10.1. Bit Error Rate Test

Na prvom OSI sloju, biti se fizički koduju i modulišu kako bi se omogućio što pouzdaniji i bezbedniji prenos. Kada se podaci prime njima se asocira odgovarajuća verovatnoća bitske greške (Bit *Error Rate* - BER), odnosno verovatnoća blok greške (*Block Error Rate* – BLER) koje su rezultat smetnji u prenosnom medijumu na mestu samog prijemnika.

Na drugom OSI sloju, sprovodi se zaštitno kodovanje radi povećanja otpornosti informacija na smetnje u kanalu. Dobijene informacione jedinice nazivaju se telegrami. Osnovno obeležje kodova ovog sloja je tzv. Hamingovo rastojanje (*Hamming Distance* - HD). Ono predstavlja najmanju razliku između dve ispravne kodne reči u sistemu izraženu u broju bita. U originalno poslatoj reči moguće je detektovati i ispraviti do HD-1 pogrešno prenetih bita. Ukoliko je broj grešaka u kodnoj reči veći, na prijemu će se detektovati neka druga kodna reč.

Greška koja postoji iznad drugog OSI sloja naziva se **rezidualna verovatnoća greške**. Ona predstavlja odnos broja nedetektovanih ili pogrešno detektovanih telegrama i ukupnog broja poslatih telegrama. Stoga se rezidualna verovatnoća greške može uzeti kao pokazatelj pouzdanosti prenosa. Ona zavisi od interferencije na kablovima, korišćenog fizičkog koda (npr. *Non-Return-to-Zero* - NRZ, *Manchester* kod itd.) i statističkog koda (telegrama).

Hamingovo rastojanje ima slisla uvesti samo ako se pouzdanost prenosa želi održati u određenim granicama. Kodovanje na drugom OSI ref. nivou smanjuje informacioni protok za fiksan digitalan protok. Ako se za dati kanal pretpostavi određena verovatnoća bitske greške (BER) i fiksira Hamingovo rastojanje, rezidualna verovatnoća greške će se povećavati sa veličinom telegrama. Visoka pouzdanost može se, dakle, postići investiranjem u fizičko kodovanje i redukciju BER-a i BLER-a na 1. OSI sloju uz fiksno Hamingovo rastojanje na 2. OSI sloju, odnosno smanjenjem veličine poslatih paketa kontrolom na 4. OSI nivou.

Mnoge komponente digitalnih komunikacionih sistema moraju zadovoljiti minimalne kriterijume u pogledu verovatnoće bitske greške $p(\varepsilon)$. Za dati sistem, $p(\varepsilon)$ se može proceniti poređenjem izlazne sekvence bita sa unapred definisanom ulaznom (pseudoslučajnom) sekvencom. Svako odstupanje izlazne sekvence od ulazne označava se kao greška, a odnos pogrešno detektovanih bita ε i ukupnog broja prenetih bita n predstavlja procenu stvarne verovatnoće greške i označava se sa $\hat{p}(\varepsilon)$ odnosno BER. Ovaj postupak poznat je pod nazivom **Bit Error Rate Test** (BERT).

Kvalitet procene stvarne verovatnoće greške kanala pomoću BERT-a poboljšava se sa svakim prenetim bitom. Ovo se može izraziti kao

$$\lim_{n\to\infty} \hat{p}(\varepsilon) = \lim_{n\to\infty} \frac{\varepsilon}{n} = p(\varepsilon) \tag{10.1}$$

Da bi se osiguralo da $\hat{p}(\varepsilon)$ predstavlja dovoljno tačnu aproksimaciju stvarne verovatnoće greške $p(\varepsilon)$, važno je preneti dovoljan broj bita kroz kanal. Nažalost, tačna vrednost bi se dobila samo ukoliko bi test trajao neograničeno dugo, pa je za neko razumno (ograničeno)

vreme merenja potrebno odrediti minimalan broj prenetih bita n kako bi BERT dao statistički prihvatljiv rezultat.

U većini slučajeva dovoljno je proveriti da li je $p(\varepsilon)$ bolje od nekog unapred definisanog standarda. Drugim rečima, potrebno je odrediti samo gornju granicu stvarne verovatnoće bitske greške. U mnogim telekomunikacionim sistemima standardima se zahteva da $p(\varepsilon)$ bude bolje od 10^{-10}. Ideja dodeljivanja statističkog nivoa poverenja ovoj gornjoj granici, može se iskoristiti za formulisanje zahteva da $p(\varepsilon)$, sa kvantitativno izraženom sigurnošću, bude manje od zahtevane gornje granice (10^{-10}). Osnovna prednost ovakvog pristupa ogleda se u mogućnosti „žrtvovanja“ preciznosti procene zarad neophodnog skraćenja trajanja merenja.

