Research on Packet Loss Issues in Unidirectional Transmission

Lin Honggang
School of Network Engineering, Chengdu University of Information Technology, Chengdu, 610225, China
linhg@cuit.edu.cn

Abstract—The unidirectional transmission technology is designed to protect the confidentiality of data on the high assurance network. It allows data to transmit only in one direction and prevents the use of acknowledgements or other connection-oriented mechanisms. This makes packet loss become a key issue in unidirectional transmission because of its influence on reliability and performance. In this paper, we build test platform of unidirectional transmission to research on packet loss issues, measure the loss data in unidirectional transmission, and analyze the correlation of the loss rate and the transmission rate, the data packet load. We use these empirical measurements to derive a Gilbert model for the characterization of Packet loss process in unidirectional transmission. The research results can help in reducing packet loss, improving the performance, and designing a good error correction coding scheme for unidirectional transmission.

Index Terms—unidirectional transmission, reliability, packet loss rate, packet load, transmission rate

I. INTRODUCTION

With the rapid development of electronic government, electronic commerce and so on, transmitting data from the external network to internal network becomes more and more frequent in the organizations. It is becoming important to provide a security data transmission mechanism for preventing intrusions and ensuring the confidentiality of data stored on internal network. Although we can use a firewall, intrusion detection and other security measures, but these techniques are based on software logic isolation and unable to meet the security requirements of important data. Traditionally, the approach to solving this problem is isolates the internal and external network physically and the transfer of electronic data therefore has to take place manually, using a USB stick, CD or similar device. Unfortunately, this approach is never real-time, time-consuming and potentially security risky. Then, the network pump [1, 2, 3] was proposed to be an effective technology for isolation internal and external network effectively and ensuring the security of information exchange between internal and external network. But the study found that network pump can not eliminate all covert channels and strictly prevent disclosure, but only reduce the covert channel risk by pragmatic engineering and parameter tweaking[4,5].Now, Data diodes[5,6,7] are generally designed to protect the confidentiality of data on the higher classified system. Data diode is a commercial product that utilizes unidirectional transmission technology. The unidirectional transmission technology allow data to travel only in one direction for guaranteeing information security and it can be implemented between networks where there is a requirement for data to be sent from the less classified or sensitive computer network to the more classified network and there is a need to protect the confidentiality of data on the higher classified system. Physical transfer can only occur in one direction, and it is impossible to transfer data back in the opposite direction. Since the technology can be physically validated that there is no reverse data flow, it has no covert channel. As no signaling, acknowledgement, and other connection-oriented mechanisms are allowed, how can all of the mentioned functionalities be ensured with a sufficient quality of service? To solve the reliability issue for unidirectional transmission, some of the strategies are proposed to decrease the chance of data loss and corruption. It is possible to decrease the chance of data loss by transferring same data multiple times, increasing the size of the kernel network buffers, adjusting the process priorities and using FEC (forward error correction)[5,6,7]. A critical issue for such applications of unidirectional transmission is the manner in which packet losses occur within the unidirectional network. Research on packet loss issues in unidirectional transmission can reduce the packet loss rate dramatically. On the other hand, if we know the loss patterns, we may be able to get a better assumption for designing protocols to reduce the packet loss dramatically and helps in making good design decisions about FEC for unidirectional transmission. In the literatures [5,6,7], the relationship between the packet loss rate and the transmission rate is analyzed simply. But we find that transmission rate and packet load result in packet loss in unidirectional transmission. In this paper, we build test platform of unidirectional transmission to research on packet loss issues, measure the loss data in unidirectional transmission, and analyze the correlation of the packet loss rate and the transmission rate, the data packet load.

II. TEST PLATFORM OF UNIDIRECTIONAL TRANSMISSION

The unidirectional transmission technology is designed to protect the confidentiality of data on the high assurance network. Many unidirectional transmitting systems are used in commercial, government and defense applications.
Douglas [8] provides a prototype design description of a low bandwidth data diode for data export and auditing. A unidirectional transmitting system is used in industrial control systems in literature [9]. Okhravi [10] uses unidirectional transmission technology to build a trustworthy cyber infrastructure. The physical nature of unidirectional transmission only allows data to pass from one side of a network connection to another, and not the other way around. So it achieves this with a high level of assurance as well as has harmful influence on reliability and performance. In this paper, we present and analyze packet loss data collected via experiments run on a unidirectional transmitting system.

