

Pendeteksian Bit Error Dalam Transmisi Data Dengan Menerapkan Cyclic Redudancy Check

¹⁾Matias Julius Fika Sirait

STMIK Budi Darma Medan, Jl. SM. Raja No. 336, Sumatera Utara, Indonesia
E-Mail : matiassirait@gmail.com

²⁾Sony Bahagia Sinaga

AMIK STIEKOM Sumatera Utara, Jl. A.H Nasution No. 19, Sumatera Utara, Indonesia
E-Mail : sony@amikstiekomsu.ac.id

ABSTRACT

The communication path that will physically connect the two technologies conceptually works together such as cables. A special feature of a channel that resembles a cable is where the bits will be forwarded in the same order along with the bits sent. Data link layers have specific functions, this function includes starting from providing interfaces for services that are good for the network layer. Communication flows often make mistakes, sometimes having limited data rates and experiencing propagation delays other than zero between when bits are sent when the bit is received. This limitation is an implication of the importance of the efficiency of data transfer. Delivery of information in the telecommunications world will often occur errors in the data to be sent. This error is caused by a disturbance at the physical level, which is a disruption of the transmission line media, such as interference with electromagnetic radiation, cross communication, lightning or noise disturbance. This interference causes the information received does not match the information sent. The Cyclical Redundancy Check method, or CRC, is a method for handling error detection, this method uses binary numbers. The CRC data detection model is sent perframe consisting of a long row of bits for each frame.

Keywords: Bit Error, Transmission, CRC, Data Communication

PENDAHULUAN

Pada dunia telekomunikasi proses pengiriman data dan informasi sangat penting. Adakalanya informasi yang sudah diterima berbeda dengan informasi yang dikirimkan[1]. Penyebab terjadinya adalah adanya trouble yang terjadi di level fisik, yakni di media atau saluran komunikasi yang digunakan ada gangguan radiasi elektromagnetik, silang komunikasi, petir atau adanya gangguan noise.

Kesalahan dapat terjadi pada tiap bagian dari sistem komunikasi data. Perlu adanya langkah-langkah untuk proses perbaikan melalui evaluasi masalah terhadap apa penyebab terjadinya kesalahan dan menyelidiki kemungkinan terjadinya kesalahan dalam proses pengiriman data maupun data pusat terminal[2].

Adapun perumusan masalah yang akan dibahas dalam penelitian ini antara lain :

1. Bagaimana mendeteksi *bit error* menggunakan *cyclic redudancy check*.
2. Bagaimana mengatasi *bit error* dalam kesalahan pengiriman data.

Penelitian ini akan menghasilkan suatu kualitas keputusan yang baik. Adapun rincian dari urgensi dari penelitian ini adalah :

1. Mengetahui cara kerja *cyclic redudancy check* dalam pendeteksi *bit error*.
2. Mengatasi permasalahan *bit error*.

DASAR TEORI

2.1. Komunikasi

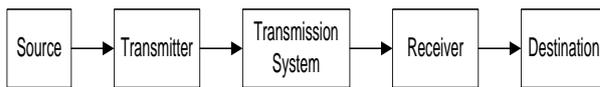
Komunikasi memiliki arti sebagai proses untuk penyampaian atau penyebarluasan data dan informasi, sedangkan informasi adalah berita, isi pikiran, juga pendapat dalam berbagai bentuk[3]. Kekurangan dan kelemahan cara komunikasi manusia, yaitu:

1. Posisi lokasi antara pengirim dan penerima yang berjauhan (menyeberangi lautan),
2. Durasi waktu yang lama untuk penyampaian pesan,
3. Biaya yang relatif mahal.