10.1.1. Statistički nivo poverenja

Statistički nivo poverenja CL, u kontekstu BERT-a, definisan je kao verovatnoća, zasnovana na skupu rezultata merenja, da je stvarna verovatnoća greške bolja od neke zahtevane vrednosti. Za svrhe ove definicije usvaja se da je stvarna verovatnoća $p(\varepsilon)$, ona vrednost BERT-a koja se dobija kada vreme merenja teži beskonačnosti. Kada se primeni na procenu stvarne verovatnoće $p(\varepsilon)$, ova definicija statističkog nivoa poverenja može se preformulisati kao aposteriori verovatnoća, zasnovana na ε detektovanih grešaka od n prenetih bita, da je stvarna $p(\varepsilon)$ bolja od zahtevane vrednosti γ (npr. 10^{-10}). Matematički, to se može zapisati kao

$$CL = P\left[p(\varepsilon) < \gamma \mid \varepsilon, n\right] \tag{10.2}$$

Zbog toga što je statistički nivo poverenja po definiciji verovatnoća, on može uzimati vrednosti od 0 do 100 %.

Nakon izračunavanja nivoa poverenja CL, možemo sa verovatnoćom od CL procenata tvrditi da je $p(\varepsilon)$ bolje od γ. Druga moguća interpretacija ove definicije je da, ako ponavljamo BERT mnogo puta i za svaki interval merenja izračunavamo $\hat{p}(\varepsilon) = \varepsilon / n$, očekujemo da $\hat{p}(\varepsilon)$ bude manje od γ u CL procenata od ukupnog broja ponovljenih merenja.

10.1.2. Izračunavanje statističkog nivoa poverenja

Izračunavanje statističkog nivoa poverenja zasniva se na binomijanoj funkciji raspodele gustine verovatnoće [1, 2]. Binomijalna funkcija raspodele definisana je kao

$$p_n(k) = \binom{n}{k} p^k (1-p)^{n-k}, \tag{10.3}$$

gde je

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{10.4}$$

$p_n(k)$ predstavlja verovatnoću da se k događaja (bitskih grešaka) pojavi u n pokušaja (prenetih bita), gde je p verovatnoća pojavljivanja događaja u pojedinačnom pokušaju (bitska greška).

Ako nas zanima verovatnoća da se N ili manje događaja pojavi u n pokušaja, koristimo se kumulativnom funkcijom binomijalne raspodele

$$P[\varepsilon \le N] = F[N] = \sum_{k=0}^{N} p_n(k) = \sum_{k=0}^{N} \binom{n}{k} p^k (1-p)^{n-k} \tag{10.5}$$

Slično je

$$P[\varepsilon > N] = 1 - P[\varepsilon \le N] = 1 - F[N] = \sum_{k=N+1}^{n} \binom{n}{k} p^k (1-p)^{n-k} = 1 - \sum_{k=0}^{N} \binom{n}{k} p^k (1-p)^{n-k} \tag{10.6}$$

Tipično merenje zasnovano na statističkom nivou poverenja započinje usvajanjem zadovoljavajuće vrednosti za CL i hipotetičke maksimalne vrednosti za p (verovatnoće greške ako se prenosi samo jedan bit). Označimo izabranu gornju granicu za p sa γ. U opštem slučaju, γ se bira u skladu sa nametnutom granicom ukupne verovatnoće greške od strane standarda (npr. ako se standardom zahteva da je $p(\varepsilon) \le 10^{-10}$, biramo $\gamma = 10^{-10}$ i nivo poverenja od, recimo, 99 %).

Zatim se koristimo gornjom relacijom da bismo odredili verovatnoću $P[\varepsilon > N \mid \gamma]$, zasnovanu na γ, da će se pojaviti više od N grešaka, ako se prenosi ukupno n bita. Ukoliko se za vreme stvarnog testiranja dogodi manje od N grešaka, i ako je $P[\varepsilon > N \mid \gamma]$ veliko, moguća su dva zaključka: (1) imali smo sreće, ili (2) stvarna vrednost za p je manja od pretpostavljene vrednosti γ. Ukoliko ponavljamo test iznova i iznova i nastavimo da primamo manje od N grešaka, postajemo sve pouzdaniji u zaključak (2), pa vrednost $P[\varepsilon > N \mid \gamma]$ definiše naš nivo poverenja u zaključak (2).

