XXI. Fiatal Műszakiak Tudományos Ülésszaka, 2016. Kolozsvár, 353–356. DOI: 10.33895/mtk-2016.05.79
http://hdl.handle.net/10598/29104

SZOFTVERRÁDIÓN ALAPULÓ ADAPTÍV ENTRÓPIAFORRÁS GENETIKUS ALGORITMUS SEGÍTSÉGÉVEL

ADAPTIVE, SOFTWARE RADIO BASED ENTROPY SOURCE WITH GENETIC ALGORITHM

Répás Sándor

Óbudai Egyetem Biztonságtudományi Doktori Iskola, Cím: 1034, Magyarország, Budapest, Bécsi út 96/b.; rsandor@ahol.co.hu

Abstract

We shortly present the main application areas of random numbers, and the creation methods of them. We briefly describe the operation of the software defined radios. We present a solution to getting the help of genetic algorithm (GA) to find the optimal setup parameters. Presented methods are useful in developing adaptive systems which use time-varying entropy source.

***Keywords**: adaptive system, genetic algorithm, RTL-SDR, TRNG*

Összefoglalás

Röviden bemutatjuk a véletlen számok főbb felhasználási területeit, és előállítási lehetőségeiket. Nagyon röviden a szoftverrádiók működését ismertetjük. Bemutatjuk azt, hogyan lehet genetikus algoritmus (GA) segítségével megtalálni az optimális beállítási paramétereket. A bemutatott módszerek jól használhatóak olyan adaptív rendszerek kialakítására, melyek időben változó tulajdonságú entrópia forrást alkalmaznak.

***Kulcsszavak:** adaptív rendszer, genetikus algoritmus, RTL-SDR, szoftverrádió, véletlenszám.*

1. Bevezetés

A véletlen számok a kriptográfiában és a szimulációkban kiemelt jelentőséggel bírnak, ugyanakkor előállításuk nem triviális feladat. A megfelelő minőségű valódi véletlen szám (True Random Number, TRN) előállításához elengedhetetlen fontosságú egy entrópia forrás, mely a véletlen szám generátor (Random Number Generator, RNG) bemeneteként használható, és segítségével, különböző algoritmusokat alkalmazva véletlen szám állítható elő. A rendkívül olcsó szoftverrádiók (Software Defined Radio, SDR) megjelenése, az SDR mind szélesebb körű alkalmazását idézte elő, valamint megjelent az igény az SDR-ek entrópia forrásként történő alkalmazására is [1]. Ugyanakkor nem megoldott az SDR-ek működési paramétereinek beállítása, valamint változó körülmények esetén, a paraméterek módosítása.

A genetikus algoritmusoknak [2] az informatikai biztonság területen történő alkalmazása széles körben elterjedt. Számtalan publikáció foglalkozik a GA behatolás detektáló [3], valamint levélszemét szűrő [4] alkalmazásokban történő alkalmazásával.

A következőkben egy szoftverrádió segítségével kialakított, genetikus algoritmus segítségével megvalósított adaptív entrópiaforrást mutatunk be.

2. Véletlen számok

A véletlen számok megjósolhatatlanok. A véletlen számokból álló sorozat tagjai közt nem található összefüggés, vagy mintázat.

2.1. Előállításuk

A véletlen számok előállítása történhet:

- valós véletlen szám generátorral (True Random Number Generator, TRNG); A hagyományos számítógépek, nem képesek valós véletlen számokat előállítani, általában valamilyen külső eseményt használhatnak fel erre a célra (pl. megszakítás, egérmozgás);
- álvéletlen szám generátorral (Pseudo Random Number Generator, PRNG); valamilyen matematikai algoritmus segítségével állítják elő a véletlennek tűnő számsorozatot, melyhez kezdeti bemenő paramétert alkalmaznak.

2.2. Felhasználásuk

A véletlen számok sok területen nélkülözhetetlenek, melyekből csak kettőt emelünk ki:

- szimuláció: általában PRNG segítségével előállított számokra van szükség, sokszor oly módon, hogy többszöri futtatás is ugyanazt az álvéletlen sorozatot eredményezze (ez azonos PRNG és kezdeti bemenő paraméterértékkel érhető el);
- titkosítás: a megfelelő biztonság eléréséhez valós véletlen számokra van szükség, vagy olyan álvéletlen számokra, melyek a támadók számára nem reprodukálhatóak (nem ismert PRNG algoritmus, és/vagy kezdeti bemenő érték).

