적으로 단순한 구조의 MPU 혹은 MCU와 같은 유닛 에서는 보안 어플리케이션이 요구하는 통계적 특성을 만족하기 어려운 한계가 있다[2]. 물리적 기반의 난수생성기는 임의의 원자 또는 물리 현상을 기반으로 하기 때문에 방사능 붕괴, 열 잡음, 하드 디스크 읽기/쓰기 등의 현상을 측정하여 엔트로피를 얻어낸다. 하지만 이러한 현상을 측정하기 위해서는 추가적인 회로와 장치를 요구하게 되기 때문에 부피의 증가와 생산 단가 증가로 이어지게 되는 문제점이 있다. 그러나 대부분의 초저가 무선 통신 컴퓨팅 환경에서 무선 통신을 위한 안테나 회로가 있으며, 이는 좋은 엔트로피 소스로 활용될 수 있다.

3. 무선 안테나를 통한 엔트로피 수집 방법

3.1 무선 통신 기본 시스템

무선 통신은 둘 또는 그 이상의 단말기가 전기 전도체의 연결 없이 정보를 전송하는 것을 말한다. 그 중 전자기파를 이용한 통신 방법에서 발신 단말기에서는 보내고자 하는 정보를 전파로 변조하여 전력증폭기를 통해 전파를 송출하고, 수신하는 단말기에서는 수신된 전파를 복조하여 정보를 수신하게 된다. 이러한 일련의 과정을 간소화하면 그림과 같이 볼 수 있다.



(그림 1) 기본적인 무선 통신 시스템 과정

송신 단말기에서는 전송할 비트열을 저주파 통과 필터(low-pass filter)를 통해 기저대역(baseband waveform)으로 변환하고, 이를 반송파(carrier waveform)와 곱하여(multiply) 송신을 하게 된다. 수신 단말기에서는 안테나를 통해 신호를 수신하여 국부적으로 생성된 반송파(locally generated carrier)와 곱하여 기저대역을 재생성하여 저주파 통과 필터를 통해 비트열을 얻어낼 수 있다.

3.2 무선통신 시스템에서의 엔트로피 수집 방법

그림1 과 같은 무선통신 시스템은 안테나 RC회로의 공진 특성에 의해 발생한 전기신호를 복조한다. 이는 근접한 공진 주파수의 신호에 의해 간섭이 발생하게 되며 이를 잡음이라 한다. 무선통신 시스템에서는 저주파 통과 필터를 비롯한 여러 필터를 통해 통신에 불필요한 잡음을 제거하며 수신 단말기는 잡음이 제거된 파형을 통해 데이터를 얻어내게 된다. 이러한 잡음은 주변에 존재하는 다양한 원인에 의해 발생하게 된다. 본 논문에서는 필터링 이전의 잡음을 활용하여 엔트로피를 확보하는 방법을 제안하고자 한다.

3.3 발생 가능한 문제점

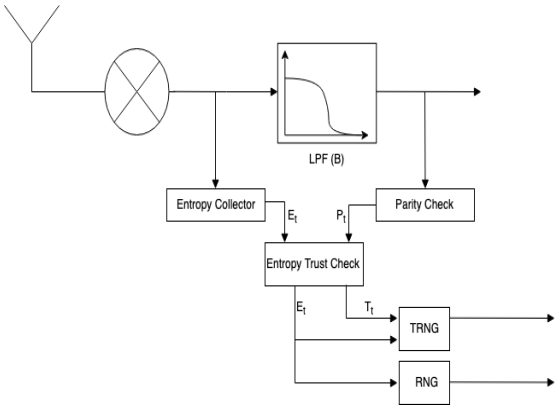
그러나 이러한 잡음을 통해 엔트로피를 확보하는 방법은 공격자가 변조된 잡음을 주입할 경우 조작된 엔트로피를 주입시킬 수 있는 문제가 존재한다. 특히 재밍 모형 중 대역 잡음 재밍(band noise jamming)과 펄스 재밍(pulse jamming) 공격에 노출 될 경우 공격자가 의도한 엔트로피를 수집하게 된다.