Ako je $\gamma = p$, postoji velika verovatnoća detekcije više od N grešaka, pa ako, u stvarnosti, detektujemo manje od N grešaka, zaključujemo da je p verovatno manje od γ i kao verovatnoću ispravnosti tog zaključka (nivo poverenja) usvajamo $P[\varepsilon > N \mid \gamma]$. Drugim rečima, CL posto smo uvereni da je stvarna verovatnoća bitske greške $p(\varepsilon)$ manja od od γ.

Izražen preko kumulativne funkcije binomijalne raspodele, statistički nivo poverenja može se definisati i kao apriori verovatnoća, što je sa stanovišta merenja daleko praktičnije

$$CL = P[\varepsilon > N \mid \gamma] = 1 - \sum_{k=0}^{N} \binom{n}{k} p_h^k (1-p_h)^{n-k} \tag{10.7}$$

Da bismo odredili potreban broj bita n za prenos, usvajamo hipotetičku vrednost za p zajedno sa željenim nivoom poverenja CL i rešavamo gornju jednačinu po n, za N ili manje detektovanih grešaka. Rešavanje po n i N veoma je teško, pa je potrebno usvojiti nekoliko aproksimacija. Ako je $np > 1$ (tj. prenosimo makar $1 / p$ bita) i k je istog reda veličine kao np, tada važi Poasonova (Poisson) teorema [1] i binomijanu raspodelu možemo aproksimirati Poasonovom.

$$p_n(k) = \binom{n}{k} p_h^k (1-p_h)^{n-k} \xrightarrow[n\to\infty]{} \frac{(np)^k}{k!} \mathrm{e}^{-np} \tag{10.8}$$

$$\sum_{k=0}^{N} p_n(k) = \sum_{k=0}^{N} \frac{(np)^k}{k!} \mathrm{e}^{-np} \tag{10.9}$$

Izraz za *CL* sada postaje

$$CL = 1 - \sum_{k=0}^{N} \frac{(np)^k}{k!} \mathrm{e}^{-np} \,, \tag{10.10}$$

odakle je

$$n = -\frac{\ln(1-CL)}{p} + \frac{\ln\left[\sum_{k=0}^{N} \frac{(np)^k}{k!}\right]}{p} \tag{10.11}$$

Za $N = 0$, drugi član u gornjem izrazu je 0, pa je jednačina jednostavna za rešavanje. Rešenja za $N > 0$, se ne mogu, u opštem slučaju, naći analitički, ali se mogu izračunati numeričkim metodama, npr. pomoću računara. Važno je pri tome uočiti da proces rekurzivnog računa, koji sledi iz gornje jednakosti, sigurno konvergira ka tačnom rešenju, bez obzira na usvojenu početnu vrednost zahvaljujući monotonosti logaritamske funkcije. Nažalost konvergencija je spora i potreban je velik broj koraka da bi se došlo do rešenja. Ubrzanje se može dobiti ako se prvo analitički izračuna vrednost $n(N = 0) = n_0$, a zatim se ona iskoristi kao početna vrednost.

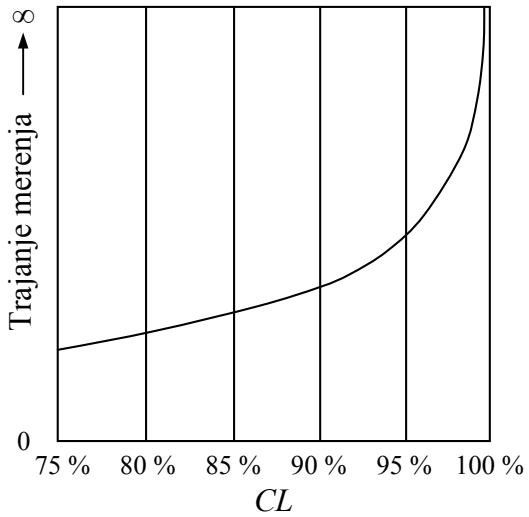
Za $N = 1$, izračunavanje se sprovodi rekurzivno

