An Efficient Prelude to Measure Packet Loss and Delay Estimate with Elevated Security Feature

Surya.S.Raju
M.Tech
Dept. of CSE, DSCE
Bangalore, India

Manjunath.S.S
Assistant Professor
Dept. of CSE, DSCE
Bangalore, India

ABSTRACT
Packet Loss ratio is among the most important metrics for identifying poor network conditions, since it affects data throughput performance and the overall end-to-end data transfer quality. An application for enhancing the security of packets in transit has been proposed. The end to end packet loss and delay is estimated in addition to providing the security to the packets. The objective of our simulation studies done in Java language is to estimate the amount of data that has been lost and the delay incurred. Encryption and decryption has been provided too. The existing methods indicate certain disadvantages in Poisson based tools. Simulation results demonstrate the effectiveness of the proposed method in terms of packet loss, delay, and encryption.

General Terms
TCP, UDP, Cryptography.

Keywords
Packet Loss, Delay, Encryption.

1. INTRODUCTION
Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss can be caused by a number of factors including signal degradation over the network medium due to multi-path fading, packet drop because of channel congestion. The fraction of lost packets increases as the traffic intensity increases. Therefore, performance at a node is often measured not only in terms of delay, but also in terms of the probability of packet loss. There are two major causes of packet loss in IP networks. One is congestion, where the network routers/switches are temporarily sent more packets than their buffers can accommodate. The other is due to link failure, when all the bits currently in transit on that link will be lost. While a packet that has been modified in transit represents clear evidence of tampering, a missing packet is inherently ambiguous: it may have been explicitly blocked by a compromised router or it may have been dropped benignly due to network congestion. Once the ambiguity from congestion is removed, subsequent packet losses can be attributed to malicious actions.

Sommers, Paul Barford, Nick Duffield, Amos Ron [1] have proposed a method to understand how to measure packet loss episodes accurately with end-to-end probes. Specifically, their method creates a probe process that (1) enables an explicit trade-off between accuracy and impact on the network, and (2) enables more accurate measurements than standard Poisson probing at the same rate. They evaluate the capabilities of their methodology experimentally by developing and implementing a prototype tool, called BADABING. The experiments demonstrate the trade-offs between impact on the network and measurement accuracy. They show that BADABING reports loss characteristics far more accurately than traditional loss measurement tools. The experimental results led to development of a probe process that provides more accurate estimation of loss characteristics than simple Poisson probing.

Yasuhiro Yamasaki, Hideyuki Shimonishi, and Tutomu Murase [2] have proposed a method to estimate the TCP packet loss rate from sampled packets. The proposed method detects packet loss events by monitoring duplicate ACK events induced by a TCP receiver indicating the loss events. Since only a portion of packet loss events can be detected from the sampled packets, the correct packet loss rate is estimated by means of statistical approximation. Conventional methods, however, cannot extend to the measurement of packet loss rate. This paper proposes a statistical method for estimation of the TCP packet loss rate from a small number of sampled packets.

Detecting malicious packet dropping is important in ad hoc networks to combat a variety of security attacks such as black hole, greyhole, and wormhole attacks. Thaier Hayajneh, Prashant Krishnamurthy, David Tipper, Taehoon Kim[3] consider the detection of malicious packet drops in the presence of collisions and channel errors and describe a method to distinguish between these types. We present a simple analytical model for packet loss that helps a monitoring node to detect malicious packet dropping attacks. The model is analyzed and evaluated using simulations. The results show that it is possible to detect malicious packet drops in the presence of collisions and channel errors.

Network traffic measurement is an effective tool for monitoring, performance evaluation, network troubleshooting and control. In this paper Imadud Din and Nazar Abbas Saqib [4] analyze the effect of packet loss on web traffic characteristics by taking passive measurements on an operational network. They show how packet loss effect duration, size, and throughput of TCP connections. In addition they also show the effect of packet loss on throughput of TCP connections and explain when this parameter can play a more effective role.

Available bandwidth is a very important characteristic of a link across a wide area network. In this paper, Hemanta Kumar Kalita, Manoj K. Nambiar, Debadatta Mishra [5] discuss a new method to measure available bandwidth of a link across a wide area network. This method does not introduce large traffic into the network during measurement. Also, it does not require both ends

of a link to run the algorithm. Theirs is a simple to use algorithm which runs at one end of the link and needs only the IP address of the other end.

