Pseudo Random Distribution dalam DotA

Hably Robbi Wafiyya – NIM : 13507128
Program Studi Teknik Informatika
Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
e-mail : if17128@students.if.itb.ac.id

ABSTRAKSI :

Agoritma pembangkitan bilangan acak semu (Pseudo random Number Generator/ PRNG) merupakan salah satu bahasan yang penting dalam kriptografi. Ada dua syarat yang harus dipenuhi dalam PRNG, yaitu harus lulus uji statistic (distribusi ideal), dan lulus uji kriptografis (tak dapat diprediksi). Namun dalam dunia game, konsep PRNG yang digunakan menjadi berbeda. Jika PRNG kriptografi menekankan pada "unpredictability" algoritmanya, PRNG game lebih menekankan pada "statistic"nya. Artinya dalam ruang lingkup yang kecil, algoritma haruslah memberikan disribusi ideal. Hal ini penting jika memperhitungkan factor game balancing. Game DotA, yang berada pada engine warcraft menggunakan Pseudo random Distribution (PRD), yaitu algoritma yang mampu menghasilkan bilangan acak yang lebih "balance"

Kata Kunci : PRNG, PRD, random, game balancing

1. PENDAHULUAN

Kriptografi merupakan suatu ilmu dan seni yang bertujuan untuk menjaga kerahasiaan pengiriman pesan. Salah satu cabang ilmu kriptografi adalah algoritma pembangkitan bilangan acak semu (Pseudo Random Number Generator / PNRG). Sebuah algoritma PRNG dianggap ideal jika memenuhi 2 buah syarat :

1. Lolos uji keacakan statistic (artinya bilangan yang dihasilkan terdistibusi sesuai teori peluang dan statistik)
2. Lolos uji kriptografis (artinya bilangan yang dihasilkan setelahnya tak adapat diprediksi, sehingga relative aman terhadap serangan)

2. PRNG KRIPTOGRAFI

Algoritma PRNG secara kriptografis lebih menekankan pada kamanannya dan "unpredictability" dari algoritma tersebut. Terdapat 2 syarat utama agar algoritma PRNG tersebut dinilai aman secara kriptografis

1. Setiap PRNG harus memenuhi sifat keacakan untuk tiap bit selanjutnya. Artinya jika diberikan k-bit bilangan acak, maka tak ada algorithma dalam waktu polynomial yang mampu memprediksi bit keluran selanjutnya (k+1) dengan peluang keberhasilan lebih besar dari ½ .
2. PRNG harus mampu menahan perluasan status, yaitu jika sebagian atau seluruh statusnya diungkap, maka tidak mungkin merekonstruksi aliran bilangan acak

Namun sayangnya hanya sedikit algoritma PRNG yang lolos uji kriptografis secara sempurna. PRNG dalam kriptografi lebih ditekankan pada keamanan (tak mungkin diprediksikan) algoritmanya. Namun dalam dunia Game, hal itu bukanlah masalah besar. Yang lebih penting dalam game adalah factor balancing, yaitu bagaimana sebuah game menggunakan random generator, namun tetap balance.

Konsep PRNG dalam game adalah untuk menghasilkan bilangan random yang digunakan untuk melakukan roll, yang menyatakan persentasi keberhasilan sebuah event. Misalnya sebuah event memiliki chance terjadi sebesar 30%, maka cukup melakukan randol roll integer number dari 1-100 , jika hasilnya di bawah 30, maka event akan terjadi (sukses). Jika tidak, maka event tak terjadi (gagal).

Konsep ini memiliki kelemahan yang cukup fatal. Ini berarti, memungkinkan event itu terjadi dalam 5x (100% success in 5 try at sequence) rolling berturut2, atau bahkan sama sekali tak terjadi sekalipun dalam permainan (0% success in 100 try). Hal ini tentu akan mempengaruhi balancing dari sebuah game. Karena itu pihak developer warcraft 3 (engine yang digunakan DotA) menerapkan system yang lebih brilian, yang disebut dengan Pseudo random distribution (PRD).

3. PSEUDO RANDOM DISTRIBUTION

Sistem random generator pada kriptografi memiliki kelemahan fatal, yaitu ketidakmampuannya mencegah suatu even yang memiliki chance terjadi berturut2, atau memastikan ia terjadi setidaknya sekali dalam beberapa trigger.