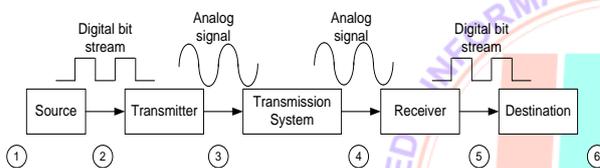
Komunikasi data merupakan sebuah cara mengirimkan data dengan memakai sistem transmisi elektronik/digital dari satu komputer ke komputer lain atau dari satu komputer ke terminal tertentu[4]. Saat ini telah terjadi pelonjakan ilmu yang pesat di

bidang ilmu komputer demikian juga dalam komunikasi data yang secara pesat mengubah peran teknologi, produksi dan perusahaan yang sekarang merupakan kombinasi industri komunikasi dan komputer[5][6], antara lain:

- Persamaan fundamental antara paket *data processing* (komputer) dengan komunikasi data (perangkat transmisi dan pengalihan).
- Fundamental antara proses komunikasi data *voice* (suara) dan video tidak ada perbedaan.
- Jalur-jalur antara *Single-processor computer*, *multi-processor computer*, baik jaringan lokal, baik jaringan metropolitan dan bahkan jaringan jarak jauh sudah kabur.



Gambar 1. Kerangka Komunikasi Dasar



Gambar 2. Proses Transmisi Data

Komputer bekerja berdasarkan data dan program. Data merupakan bentuk lain dari informasi. Satu data dapat di bedakan dari data lainnya karena memiliki bentuk yang baku. Adapun program berfungsi untuk mengolah data di dalam komputer, tersimpan di dalam RAM dan Harddisk, menjadi sesuatu yang diinginkan dan dapat dimengerti oleh manusia. Oleh karena itu, komputer berkomunikasi memakai data yang diproses oleh sebuah program serta mengolah data tersebut menjadi informasi yang dimengerti pengguna komputer.



Gambar 3. Model Komunikasi Data

2.2. Cek Paritas

Pendeteksian kesalahan yang paling sederhana pada komunikasi data adalah melampirkan *bit* paritas ke ujung blok data. Penerima akan selalu menguji semua

karakter yang diterima dari pengirim dan bila total jumlah akhirnya adalah 1 atau ganjil, diasumsikan tidak akan terjadi eror. Bila satu *bit* (atau apapun angka *bit* yang ganjil) dibalik secara salah selama transmisi (misalnya 1100011), maka sipenerima akan selalau mencek apakah ada kesalahan. Apapun hasilnya, bila ada dua (atau semua angka bernilai genap) *bit* akan dibalik karena terjadi suatu kesalahan, selanjutnya akan muncul kesalahan yang tidak dapat terdeteksi. Biasanya paritas genap dipakai untuk proses transmisi *synchronous*.

Penggunaan *bit* paritas bukanlah suatu teknik pembuktian yang sia-sia, gangguan-gangguan nois yang biasanya sering dan cukup panjang untuk dapat merusak lebih dari satu *bit*, utamanya pada *rate* data yang bernilai tinggi.

2.3. Cyclic Redundancy Check

Ciri pendeteksian kesalahan paling umum serta paling hebat adalah metode *Cyclic Redundancy Check* (CRC), dengan adanya blok *bit k-bit* atau pesan, *transmitter* dalam mengirimkan suatu deretan pesan *n-bit*, ini disebut sebagai *Frame Check Sequence* (FCS)[7], sehingga *frame* yang dihasilkan, terdiri dari *k+n bit*, dapat dibagi dengan nyata oleh beberapa nomor atau blok yang sebelumnya sudah ditetapkan. Kemudian Penerima membagi *frame* yang datang dengan nomor tersebut dan bila tidak ada yang sisa, maka dianggap tidak ada lagi terdapat kesalahan.

Prosedur dalam menjelaskan hal ini boleh dijelaskan dengan tiga cara, yakni modulo 2 aritmatik, polinomial dan logik digital.

2.4. Polinomial

Model kedua untuk mengamati proses CRC adalah dengan menjelaskan seluruh nilai sebagai polinomial dalam suatu model variabel X, dengan koefisien – koefisien biner. Koefisien berhubungan dengan bit – bit dalam biner. Jadi, untuk $M = 110011$, diperoleh $M(X) = X^5 + X^4 + X + 1$, dan untuk $P = 11001$, diperoleh $P(X) = X^4 + X^3 + 1$. Operasi aritmatik lagi – lagi berupa modulo 2.