A. Hardware Design of Test Platform

The unidirectional transmission system hardware refers to rendering a unidirectional transmission security policy in one or more computing platforms using specially designed hardware. In general, this is the most secure unidirectional transmission policy enforcement method. Security is typically enforced by circuitry on the network interface cards in either the sender or receiver or both. We use optical network interface card (NIC) to build the test platform of unidirectional transmission and hardware enforced unidirectional transmission architecture is shown in Figure 1.

A hardware design can be made with three optical NICs embedded directly in the computers. The receive links (RX) of optical NIC C need to be connected to the transmit links (TX) of optical NIC B by one optical cable. This enables transfer data only occur in one direction. In both cases, optical NIC A is required simply to supply a carrier signal to optical NIC B which will not work if it does not see the appropriate carrier signal.

B. Software Design of Test Platform

It is physically impossible for data to travel in the opposite direction of the unidirectional transmission system. Protocols normally used over network connections, such as TCP/IP, that require acknowledgments to be sent back, cannot be used over a unidirectional network. To communicate over a unidirectional network, a connectionless protocol must be used. A connectionless protocol is a protocol in which there is no persistent logical connection established between the points that are communicating, and each unit of data received is treated as being independent. User Datagram Protocol (UDP) is a connectionless protocol over IP, and is well suited to implementing unidirectional communications.

We wrote two application layer programs (sender program and receiver program) to measure the loss data and analyze the correlation of the loss rate and the transmission rate, the data packet load, in unidirectional transmission system. The figure 2 and 3 show their finite-state machine (FSM) definitions. The FSM in figure 2 defines the operation of the sender, while the FSM in figure 3 defines the operation of the receiver[11].

![Figure 2. Sender program FSM](image2)

The sender side has two states. In the left state, the sender program is waiting for data to be sent over the unidirectional transmission system. The sender program first send an advertise packet to the receivers and the packet contain name and size of the file which is going to be sent to the receivers. Then, the sender program sends the packet to a fixed address over the unidirectional network and move to the right state. To pace the send data with sufficient time resolution to insure that the receiver is always able to receive data, the sender program is waiting for a fixed interval time to send the next data packet. The program uses the interval timer to schedule transmission of packets as if sender can send packets in a fixed flow rate to the fixed address. If the interval time is over, the sender program creates the data packet attaching a sequence number and a file number and sends the packet to the same address. For error detection, the sender adds checksums and sequence numbers to each packet, so the receiver can detect when a packet is the lost or corrupted and an error is signaled.

![Figure 3. Receiver program FSM](image3)

The receiver side also has two states. In the left state, the receiver program is waiting to receive a packet from the same pre-specified address. If the receiver program receives the advertise packet, it extracts the file information; then, it opens a big buffer to record packet received or lost information and moves to the right state. In the right state, the receiver program is waiting to receive any data packet. If the receiver program receives a data packet, detection of lost data can be done by...
tagging data with sequence numbers to insure detection of lost packets and data within a packet can be verified through checksum. Packet loss can be reduced by increasing the size of the kernel network buffers and adjusting the process priorities, so that the receiver is carried out with a high priority and with enough buffer space to cope with short delays.

III. EXPERIMENT DESIGN

UDP is often referred to as ‘send and pray’. The transmitting computer has no idea whether or not the destination computer successfully received its transmission. It is impossible to guarantee error free delivery of data over a unidirectional link. Even if the receiving computer is able to deduce that data is corrupt or missing, there is no way for it to inform the source. In software design of test platform, many mechanisms are used to minimize the effect of unidirectional transmission. But packet loss can occur when the receiving side buffers are overloaded in hardware, memory or CPU. So we design a series of experiment to research the correlation of the packet loss rate and the transmission rate, the data packet load.

A. Relevant Parameters Introduction

Packet loss rate refers to the proportion of lost packets to total sent packets. Packet loss rate calculation method: the lost number of packets (LossPacket) divided by the sent number of packets (SendPacket). Packet loss rate (PLR) is specifically calculated as follows:

\[ PLR = \frac{\text{LossPacket}}{\text{SendPacket}} \]  

(1)

Transmission rate refers to the size of the amount of data transmitted in per unit time of the network layer. The unit is Mbps.