Ilustrasinya adalah berikut :

Mortred (salah satu karakter dalam DotA) memiliki 15% chance melakukan 4x critical damage, dalam setiap serangan. 4x critical adalah angka yang sangat besar, yang mampu merubah damage 250 menjadi 1.000, yang jika terjadi 2x berturut2 mampu membunuh lawan dengan sangat cepat. Namun, dengan system random biasa, (roll 1-100, jika nilai kurang dari 15, maka success, jika tidak, maja fail) sangatlah mungkin terjadi 5x critical dalam 5x serangan secara berturut2, atau bahkan sama sekali tak pernah ciritical dalam 100 serangan. Hal ini tentu akan menjadi isu penting dalam game balance. Dimana jika terjadi 5x berturut2 akan menyebabkan mortred terlalu powerful, dan sebaliknya menjadi terlalu lemah jika dalam 100 serangan sama sekali tak keluar Criticalnya.

Maka dari itu, developer warcraft 3 (engine DotA) menerapkan system Pseudo random Distribution (PRD) untuk menangani isu ini. Yaitu agar memastikan suatu event tak pernah “tak terjadi sama sekali”, dan tak pernah “selalu terjadi setiap trigger”.

3.1 Konsep Dasar PRD

Konsep dasar PRD adalah dengan memberikan konstanta peluang yang bertambah jika event tersebut fail.

Misalkan, si A memiliki 30% chance untuk critical, maka yang sebenarnya dilakukan oleh program adalah sebagai berikut :

- Pada serangan pertama, A memiliki 5,57% chance buat trigger critical
- Jiika gagal, maka serangan berikutnya akan memiliki 11,14% chance buat critical (bertambah 5,57% chance dari chance sebelumnya)
- Jika gagal lagi, maka serangan berikutnya akan memiliki 16,71% chance
- Jika gagal lagi, maka akan bertambah 5,57% chance lagi.
- Jika berhasil, maka counter akan direset dan A akan kembali memiliki 5,57% chance untuk critical

Dengan cara demikian, maka setelah 18x gagal, serangan ke 19 memiliki chance di atas 100% yang artinya pasti berhasil. Ini akan mencegah adanya kasus “tak pernah terjadi sekalipun dalam permainan”. Tambah lagi, peluang terjadinya critical

lebih dari 3x berturut2 sangatlah kecil. Karena starting chance lebih kecil daripada actual chance. Ini akan mencegah kasus "selalu terjadi dalam beberapa trigger berturut-turut"

Konstanta yang digunakan untuk setiap chance berbeda2. Konstanta ini diperoleh dengan melakukan uji coba dengan jumlah eksperimen hamper tak hingga, untuk membuktikan uji statistic secara global.

Namun, ternyata terdapat error pada konstanta chance lebih dari 30%. Error ini disebabkan dalam game ladder maksimal percentage yang ada sebesar 30%, Kesalahan ini sangat kecil, namun melebar menjadi sangat signifikan untuk konstanta chance besar.

Walaupun penggunaan PRD pada engine Warcraft 3 memiliki beberapa kelemahan, dikarenakan kurang pasnya kosntanta yang digunakan, namun ide dan konsep dasar PRD sangatlah brilian. Yang membuat PRD berguna untuk dimanfaatkan dalam random generator game lain.

Tetapi, system PRD tak selalu cocok digunakan dalam game. PRD akan efektif jika digunakan dalam game online dan strategy dimana event trigger erjadi berulang kali, namun dengan chance value yang cukup rendah. Ini akan membuat system membutuhkan algoritma yang menjamin keseimbangan game. Contohnya seperti pada game online yang tiap karakternya memukul monster berkali-kali, dan setiap serangan memiliki x% chance untuk mentrigger suatu event.

Namun untuk game tipe stragey yang lebih berkonsep turn-based, maka sebaiknya menggunakan random biasa, dikarenakan konsep PRD kurang pas diterapkan. Biasanya system turn-based memiliki trigger hanya beberapa kali (sedikit), namun memiliki chance occur yang cukup besar. Sehingga konsep PRD yang "memastikan akan terjadi" setelah beberapa trigger gagal, malah akan mengancurkan keseimbangan game.