A. Rajaram, Dr.S.Palaniswami [6] develop a trust based security protocol based on a cross-layer approach which attains confidentiality and authentication of packets in both routing and link layers of MANETs. In the first phase of the protocol, they design a trust based packet forwarding scheme for detecting and isolating the malicious nodes using the routing layer information. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious. In the next phase of the protocol, they provide link-layer security using the CBC-X mode of authentication and encryption.

Chinawat Wongvivitkul, Sudsanguan Ngamsuriyaroj [7] proposes a model to measure the effectiveness of filtering malicious traffic while actual attacks aim at a target server. The model performs a simple anomaly detection using the rates of input traffic which is classified into normal, suspicious and malicious traffic based on the pre-defined threshold values. If the input traffic is regarded as suspicious or malicious, the model will substantially drop part of the input traffic to an acceptable level so that only the small amount of traffic is allowed to pass and reach the target server. As a result, the server survives the attacks.

Of particular importance is the understanding of the dynamics of packet loss behavior since it can have significant impact on TCP and UDP applications. Packet Loss can have a significant impact on the performance of both TCP and UDP based applications. Email for example, may involve text and still images and the performance degradation caused by losses can be corrected by retransmitting the packets with the help of TCP. But retransmissions gradually increases the load, so increasing the loss and hence the number of retransmissions. However, for UDP based applications, like VoIP, timely packet delivery and packet ordering is important [8].

In our method, packet loss model is created and security is provided to the packets in transit. This security implies providing encryption and decryption. The rest of the paper is organized as follows: Section 2 introduces proposed method. Section 3 gives introduction to cryptography. Section 4 gives Simulation results and this paper is finalized in Section 5. This is followed by Acknowledgement and References.

2. PROPOSED METHOD

The block diagram of the work undertaken is shown in Fig.1

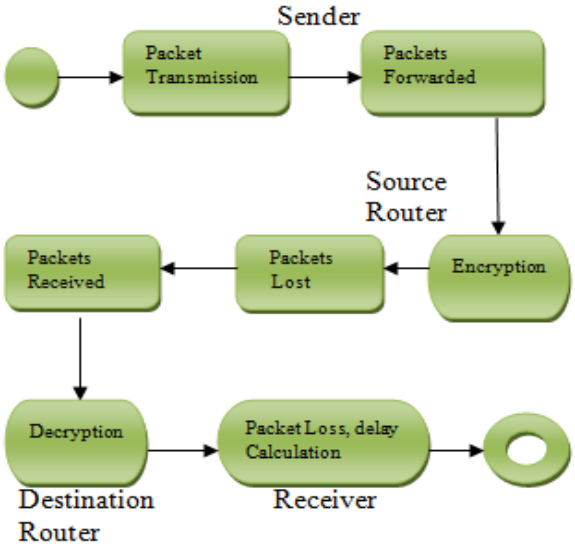

Fig 1: Block Diagram of the work undertaken

The purpose of our study was to calculate end-to-end packet loss and delay estimate with enhanced security features. There are four modules in the overall work:

- Sender
- Source Router
- Destination Router
- Receiver

The module descriptions are as follows:

Sender

The input data is split into packets. These packets are then transmitted to the Source Router Module.

Source Router

A packet loss model is created here which loses packets in random. These packets are then encrypted using any one of the cryptographic algorithms available. A modification to the existing RSA algorithm has been presented. The encrypted text so got by applying RSA algorithm is left shifted to 'n' levels in order to get a new encrypted text. This is then transmitted to the Destination Router.

Data → RSA→ encrypted text→ << 'n' levels→ new encrypted text

Destination Router

The remaining packets after packet loss arrive at the Destination Router. These packets are then decrypted by right shifting them to 'n' levels and then applying the RSA algorithm. These are then transmitted to the Receiver.

new encrypted text→ >>'n' levels→ encrypted text→ RSA algorithm→ original data

RECEIVER

The packets after decryption arrive at the Receiver. Packet loss and the delay incurred are calculated. Hence a more accurate approach has been presented.