Complete file rate (CFR) refers to the proportion of the number on received complete file (CompleteFile) to the total number of sent file (SendFile). Complete file rate is specifically calculated as follows:

\[ CFR = \frac{\text{CompleteFile}}{\text{SendFile}} \]

(2)

The event probability of packet loss (p) refers to the proportion of the number on packet loss event (PLN) accounted receive packet number (RPN). If several consecutive packets are lost, it denotes only one loss event. P is computed based on the following formula:

\[ P = \frac{\text{PLN}}{\text{RPN}} \]

(3)

B. Experiment about Correlation between the Packet Loss and Transmission Rate

In order to reduce the complexity of the experiment, we only take the transmission rate as variable parameters to analyze the change condition of PLR with different transmission rate, and design the following experiment. Using the unidirectional transmission system, we transmit four different size files (1.5G, 3G, 5G, 10G) at different transmission rates (200, 300, 350, 400, 480, 500, 600 by Mbps), record test data, and calculate the PLR at different transmission rate using the formula (1). Large files in real environment need to be stored on disk, so we decide that the maximum data recording speed 600Mbps of the disk regard as the maximum speed of experiment. For excluding the effect of IP packet augmentation and reassembly, we choose the 1460 bytes as the packet load. The other specific parameters are shown in Table I.

C. Experiment about Correlation between Packet Loss and Packet Load

In order to reduce the complexity of the experiment, we only take the packet load as variable parameters, to analyze the change condition of PLR with different packet load in the experiment. Using the unidirectional transmission system, we take different packet load size (512, 1024, 1331, 1460, 1500, 2K, 4K, 8K, 16K, 32K, 64K bytes), transmit four different size files (1.5G, 3G, 5G, 10G) at same transmission rates (300Mbps), and calculate the PLR using the formula (1). IP packet header only has two bytes to represent the length of the packet, which means the maximum length of the IP packet is \(2^{16} - 1 = \)
So the maximum size of the load can only be tested to 64K. In order to ensure the availability of test data, the transmission rate is set as 300Mbps. If the transmission rate is too low, it is very hard to loss packet. If the transmission rate is too high, the packet loss rate is so higher that the experiment results have a bad discrimination index. Therefore we choose intermediate value 300Mbps. The other specific parameters are shown in Table II.

D. Experiment about Packet Loss Correlation

Packet Loss in the network data transmission divided into random packet loss and congestion packet loss. Random packet loss is due to link transmission error, resulting in packet bit errors. Upper layer protocol will simply discard the packet, and the bit error rate (BER) are $1 \times 10^{-8}$ or less frequent (for fiber optic transmission system, the error rate is usually between $10^{-9}$ and $10^{-12}$). Congestion packet loss is due to network nodes too late to process the reached packet, the cache will be overloaded, and then the arrived packets will be discarded.

Random packet loss event in the unidirectional transmission is due to link or equipment error. Packet loss is independent event, so they are random distribution and have no correlation with each other. Congestion packet loss is due to network congestion. The network nodes use FIFO (First In First Out) and have the feature of “lost tail”, so that the correlation exists shortly between two drops. To study packet loss correlation in congestion packet loss, design experiment as follows. Using the unidirectional transmission system, we collect experiment data under different parameters to calculate the $p$ using the formula (2). The specific experiment parameters are shown in Table III.

### Table III. Experiment Parameters of Packet Loss Correlation

<table>
<thead>
<tr>
<th>Transmission rate</th>
<th>Load</th>
</tr>
</thead>
<tbody>
<tr>
<td>320Mbps</td>
<td>8K byte</td>
</tr>
<tr>
<td>480Mbps</td>
<td>1460 byte</td>
</tr>
<tr>
<td>560Mbps</td>
<td>1460 byte</td>
</tr>
<tr>
<td>560Mbps</td>
<td>1331 byte</td>
</tr>
</tbody>
</table>

IV. ANALYSIS AND DISCUSSION

A. Analysis about Correlation between Packet loss and Transmission Rate

Table IV contains the main data of experiment about correlation between the packet loss and transmission rate, and result of analysis and calculation based on the experiment data. The parameters in the table include the load size, the data transmission rate, data packet loss number and PLR.