$$\begin{aligned} n_0 &= -\frac{\ln(1-CL)}{p} \\ n_1^{(0)} p &= n_0 p + \ln\left(\sum_{k=0}^{N} \frac{(n_0 p)^k}{k!}\right) \\ n_1^{(1)} p &= n_0 p + \ln\left(\sum_{k=0}^{N} \frac{(n_1^{(0)} p)^k}{k!}\right) \\ &\vdots \end{aligned} \tag{10.12}$$

$$n_1^{(\infty)} p = n_0 p + \ln\left(\ldots \ln\left(n_0 p + \ln\left(n_0 p + \sum_{k=0}^{N} \frac{(n_0 p)^k}{k!}\right)\right)\right) \tag{10.13}$$

Kompletna procedura za određivanje potrebnog broja prenetih bita sastoji se iz sledećih koraka:

1. Bira se hipotetička vrednost za p. Ovo je vrednost bitske verovatnoće greške koju želimo da proverimo. Npr. ako želimo da pokažemo da je $p(\varepsilon) \leq 10^{-10}$, usvojićemo da je $p = 10^{-10}$.
2. Bira se željeni nivo poverenja. Ovde smo prinuđeni da trampimo pouzdanost sa trajanjem merenja.. Da bi se minimizovalo vreme testa, potrebno je usvojiti najmanji razumi nio poverenja. Treba ipak imati na umu da je zavisnost vremena merenja od statističkog nivoa poverenja logaritamska, kao što je prikazano na slici 10.1.



Slika 10.1. Zavisnost trajanja BERT-a od usvojene vrednosti statističkog nivoa poverenja

3. Reši se jednačina

$$n = -\frac{\ln(1-CL)}{p} + \frac{\ln\left(\sum_{k=0}^{N}\frac{(np)^k}{k!}\right)}{p} \tag{10.14}$$

   U većini primena ovo je pojednostavljeno pretpostavkom da se nijedna greška neće detektovati prilikom testa ($N = 0$).

4. Izračuna se potrebno trajanje merenja. Ako je v_b bitska brzina signalizacije u sistemu, potrebno vreme merenja je n / v_b.

10.1.3. Primer korišćenja *CL* da bi se procenilo $p(\varepsilon)$

Mnogi telekomunikacioni sistemi deklarišu potrebnu vrednost za $p(\varepsilon)$ kao10^{-10} ili manju. Pretpostavimo da moramo testirati dve linije sa clock/data-recovery čipovima, MAX3675 (622 Mbps) i MAX3875 (2,5 Gbps), da bismo ustanovili njihovu usaglašenost sa standardima.

Prvo usvajamo da je $p_h = 10^{-10}$. Želeli bismo da nam test da 100 % pouzdanosti, ali to bi zahtevalo beskonačno vreme testiranja. Zato usvajamo nivo poverenja od 99 %. Nalazimo potreban broj bita za prenos n koristeći različite vrednosti za N (0, 1, 2, 3, itd.). Rezultati su prikazani u tabeli 10.1.

Iz tabele 10.1 se vidi da, ako nijedan bit nije detektovan za 18 s u 2,5 Gbps sistemu, tada imamo nivo poverenja od 99 % da je $p(\varepsilon) \leq 10^{-10}$. Ako se detektuje jedna greška u 27 s ili dve greške u 34 s, rezultat je identičan: 99 % verovatnoće da je $p(\varepsilon) \leq 10^{-10}$.
Da bi se konstrukcija instrumenta i procedura merenja uprostile, možemo usvojiti da uvek prenosimo 10^{11} bita. Ako je na prijemnoj strani broj pogrešno detektovanih bita manji ili jednak 3, uređaj je prošao test i sa verovatnoćom od 99 % tvrdimo da je $p(\varepsilon) \leq 10^{-10}$.