Error E(X) hanya akan menjadi tak terdeteksi bila dibagi dengan $P(X)$. Hal ini berarti bahwa semua kesalahan berikut ini tidak dibagi dengan pilihan $P(X)$ yang sesuai dan karenanya mampu dideteksi:

- Setiap *bit* kesalahan tunggal.
- Setiap *bit* dengan kesalahan ganda, selama $P(X)$ memiliki sedikitnya tiga 1s.
- Apapun angka kesalahan yang ganjil, selama $P(X)$ memuat faktor $(X + 1)$.

4. Bagaimanapun banyaknya kesalahan dimana panjangnya kurang dari panjang polinomial pembagai, yakni kurang dari atau setara dengan panjang FCS.
5. Error komunikasi yang besar sekali.

METODE PENELITIAN

Dalam pelaksanaan penelitian ini aktivitas yang dilakukan dalam penelitian ini yaitu mengadakan studi eksplorasi terhadap konsep dan algoritma yang akan digunakan dalam pembangunan, melakukan analisis terhadap permasalahan yang ada, melakukan perancangan sistem berdasarkan hasil analisis tersebut, melakukan implementasi sistem tersebut dengan perangkat yang telah ditentukan dan yang terakhir adalah mengadakan testing terhadap sistem tersebut.

HASIL DAN PEMBAHASAN

Untuk mendapat nilai CRC melakukan perhitungan sebagai berikut :

1. Bit data yang akan dikirim oleh transmitter.

Pesan akan ditambahkan dengan nilai bit nol sebanyak lebar bit polinomial.

Pesan = 110101
 Polinomial = 101

Dalam hal ini, lebar bit polinomial adalah 2, maka pesan ditambah dengan nilai 00 menjadi 11010100, dan akan dibagi dengan polinomial. Pembagian tersebut sama dengan melakukan XOR pada semua bit yang dibagi dengan bit pembagi.

Perhitungannya [p(x)] adalah sebagai berikut:

$$\begin{array}{r}
 11010100 / 101 \\
 \underline{11010100} \\
 101 \\
 \underline{111} \\
 101 \\
 \underline{100} \\
 101 \\
 \underline{010} \\
 101 \\
 \underline{110} \\
 101 \\
 \underline{11} \quad \text{sis} = \text{CRC} \\
 \text{checksum}
 \end{array}$$

Pesan yang didapat dengan CRC [px(x)] = 11010111

2. Perhitungan bit data yang diterima oleh receiver, dapat dilakukan dengan dua cara:

Cara I

- a. Receiver berfungsi untuk memisahkan pesan dan checksum, lalu akan menghitung checksum untuk pesan setelah menambahkan bit nol sebanyak lebar bit polinomial.
- b. Receiver akan membandingkan kedua checksum tersebut, termasuk yang diterima dan yang dihitung.
- c. Jika checksum tersebut sama besar, maka tidak terjadi error. Sebaliknya, bila kedua checksum tidak sama maka telah terjadi error.

Pesan = 11010111
 Checksum pesan yang diterima = 11
 Polinomial = 101
 11010100 / 101

$$\begin{array}{r}
 11010100 \\
 \underline{101} \\
 111 \\
 \underline{101} \\
 100 \\
 \underline{101} \\
 010 \\
 \underline{101} \\
 110 \\
 \underline{101} \\
 11 \quad \text{sis} = \text{CRC} \\
 \text{checksum}
 \end{array}$$

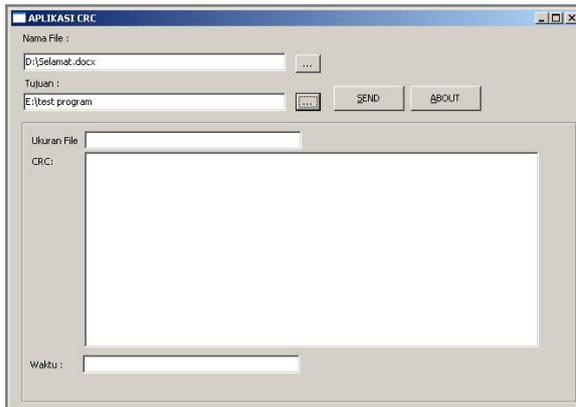
Cara II

1. Receiver akan menghitung checksum untuk keseluruhan pesan.
2. Kemudian memeriksa apakah hasilnya sama dengan nol (berarti tidak terjadi error).