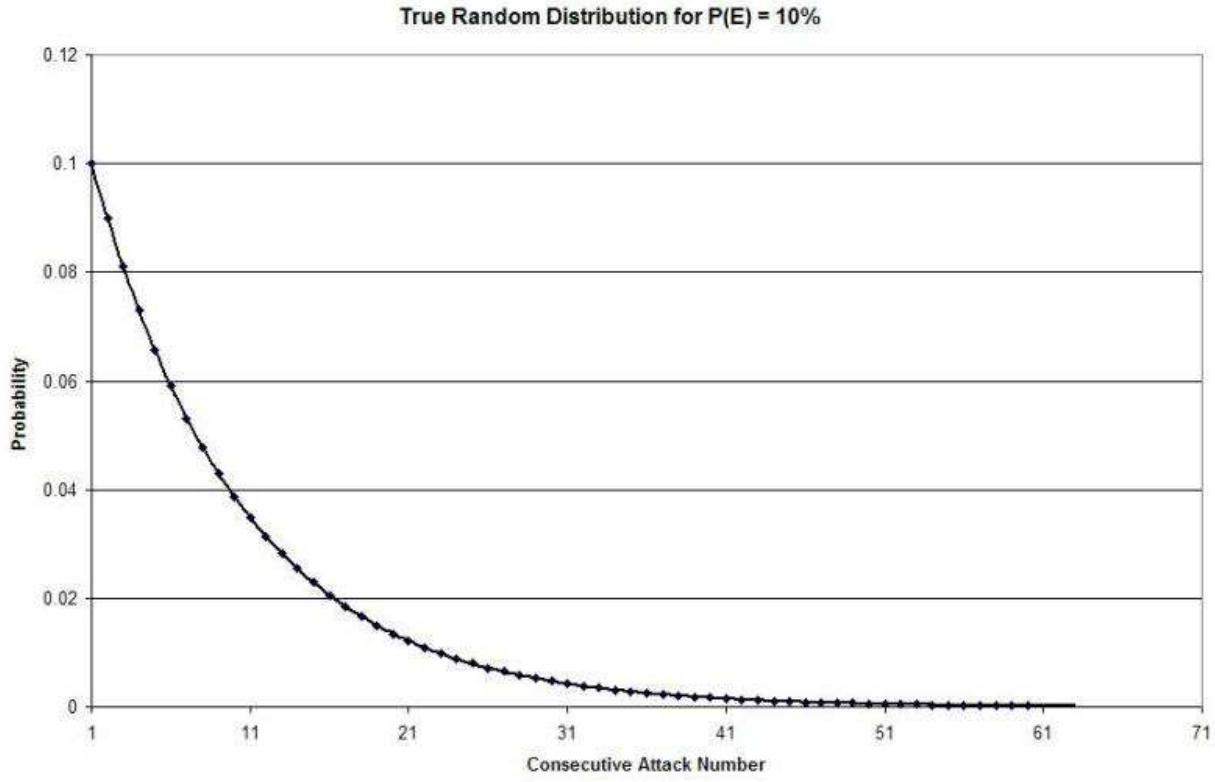
Theoritical			Actual		
P (E)	C	Max N	P (E)	C	Max N
5%	0.00380	263	5.0%	0.00380	263
10%	0.01475	67	10.0%	0.01475	67
15%	0.03222	31	15.0%	0.03222	31
20%	0.05570	17	20.0%	0.05570	17
25%	0.08474	11	24.9%	0.08474	11
30%	0.11895	8	29.1%	0.11895	8
35%	0.15798	6	33.6%	0.15798	6
40%	0.20155	4	37.8%	0.20155	5
45%	0.24931	4	41.6%	0.24931	4
50%	0.30210	3	45.7%	0.30210	3
55%	0.36040	2	49.4%	0.36040	3
60%	0.42265	2	53.0%	0.42265	3
65%	0.48113	2	56.4%	0.48113	2
70%	0.57143	1	60.1%	0.57143	2
75%	0.66667	1	63.2%	0.66667	2
80%	0.75000	1	66.7%	0.75000	1
85%	0.82353	1	70.3%	0.82353	1
90%	0.88889	1	75.0%	0.88889	1
95%	0.94737	1	81.3%	0.94737	1