4. 제안하는 엔트로피 수집 모델

4.1 에러 검출을 활용한 신뢰 여부 판단

대역 잡음 재밍과 펄스 재밍 모형은 물리계층에서 본 모형이기 때문에 수신 단말기가 해당 공격에 노출될 경

우 복조과정에서 비정상적인 데이터를 얻어낼 수 있다[3]. 그리고 이러한 공격에서 복조 된 데이터는 OSI 7계층 구조 중 데이터 링크 계층의 패리티 검사에서 오류를 검출할 수 있다. 따라서 설계한 모델 에서는 해당 패리티 검사 결과를 활용하여 수집한 엔트로피의 신뢰 여부를 판단할 수 있게 된다.



(그림 2) 제안하는 Parity-Feedback 모델

이러한 신뢰를 판단하여 RNG를 통해 난수를 생성할 경우 충분한 수집을 기다리는 동안 장치가 동작하지 않는 상태를 피하기 위해 본 모델에서는 RNG와 TRNG(True Random Number Generator) 두가지를 제공하게 된다. TRNG는 신뢰 확보 후 출력하기 때문에 요구하는 신뢰도 확보까지 대기하는 반면 RNG는 신뢰 확보 여부 상관없이 요청시 즉시 난수를 출력한다. 현제 시점 t에 대하여, Entropy Collector(EC)를 통해 수집한 비트열 E_t, Parity Check(PC) 를 통해 검출한 결과값 P_t을 통해 Entropy Trust Check(ETC)에서는 신뢰 여부를 가리키는 T_t를 출력 한다.

$$C_t = PC(t)$$

$$E_t = EC(t)$$

$$T_t = \sum_{i=t-n}^{t} C_i = ETC(t,n)$$

그리고 TRNG 에서는 T_t값이 양수일 경우 E_t값을 신뢰할 수 없다고 판단하게 된다. $PC(t)$의 에러 검출 확률을 P_c로 정의할 때, T_t가 양수일 확률$P(T_t > 0)$ 은 다음과 같다.

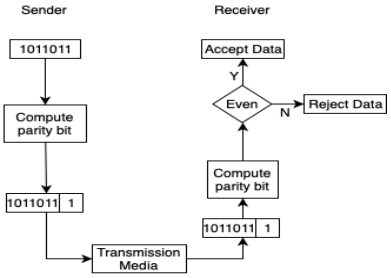
$$P(T_t > 0) = (P_c)^n$$

따라서 E_t의 신뢰도는 다음과 같이 정의된다.

$$1 - (P_c)^n$$

따라서 Entropy Trust Check의 인자 n은 패리티 검사 알고리즘의 에러 검출 확률과 요구하는 신뢰도에 의해 값이 결정된다.

4.2 짝수 패리티 검사



(그림 3) 짝수 패리티 기법

가장 잘 알려진 패리티 검사 기법은 짝수 패리티 기법이다[4]. 이는 송신할 데이터 블록에 모든 비트의 합이 짝수가 되도록 비트를 추가하여 전송 후, 수신자는 데이터 블록과 추가된 비트의 합이 짝수인지 확인하여 에러 여부를 판단한다. 따라서 해당 알고리즘의 에러 검출 확률은 약 $\frac{1}{2}$이며, $(\frac{1}{2})^6 > 0.001 > (\frac{1}{2})^7$이므로, 시스템에서 요구하는 E_t의 신뢰도가 99%일 경우 n값은 7이상이 되어야 한다.