In figure 4 we plot transmission rate Vs packet loss rate. When the transmission rate enhances from 0 to 300Mbps, PLR was zero and packets don’t loss. When transmission rate enhances from 300 Mbps to 350Mbps, packet loss begin and PLR maintain at $10^{-9}$. When transmission rate increase from 350 Mbps to 400Mbps, PLR increase rapidly from $10^{-9}$ to $10^{-6}$. When transmission rate increase from 400 Mbps to 600Mbps, amounts of packets are discarded and PLR increase rapidly from $10^{-6}$ to $10^{-2}$. Evidently, packet loss is varies for different transmission rate, we can see from the plot graph, when transmission rate is lower than 300Mbps, it has no packet loss. When transmission rate is higher than 300Mbps, PLR increase rapidly. So 300Mbps transmission rate provides good efficiency of unidirectional transmission while ensuring the reliability.

### Table IV. Experiment Result of Correlation between Packet Loss and Transmission Rate

<table>
<thead>
<tr>
<th>Load(byte)</th>
<th>Transmission rate</th>
<th>Packet loss number</th>
<th>PLR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1460</td>
<td>200 Mbps</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td>1460</td>
<td>300 Mbps</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td>1460</td>
<td>350 Mbps</td>
<td>7</td>
<td>$4.0 \times 10^{-9}$</td>
</tr>
<tr>
<td>1460</td>
<td>400 Mbps</td>
<td>4745</td>
<td>$3.1 \times 10^{-6}$</td>
</tr>
<tr>
<td>1460</td>
<td>480 Mbps</td>
<td>6545806</td>
<td>$4.3 \times 10^{-3}$</td>
</tr>
<tr>
<td>1460</td>
<td>600 Mbps</td>
<td>38209238</td>
<td>$2.5 \times 10^{-2}$</td>
</tr>
</tbody>
</table>

B. Analysis about Correlation between Packet Loss and Packet Load

Table V contains the main data of experiment about correlation between the packet loss and packet load, the parameters in the table includes the size of the load, the number of packet loss under each load size and PLR.

In figure 5 and figure 6 we plot packet load size Vs packet loss rate. Figure 5 is a complete Figure which load increase from 0 to 8K byte. Figure 6 is a portion of Figure 5 which load increase from 500 byte to 1500 byte. PLR maintained at $10^{-8}$ when the load size increase from 0 byte to 1460 byte and it has the minimum PLR when packet load size is 1460 byte. When the load size exceeds 1460 byte, PLR exhibited an exponential increase with respect to packet load size. Evidently, PLR
is varies for different packet load, we can see from the plot graph, when packet size is 1400 it has the minimum PLR. When packet size is 8K it has the maximum PLR. So when the packet size is 1460 bytes can improve the performance of unidirectional transmission for keeping the reliability. As packet load size 1500 is exactly the value of the IP data packet fragmentation, it is reasonable to believe that the IP packet fragment reassembly can cause packet loss rate to increase.

C. Analysis about Correlation between Complete File Rate and Packet Load

Through the statistical of receiver’s logs, we can gain the sum of the complete file with different packet load. We calculate the CFR using the formula (2). In Figure 7 we plot complete file rate due to packet load. CFR be close to 100% when the load size increases from 0 byte to 1460 byte. When the load size exceeds 1460 byte, CFR exhibited an exponential decrease with respect to packet load size. Evidently, CFR is varies for different packet load, and we can find from the plot graph that when packet size is 1460 byte it has the maximum CFR.

D. Distribution Character of Packet Loss

The experiment data is analyzed by Kolmogorov-Smirnov test (KS-test) [12, 13]. The KS-test tries to determine if two datasets differ significantly. The KS-test has the advantage of making no assumption about the distribution of data. The one-sample Kolmogorov-Smirnov test belongs to the category of nonparametric tests and we use it to decide whether a sample of experiment data comes from a population with a pacific distribution. From the output of the KS-test results about the sample variables of packet loss, we can find that the distribution of packet loss depends on the length of the packet transmitted and the packet loss obey the Poisson distribution in the different parameters when the load size increase from 512 byte to 1460 byte and the transmission rate enhances from 0 to 350Mbps. However, with the transmission rate grows, the packet loss may not be assumed to come from Poisson distribution. In Figure 8 we plot the probability of packet loss due to the number packet loss.