3.2 Kurva Probabilitas PRD

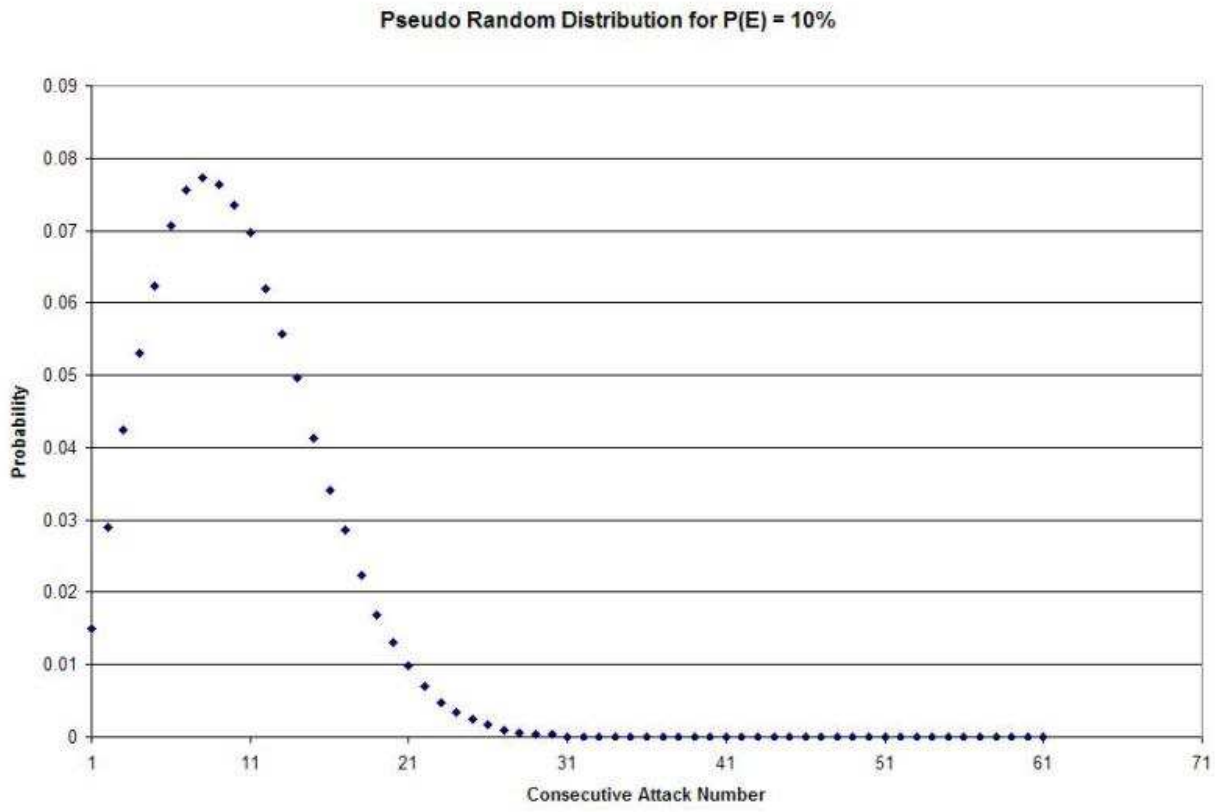
Untuk memahami PRD lebih jelas lagi, maka kita dapat membandingkan kurva PRD dengan kurva random distribution biasa. Anggaplah kita memiliki peluang terjadinya sebuah event sebesar 10%)P(E) = 10%). Jika menggunakan random distribution biasa, maka yang dilakukan adalah me-roll nilai 1-100. Jika hasilnya di bawah 10, maka event berhasil. Selain itu, event gagal.

Maka peluang kberhasilan event pada trigger pertama adalah 0.1. Pada trigger kedua, peluang kberhasilannya sebesar 0.09 (90% chance gagal pada trigger pertama x 10% chance berhasil di trigger kedua). Dan seterusnya dengan pola yaitu P(n) sebesar

$$\frac{P(E)}{(1-P(E))^{n-1}}$$



Sementara untuk kurva probabilitas PRD, maka kemungkinan berhasil untuk trigger pertama menjadi jauh lebi kecil, yaitu hanya sebesar 1,475%. Tetapi akan meningkat terus hingga melebihi 100%. Kemudian mengalami titik balik. Hal ini disebabkan sifat PRD yang melakukan penambahan chance value setiap event gagal terjadi.



4. KESIMPULAN

PRD yang digunakan dalam DotA cukup efektif dalam menangani factor balancing game. Namun terdapat beberapa kesalahan penggunaan konstanta pada prakteknya. Hal ini mungkin disebabkan developer game hanya mencari kosntanta sampai 30% chance, kemudian meregresikan untuk chance di atasnya, sehingga hasilnya kurang optimal.

5. DAFTAR PUSTAKA

[1] Munir, Ir. Rinaldi. *Diktat kuliah Kriptografi*. 2006. Bandung.

[2] http://forums.dota-allstars.com/index.php?showtopic=245439

[3] http://www.dotastrategy.com/forum/ftopic18287.html

6. SIGNATURE