3. Szoftverrádió

A szoftverrádió alapelve, hogy az analóg-digitális átalakítás az antennához a lehető legközelebb történjen meg, és a jelfeldolgozás minél nagyobb része történhessen meg digitális módszerekkel. Ezáltal az SDR működése újradefiniálható, nincs szükség különféle eszközökre, hanem egységes hardveren, eltérő szoftverek segítségével kivitelezhetőek a kívánt funkciók [4-5].

Az RTL2832U félvezetőre épülő eszközök [7], valamint az RTL-SDR programkönyvtár [8] megjelenésével, bárki számára elérhetővé váltak az SDR eszközök. Egy RTL2832U-ra épülő USB DVB-T vevő már 10 USD alatt is elérhető, és kiválóan használható SDR-ként, így számos érdekes kutatás készült segítségével, valamint egyre szélesebb körben alkalmazzák az oktatás területén is [9]. Egy ilyen eszköz, az alkalmazott tuner típusától függően, akár 52 és 2200Mhz közötti tartományban, 7bites felbontással 2,56MS/s mintavételezéssel is képes lehet az érzékelt jelet IQ értékekként a számítógépnek továbbítani [7-8].

4. Véletlen számok előállítása SDR és GA segítségével

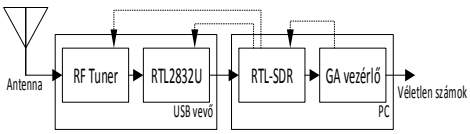
4.1. SDR mint entrópia forrás

A különböző elektromágneses zajok entrópia forrásként történő felhasználása általánosan elterjedt. Erre a célra az SDR is jól használható. Elégséges egy nem, vagy alig használt frekvenciára hangolni, majd az IQ demodulátor kimeneteit felhasználni. A legjobb eredmény akkor érhető el, ha a 7 bites kimenetből csak a legalacsonyabb helyi értéket használjuk fel.

Problémaként merül fel azonban, annak a frekvenciának a beállítása, mely a leginkább megfelel a véletlen számok generálásához, ráadásul ez a frekvencia helytől és időtől is függ, tehát adaptív rendszer kialakításra van szükség. A probléma megoldá-

sára kiválóan alkalmazható a genetikus algoritmus.

A rendszer blokkvázlata az **1. ábrá**n látható.



1. ábra. *A GA segítségével vezérelt SDR entrópia forrás blokkvázlata*

A tuner és az SDR mintavételezési beállításait a GA segítségével (az RTL-SDR interfészen keresztül) beállítjuk, majd következik a mintavételezés, a feldolgozás, végül a kimeneten megjelenik az érzékelt bitsorozat.

4.2. A GA vezérlő

A vezérlés sokféle módszerrel megoldható, a következőkben csak egy lehetséges megoldást ismertetünk.

4.2.1. Egyedek és populáció

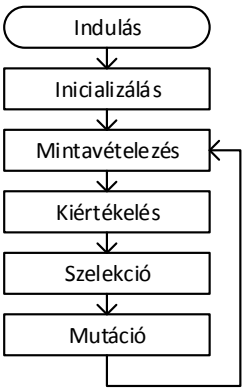
Húsz egyedből álló populáció került kialakításra. Az alacsony szám oka, hogy a mintavételezés egy eszköz alkalmazásával csak egymás után végezhető el, így viszonylag hosszú időt vesz igénybe. Az egyes egyedek két tulajdonsággal rendelkeznek: Mintavételi sebesség, frekvencia. A tulajdonságok jellemzőit az **1. táblázat** tartalmazza.

Az egyes tulajdonságok a táblázatban megadott bitszámon egész értékként kerülnek ábrázolásra. A választott értékek a mutáció ismertetésénél kerülnek indoklásra.

A vezérlés működése a **2. ábrá**n látható.

1. táblázat. *Egyed tulajdonságai*

Tulajdonság	mintavétel (S/s)	frekvencia (Hz)
minimum	1751425	692258177
maximum	2800k	1766M
hossz (bit)	20	30



2. ábra. *A GA vezérlés működése*

4.2.2. Inicializálás

A kezdeti populáció előállítása során az egyes egyedek mindkét tulajdonságát véletlenszerűen értékekre állítjuk be. Azonos egyedek nem kerülhetnek a populációba.

4.2.3. Mintavételezés

A mintavételezés során, minden egyed tulajdonságai által meghatározott paraméterekkel meghívásra kerül az RTL-SDR, mely minden esetben 8MB-os állományokat hoz létre. (A felhasználást megelőzően, az egyed tulajdonságaiként megadott mintavételi és frekvenciaértékek növelésre kerülnek a minimum értékekkel.)