Tabela 10.1. Procena verovatnoće bitske greške (CL = 99 %, $p_h = 10^{-10}$)

Broj detektovanih grešaka N	Potreban broj bita n	Vreme merenja za 622 Mbps (s)	Vreme merenja za 2,5 Gbps (s)
0	$4.61 \cdot 10^{10}$	74	18
1	$6.64 \cdot 10^{10}$	106	27
2	$8.40 \cdot 10^{10}$	135	34
3	$1.00 \cdot 10^{11}$	161	40
4	$1.16 \cdot 10^{11}$	186	47

10.1.4. Skraćivanje vremena merenja opterećivanjem sistema

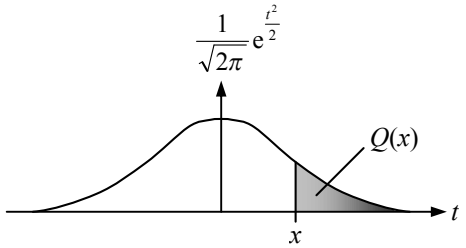
U praksi je za niže brzine signalizacije neophodno još više redukovati vreme testiranja. Dan Wolaver je pronašao metod za skraćenje vremena testiranja opterećivanjem sistema [3]. Ovaj metod zasniva se na pretpostavci da je dominantan uzrok bitske greške termički (Gausov) šum na ulazu prijemnika i da se uticaj džitera i drugih potencijalnih uzroka grešaka može zanemariti. Za sisteme za koje je ova pretpostavka ispravna, odnos signal-šum može se veštački smanjiti ubacivanjem fiksnog slabljenja u transmisioni put (slabljenje utiče na nivo signala, ali ne i na nivo šuma na prijemu). U prethodnom primeru (MAX3675 i MAX3875), gde je brzina signalizacije izuzetno velika, pokazuje se da usled džitera i nelinearnosti prijemnog pojačavača, nije zadovoljena pretpostvka o dominantnom uticaju Gausovog šuma.

Srećom, termički šum ima najveći uticaj na neispravnu detekciju simbola u sistemima sa nižom brzinom signalizacije, gde je i najveći interes za smanjenje vremena testiranja. Prema [4, 5] verovatnoća bitske greške može se, u opštem slučaju, izračunati kao

$$p(\varepsilon) = Q\left(\frac{\sqrt{SNR}}{2}\right) \tag{10.15}$$

gde je $Q(x)$ komplementarna greška normalne raspodele („Q" funkcija, koja se može naći u mnogim udžbenicima [6]) data sa

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \mathrm{e}^{\frac{t^2}{2}} dt \tag{10.16}$$



Slika 10.2. Komplementarna funkcija greške *Q*

Verovatnoća greške se povećava kako se odnos signal-šum smanjuje. Kada se u liniju ubaci fiksno slabljenje *a*, snaga signala se smanji *a* puta, a snaga šuma na prijemu ostaje nepromenjena. Na taj način je smanjen odnos signal-šum *a* puta, pa je verovatnoća greške $p(\varepsilon)$ povećana za faktor određen Q funkcijom.

Sada se ranije opisan postupak može primeniti, ali sa modifikovanom hipotetičkom vrednošću p_h. Rezultat je isti, ali je vreme merenja znatno kraće.

Osnovna mana optrećivanja sistema je potreba za daleko osetljivijim prijemnikom, odnosno za mnogo preciznijim merenjem, zbog toga što ekstrapolacija rezultata na opseg van opterećenja multiplicira grešku usled zaokruživanja, odsecanja, merne nesigurnosti itd.

10.1.5. Uticaj redudantnosti protokola na trajanje merenja

Važno je imati na umu da se izračunata vrednost za potreban broj prenetih bita *n* odnosi na informacione, a ne na sve bite. Zbog toga se prilikom BERT-a izbegava signaliziranje uz korišćenje komunikacionog protokola kad god je to moguće (signalizacija bez uokviravanja), jer bi se zahtevalo ubacivanje dodatnih neinformacionih bita za uokviravanje poruka (redudantnost protokola), čime se dodatno produžava vreme merenja. Ovo, nažalost, nije moguće uvek izbeći kao npr. u situacijama gde signala prolazi kroz javnu komutacionu mrežu, kada je neophodno obezbediti odgovarajuću signalizaciju i sistemske poruke kako bi mreža uopšte prenela poslate pakete ili ih prosledila do odredišta.

Ako je redudantnost korišćenog protokola velika, potrebno trajanje merenja može biti znanto veće od procenjenog. Uzmimo npr. da je redudantnost upotrebljenog protokola 10 %. Tada je kroz kanal potrebno preneti 10 % više bita, pa je i vreme merenja povećano za 10 %.

Sa druge strane, greška se ravnopravno može javiti i na informacionim bitima kao i na nekom od bita za uokviravanje. Ako se greška javi na bitima za uokviravanje, koji su neophodni za rutiranje ili dekodovanje informacione sekvence, prenos će biti prekinut i merenje neće biti ispravno.