4.3 Low-Density Parity-Check

보다 높은 확률의 패리티 체크 알고리즘을 활용할 경우 본 모델은 보다 높은 응답성을 가지게 된다. BSC(Binary Symmetric Channels)에서 LDCP(Low-Density Parity-Check)의 에러 확률을 추정한 계산식에 따르면, FER(Frame Error Rate Estimation)은 기본적으로 교차 확률이 ε인 BSC를 통해 지정된 하드 결정 반복 알고리즘에 의해 디코딩 된 블록 길이 n에 크게 영향을 받는다[5, 6]. 따라서 LDPC를 활용하여 본 모델에 적용할 경우 시스템에서 요구하는 E_t의 신뢰도가 99%일 경우, 요구되는 n값은 4이다. 단, Gallager algorithms을 LDPC의 디코딩 알고리즘으로 사용하면서, 교차확률 ε를 0.1% 이하로 유지해야한다.

4.4 신호 양자화 특성을 활용한 공격 차단

앞서 기술한 방법으로 엔트로피를 수집할 경우 Data Error를 유발시키지 않을 정도의 의도된 잡음을 발생하였을 경우 Parity 검사에 영향을 미치지 않으나, RNG Seed 생성에 있어서는 영향을 미칠 가능성이 존재한다. 그러나 이는 양자화 특성을 통해 보완할 수 있다. 신호처리에서 연속적인 양을 기본 단위의 정수배로 측정하는 양으로 재해석하는 것을 양자화라고 한다. 이 작업은 대량의 정보를 상대적으로 적은 데이터로 대입을 하기 때문에 필연적으로 오차가 발생하게 된다. 또한 해당 정보는 진폭이 0에 수렴할 시점에 오차의 발생 주기가 가장 높아지므로[7] 해당 시점에 양자화를 진행한다. 따라서 양자화 된 값의 최하위 비트를 수집할 경우 본 절에서 언급한 문제를 보완할 수 있다.

5. 결론

본 논문에서 제안하는 PF-RNG 모델은 초저가 무선 통신 컴퓨팅 환경에 이미 존재하는 무선 통신 모듈을 활용하여 엔트로피를 수집하는 방법을 통해 원가절감의 요구사항을 만족시킬 수 있다[8]. 또한 제안하는 수집한 엔트로피에 대한 신뢰도를 측정 방안은 각 사용 환경의 요구사항에 따라 적합한 패리티 검사 알고리즘을 적용함으로써 다양한 환경에서 적용 가능 할 것으로 예상된다. 또한 신호 양자화의 특성과 패리티 검사 모델을 함께 적용할 경우 상호 보완적인 효과로 인해 외부 공격에 대해 감지 및 차단할 수 있게 될 것으로 예상된다.

Acknowledgement

본 연구는 2019년도 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원(No.2019-0-00426)의 지원을 받아 수행된 연구임.

참고문헌

[1] Ratasuk, Rapeepat, et al. "NB-IoT system for M2M communication." 2016 IEEE wireless communications and networking conference. IEEE, 2016.

[2] Muller, S. "Cpu time jitter based non-physical true random number generator." Ottawa Linux Symposium. 2014.

[3] 이두호, 고병훈, and 김광순. "Anti-Jamming 기반 전술통신 기술." 한국통신학회지 (정보와통신) 24.10 (2007): 24-33.

[4] NPTEL. 2009. Module 3 Data Link control. In Courses of Computer Science and Engineering, version 2 CSE, Indian Institute of Technology (IIT), Kharagpur, India. https://nptel.ac.in/courses/106105080/pdf/M3L2.pdf

[5] Xiao, Hua, and Amir H. Banihashemi. "Improved progressive-edge-growth (PEG) construction of irregular LDPC codes." IEEE Communications Letters 8.12 (2004): 715-717.

[6] 박호성, and 노종선. "차세대 통신 시스템을 위한 오류 정정 부호." 한국통신학회지 (정보와통신) 29.8 (2012): 26-33.

[7] Bennett, William Ralph. "Spectra of quantized signals." The Bell System Technical Journal 27.3 (1948): 446-472.

[8] 박현호, and 송익환. "IoT 환경에서의 EMC 기술 전망." 전자파기술 28.1 (2017): 41-47.