Az előzetes feldolgozás során az állományokból a legalacsonyabb helyi értékű bitek átmásolásra kerülnek új állományokba, melyek mérete így 1MB-ra csökken.

4.2.4. Kiértékelés

A kiértékelés során minden egyedre meghatározásra kerül a fitneszfüggvény értéke.

A fitneszfüggvény kialakításánál fontos szempont a végrehajtási sebesség, így az egyes egyedekhez tartozó állományoknak csak a következő három tulajdonsága kerül vizsgálatra, majd a kapott eredmények kerülnek összegzésre:

- X^2 eloszlással számított értéket meghaladó esetek számának 50%-tól eltérése;
- Monte-Carlo szimuláció segítségével meghatározott π értékének, a tényleges értéktől való eltérése;
- Soros korrelációs együttható 0-ától való eltérése.

Az értékek kiszámítása az ent [10] külső program meghívásával végezhető el egyszerűen.

4.2.5. Szelekció

A fitneszfüggvény értékek alapján csökkenő sorba rendezett egyedek közül, az első tíz kiválasztásra kerül, melyek változatlanul bekerülnek az új populációba. A kiválasztott egyedekből, azon egyedekhez tartozó minták, melyek elérik a fitnesz függvény minimálisan megadott értékét, kerülnek továbbításra a véletlen szám generátor bemenetére. (Ez biztosítja azt, hogy csak megfelelően véletlen eloszlású bitsorozat kerülhessen ki a rendszerből.)

4.2.6. Mutáció

Ez az első tíz egyed képezi az alapját a mutációnak is. Minden egyed egy új egyednek képezi az alapját. Az új egyed képzésekor, annak mindkét tulajdonságánál véletlenszerűen kiválasztásra kerül egy-egy bit, melynek értéke negálásra kerül.

Ha a populáció két ugyanolyan egyedet tartalmazna, úgy másik bit kerül negálásra.

5. Következtetések

Genetikus algoritmus segítségével előállítható egy adaptív entrópia forrás, mely a jelenleg is elérhető RTL-entropy alkalmazásánál lényegesen nehezebben támadható. Ezáltal titkosítási feladatokra alkalmazása sokkal jobban megfelel. [11]

A jövőben külső programok meghívása helyett, integrált megoldás elkészítését tervezzük, mely ugyan tanulásra nehezebben alkalmazható, de valós felhasználásra jobban megfelel. Több rádió egyidejű alkalmazásának és a párhuzamos kódfuttatásnak megoldása is fontos feladat.

Szakirodalmi hivatkozások

[1] Warren, Paul: RTL-Entropy, https://rtl-entropy.org/, Elérve: 2015. október 29.

[2] Coley, David A: *An introduction to genetic algorithms for scientists and engineers*. World scientific, 1999.

[3] Chittur, Adhitya: *Model generation for an intrusion detection system using genetic algorithms,* http://www1. cs. columbia. edu/ids/publications/gaids-thesis01. pdf, Elérve: 2015. október 29.

[4] Oda, Terri, White, Tony: *Immunity from spam: an analysis of an artificial immune system for junk email detection*, Artificial Immune Systems, 2005. 276-289.

[5] Eged Bertalan: *Elektronikai hadviselési és felderítő rendszerek integrációja korszerű digitális- és szoftver rádió technológiával*, Hadmérnök, 2009. június, 274.

[6] Erdei Márk, Wagner Margit Katalin: *Szoftverrádió-rendszerek: új trendek*, Híradástechnika, 2005/8.

[7] RTL2832U, http://www.realtek.com.tw/products/productsView.aspx?Langid=1&PFid=35&Level=4&Conn=3&ProdID=257, Elérve: 2015. október 30.

[8] OsmocomSDR -rtl-sdr, http://sdr.osmocom.org/trac/wiki/rtl-sdr, Elérve: 2015. október 30.

[9] Uengtrakul, Boonyarit, Bunnjaweht, Dahmmaet: *A Cost Efficient Software Defined Radio Receiver for Demonstrating Concepts in Communication and Signal Processing using Python and RTL-SDR*, Bangkok, 2014. május 6-8. 394-399.

[10] Walker, John: ENT *A pseudorandom number sequence test program*, http://www.fourmilab.ch/random/, Elérve: 2015. december 10.

[11] *Un portrait militaire au reflet de l'insurrection hongroise*, ORIENTS (ISSN: 1769-6321) 2013: (10) pp. 93-96. (2013)