When the load size increase from 512 byte to 1460 byte and the transmission rate enhances from 0 to 350Mbps, packet loss obey the Poisson distribution in the different parameters. The bit errors obey the Poisson distribution in the different parameters, and the distribution depends on the length of the frames transmitted [14, 15]. Consider the transmission of n packets over a unidirectional transmitting channel. Let the random variable X equal the number of packet loss. When the probability that a packet is lost is constant and the transmissions are independent, X has a binomial distribution. Let p denote the probability that a packet is lost. Then \(E(x) = np = \lambda\) and

<table>
<thead>
<tr>
<th>Load size</th>
<th>Packet loss</th>
<th>Test number</th>
<th>PLR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000 byte</td>
<td>84</td>
<td>100</td>
<td>2.12*10^-8</td>
</tr>
<tr>
<td>1200 byte</td>
<td>39</td>
<td>100</td>
<td>1.97*10^-8</td>
</tr>
<tr>
<td>1400 byte</td>
<td>6</td>
<td>100</td>
<td>3.94*10^-9</td>
</tr>
<tr>
<td>1460 byte</td>
<td>11</td>
<td>100</td>
<td>7.78*10^-9</td>
</tr>
<tr>
<td>1550 byte</td>
<td>5189</td>
<td>100</td>
<td>3.93*10^-6</td>
</tr>
<tr>
<td>2K byte</td>
<td>8746</td>
<td>100</td>
<td>8.84*10^-6</td>
</tr>
<tr>
<td>4K byte</td>
<td>24535</td>
<td>100</td>
<td>4.97*10^-5</td>
</tr>
<tr>
<td>8K byte</td>
<td>20933</td>
<td>100</td>
<td>8.09*10^-4</td>
</tr>
</tbody>
</table>
\[ p(X = x) = \binom{n}{x} p^x (1 - p)^{n-x} \]
\[ = \binom{n}{x} \frac{\lambda^x}{n^x} (1 - \lambda/n)^{n-x} \quad (4) \]

Now, suppose that the number of packets transmitted increases and the probability of a loss decreases exactly enough that \( pn \) remains equal to a constant. That is, \( n \) increases and \( p \) decreases accordingly, such that \( E(X) = \lambda \) remains constant. Then, with some (non-trivial) work, it can be shown that
\[
\lim_{n \to \infty} p(X = x) = \frac{e^{-\lambda x} \lambda^x}{x!}, \ x = 0, 1, 2\ldots \quad (5)
\]

Also, because the number of packets transmitted tends to infinity, the number of loss can equal any non-negative integer. Therefore, the range of \( X \) is the integers from zero to infinity. The results of the Poisson distribution are remarkably close to experimental data. Our analysis results indicated that packet loss due to bit errors at the physical layer when the load size increase from 512 byte to 1460 byte and the transmission rate enhances from 0 to 350Mbps.

### E. Analysis about Packet Loss Correlation

When the load size increase from 0 byte to 1460 byte and the transmission rate enhances from 0 to 350Mbps, packet loss occur very few. The bit error rate of the unidirectional transmission system is usually between \( 10^{-9} \) and \( 10^{-12} \), so loss pattern of unidirectional transmission is random packet loss and packet loss is discrete distribution and has no mutual relationship. However, with the transmission rate grows, the PLR grows rapidly and loss pattern of unidirectional transmission is congestion packet loss.

Analysis of the nature of the packet loss indicated that packet loss is burst and amounts of packet loss episode are found. A packet loss episode begins with a lost packet if the previous packet was successfully received; a loss episode is of length \( L \), if it consists of \( L \) consecutively lost packets. Therefore, we examine the loss patterns in more details, focusing on the loss episodes. We found that consecutive packet losses represent the majority of the overall packet loss, even though lengths of loss episodes over 150 represent a high percentage of all loss episodes. The packet-loss process is modeled here by the Packet loss rate and the probability distribution of burst length, which in turn corresponds to the number of consecutive lost or received packets. A two-state Markov chain model [16, 17, 18] also known as the Gilbert model can be used as a simple model for burst packet loss. The state diagram of the model is shown in Figure 9.

State 0 represents the state of successful packet arrival, while state 1 represents the state of packet being lost. State transition probabilities are \( \lambda \) being the associated random variable with \( X = 0 \): “no packet lost”, \( X = 1 \) “a packet lost”:
\[
p_{01} = p(X = 1 | X = 0) = p \quad \text{(packet n is lost packet n - 1 is received)}
\]
\[
p_{10} = p(X = 0 | X = 1) = p \quad \text{(packet n is received packet n - 1 is lost)} \quad (6)
\]

Let \( p_{01} \) denote the probability of transition from state 0 to state 1 and \( p_{10} \) the probability of transition from state 1 to state 0, as shown in the figure 9.