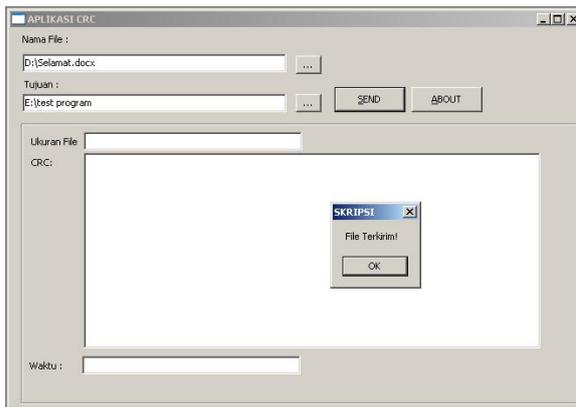
Pesan = 11010111
 Checksum pesan yang diterima = 11
 Polinomial=101
 11010111 / 101

$$\begin{array}{r}
 11010111 \\
 \underline{101} \\
 111 \\
 \underline{101} \\
 100 \\
 \underline{101} \\
 111 \\
 \underline{101} \\
 101 \\
 \underline{101} \\
 00 \quad \text{checksum} = 0 \\
 \text{(tidak terdapat error)}
 \end{array}$$

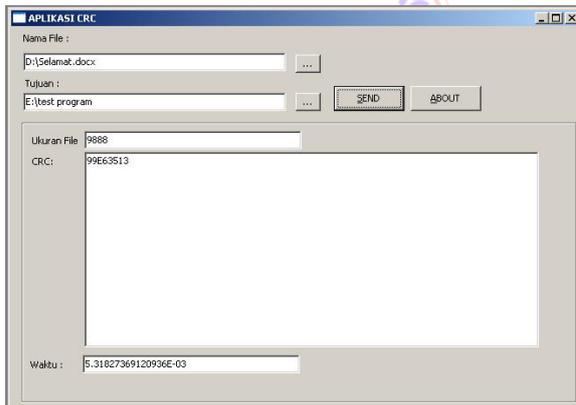
Untuk lebih jelasnya pada penerapan pengujian dapat dijelaskan dengan gambar dan tampilan form berikut ini:



Gambar 4. Pengisian File Address



Gambar 5. Pesan Yang Terkirim



Gambar 6. Hasil Proses Nilai Checksum

- BERBASIS CLIENT-SERVER,” *Maj. Ilm. INTI (Informasi dan Teknol. Ilmiah)*, vol. 13, no. 2, pp. 141–145, 2018.
- [3] S. Syamsu, “PENINGKATAN PERFORMA PROXY SERVER BERBASIS SQUID DENGAN TUNING PARAMETER KONFIGURASI,” *J. Inspir.*, vol. 2, no. 2, pp. 41–47, 2012.
- [4] W. Sugeng, “Jaringan Komputer Dengan TCP/IP,” *Bandung Modul.*, 2010.
- [5] S. B. Sinaga and Y. Hasan, “Pengukuran Kualitas Jaringan Internet Dengan Sinyal 3G Lte Pada STMIK Budi Darma Medan dengan Metode Quality Of Service (QoS),” *Media Inf. Anal. dan Sist.*, vol. 2, no. 2, pp. 26–29, 2018.
- [6] S. B. Sinaga, “ANALISA JARINGAN VOIP DENGAN SESSION INITIATION PROTOCOL MENGGUNAKAN MEAN OPINION SCORE.”
- [7] G. Natalia, T. Suryani, and A. C. R. Check, “Implementasi Encoder dan Decoder Cyclic Redundancy Check Pada TMS320C6416T,” *J. Tek. POMITS*, vol. 3, no. 1, pp. 92–97, 2014.

DAFTAR PUSTAKA

- [1] E. Sutanta, “Komunikasi data dan jaringan komputer,” *Yogyakarta Graha Ilmu*, 2005.
- [2] R. W. Simanullang, H. Sunandar, and S. B. Sinaga, “ANALISA DAN IMPLEMENTASI METODE RADIO FREQUENCY IDENTIFICATION PADA PERPARKIRAN MALL