In steady-state, transition and state probabilities can be expressed in matrix form:
\[
\begin{pmatrix}
1 - p_{01} & p_{01} \\
p_{10} & 1 - p_{10}
\end{pmatrix}
\begin{pmatrix}
p(X = 0) \\
p(X = 0)
\end{pmatrix}
= \begin{pmatrix}
p(X = 0) \\
p(X = 0)
\end{pmatrix} \quad (7)
\]

From equation (6) and the equation \( p(0) + p(1) = 1 \), the unconditional loss probability is:
\[
p(X = 1) = \frac{p_{01}}{p_{01} + p_{10}} \quad (8)
\]
Equation (8) refers to PLR.

The conditional loss probability (CLP), equal to the probability of having a loss, given the previous packet was lost, is:
\[
p(X = 1 | X = 1) = 1 - p_{01} \quad (9)
\]

When \( p_{10} \) equals \( 1 - p_{01} \) this model reduces to the Bernouilli model. Burst packet loss can be modeled by choosing appropriate values for \( p_{01} \) and \( p_{10} \).

The random variable \( Y \) is related to the probability distribution of the lengths of loss episodes in burst packet loss. The probability of having a loss episode with length \( k \) (\( k \) consecutively lost packets) given that we begin with the loss state \( X = 1 \) is:
\[ p(Y = k) = p(x = 1 | x = 1)^{k-1} p(x = 0 | x = 1) \]  \hspace{1cm} (10) \\

Hence, the lengths of loss episodes given by the Gilbert model are geometrically distributed. The average packet loss rate is given by \( p_{in} / (p_{in} + p_{out}) \). The probability \( p_{in} \) is related to the burstiness of the packet loss, with the probability of getting a burst of length \( k \), equal to \( p_k = (1 - p_{in})^{k-1} \cdot p_{in} \). Then, \( E(Y) \) is related to the average loss length of a packet loss episode.

\[
E(Y) = \sum_{k=0}^{\infty} kp_k = \sum_{k=0}^{\infty} k(1 - p_{in})^{k-1} \cdot p_{in} \\
= \sum_{k=0}^{\infty} k(1 - p_{in}) \cdot p_{in}^{k-1} = (1 - p_{in}) \sum_{k=1}^{\infty} kp_{in}^{k-1} \\
= (1 - p_{in}) \frac{d}{dp_{in}} \sum_{k=0}^{\infty} p_{in}^k = (1 - p_{in}) \frac{d}{dp_{in}} \left( \sum_{k=0}^{\infty} p_{in}^k - 1 \right) \\
= (1 - p_{in}) \frac{d}{dp_{in}} \left( \frac{1 - p_{in}}{1 - p_{in}} - 1 \right) = (1 - p_{in}) \frac{d}{dp_{in}} \frac{1 - p_{in}}{1 - p_{in}} \\
= (1 - p_{in}) \frac{1}{1 - p_{in}} = \frac{1}{1 - p_{in}} = \frac{1}{1 - p_{in}} \\
\]

The Gilbert model memorizes only one past event. The probability that the next event will be either a successfully received or a lost packet depends only on the previous state. The model can be implemented using a random number generator and a state machine to generate a sequence of packets with loss. The values for transition probabilities \( p_{01} \) and \( p_{10} \) in the Gilbert model are based on a packet trace containing the information about the lost and successfully received packets:

\[ P_{10} = p(X = 1 | X = 0) = \sum_{k=1}^{\infty} \frac{O_k}{a} \]  \hspace{1cm} (11) \\

\[ 1 - P_{10} = p(X = 1 | X = 1) = \frac{\sum_{k=1}^{\infty} (k - 1) \cdot O_k}{d - 1} \]  \hspace{1cm} (12) \\

Where \( O_k \) is the number of loss episodes of length \( k \), \( a \) is the total number of packets (successfully received and lost), and \( \sum_{i=1}^{\infty} (k - 1) \cdot O_k \) is the total number of lost packets.

Results obtained from our experiment data under different test environments are shown in Table VI. For instance, we send a file over the unidirectional network, the packet load size is 8K bytes and the length of the file is 1522280KB. So, the sender program must send 190285 (1522280/8) packets. The sum of packet loss is 138 in the process of transmission. The probability \( p \) is computed as:

\[ P = \frac{138}{190285} = 7.257 \times 10^{-4} \]

From equation (10) and equation (11) we can calculate the probability of having a loss episode. The simulation results for the Gilbert model is given in Table VII. Given values of conditional loss probability, and packet loss rate, the probability \( p \) is computed as:

\[ P_1 = \frac{138}{190285} = 7.257 \times 10^{-4} \]

<table>
<thead>
<tr>
<th>Test Environment</th>
<th>Test result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load size 8K</td>
<td>PLR=8.09*10^4</td>
</tr>
<tr>
<td>Transmission rate 320Mbps</td>
<td>CLP=0.1</td>
</tr>
<tr>
<td>p=7.31*10^4</td>
<td></td>
</tr>
<tr>
<td>Load size 1500</td>
<td>PLR=4.30*10^4</td>
</tr>
<tr>
<td>Transmission rate 480Mbps</td>
<td>CLP=0.2</td>
</tr>
<tr>
<td>p=3.41*10^4</td>
<td></td>
</tr>
<tr>
<td>Load size 1500</td>
<td>PLR=2.51*10^4</td>
</tr>
<tr>
<td>Transmission rate 560Mbps</td>
<td>CLP=0.3</td>
</tr>
<tr>
<td>p=5.11*10^4</td>
<td></td>
</tr>
<tr>
<td>Load size 1500</td>
<td>PLR=1.97*10^4</td>
</tr>
<tr>
<td>Transmission rate 560Mbps</td>
<td>CLP=0.9</td>
</tr>
<tr>
<td>p=2.01*10^4</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Simulation parameter</th>
<th>Simulation results</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLR=8.09*10^4</td>
<td>CLP=0.1</td>
</tr>
<tr>
<td>P=7.281*10^4</td>
<td></td>
</tr>
<tr>
<td>PLR=4.30*10^4</td>
<td>CLP=0.2</td>
</tr>
<tr>
<td>P=3.440*10^4</td>
<td></td>
</tr>
<tr>
<td>PLR=2.51*10^4</td>
<td>CLP=0.3</td>
</tr>
<tr>
<td>P=5.149*10^4</td>
<td></td>
</tr>
<tr>
<td>PLR=1.97*10^4</td>
<td>CLP=0.9</td>
</tr>
<tr>
<td>P=2.01*10^4</td>
<td></td>
</tr>
</tbody>
</table>

The Simulation results of loss-episode lengths derived from the Gilbert model and the test result obtained from our experiment show a good consistency. Therefore, we can use the run length distribution for a simple computation of the parameters of the Gilbert model to characterize the loss process of unidirectional transmission.

V. CONCLUSIONS

After analyzing all the experimental data from unidirectional transmission, we conclude our findings in the below. (1)There is an obvious correlation between the packet loss rate and packet transmission rate and when
transmission rate is higher than the threshold value, PLR increase rapidly. This threshold value can vary depending on the hardware of test platform. (2) The packet size effect on the packet loss, and packet loss rate. The experiment results elicited that the best packet size is 1460 bytes. (3) Packet loss in the unidirectional transmission divided into random packet loss and congestion packet loss. Random packet loss is due to link transmission error, resulting in packet bit errors. When the load size increase from 512 byte to 1460 byte and the transmission rate enhances from 0 to 350Mbps, packet loss obey the Poisson distribution in the different parameters. When loss pattern of unidirectional transmission is random packet loss packet loss is discrete distribution and has no mutual relationship. (4) With the transmission rate grows, the PLR grows rapidly and loss pattern of unidirectional transmission become congestion packet loss. Analysis of the nature of the packet loss indicated that packet loss is burst and that consecutive packet losses significantly contribute to the overall packet loss. We can use the Gilbert model to characterize the congestion loss process of unidirectional transmission. The analysis result of the experiments can reduce the packet loss rate dramatically and improve the performance of unidirectional transmission. The design scheme of protocol or FEC for unidirectional transmission should also benefit from the results discussed in this paper.

ACKNOWLEDGMENT

This work was supported in part by the Key Science and Technology Program of Sichuan Province, China; under Grant No. 2012FZ0016.

REFERENCES


Lin Honggang received the BS degree in computer science from Sichuan University, China, in 2003 and the PhD degree in applied mathematics from the Sichuan University of China in 2006. He is an associate professor at Chengdu University of Information Technology, China. His research is focused towards network security and security of cloud computing. Other areas of interest include fault-tolerant computing, distributed computing, and hardware/software code sign.