3. CRYPTOGRAPHY

Cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process. It is a science of protecting information by encoding it into an unreadable format. Cryptography is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths. Although the ultimate goal of cryptography, and the mechanisms that make it up, is to hide information from unauthorized individuals, most algorithms can be broken and the information can be revealed if the attacker has enough time, desire, and resources. So a more realistic goal of cryptography is to make obtaining the information too work-intensive to be worth it to the attacker. A system that provides encryption and decryption is referred to as a cryptosystem and can be created through hardware components or program code in an application. The cryptosystem uses an encryption algorithm, which determines how simple or complex the process will be. Most algorithms are complex mathematical formulas that are applied in a specific sequence to the plaintext.

3.1 Symmetric Cryptography

In a cryptosystem that uses symmetric cryptography, both parties will be using the same key for encryption and decryption. This provides dual functionality. Symmetric keys are also called secret keys because this type of encryption relies on each user to keep the key a secret and properly protected. If this key got into an intruder's hand, that intruder would have the ability to decrypt any intercepted message encrypted with this key. The following are examples of symmetric key cryptography algorithms:

- RC4, RC5, and RC6
- Data Encryption Standard (DES)
- Triple DES (3DES)

3.2 Asymmetric Cryptography

In public key systems, each entity has different keys, or asymmetric keys. The two different asymmetric keys are mathematically related. If a message is encrypted by one key, the other key is required to decrypt the message. In a public key system, the pair of keys is made up of one public key and one private key. The public key can be known to everyone, and the private key must only be known to the owner. Many times, public keys are listed in directories and databases of e-mail addresses so they are available to anyone who wants to use these keys to encrypt or decrypt data when communicating with a particular person. The following are examples of asymmetric key algorithms:

- RSA
- Diffie-Hellman
- Digital Signature Standard (DSS)

4. SIMULATION RESULTS

Simulation has been done in Java language. The graphical user interfaces developed have been presented in the Figs. 2-10. It indicates browsing for a file, breaking the file into packets, sending the packets to the sender module, creation of packet loss, encryption, decryption, packet loss and delay statistics.

Fig 2: Browse for a file

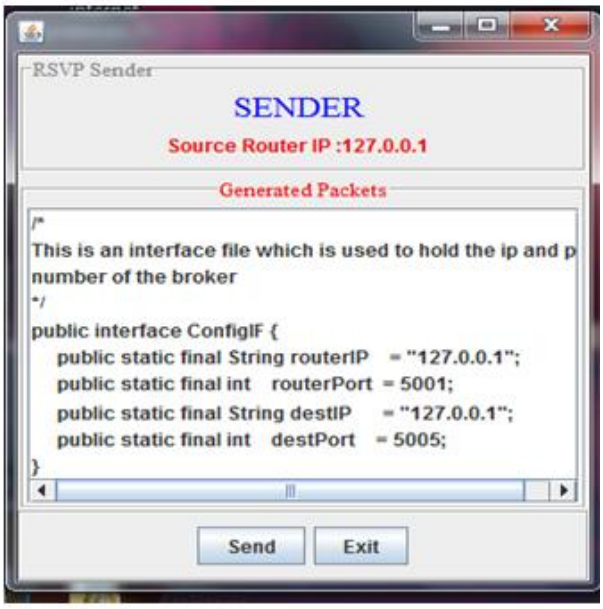

Fig 3: Source Router

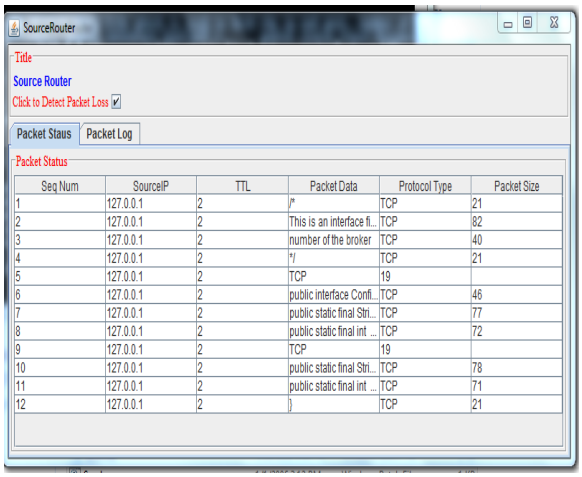

Fig 4: Source Router

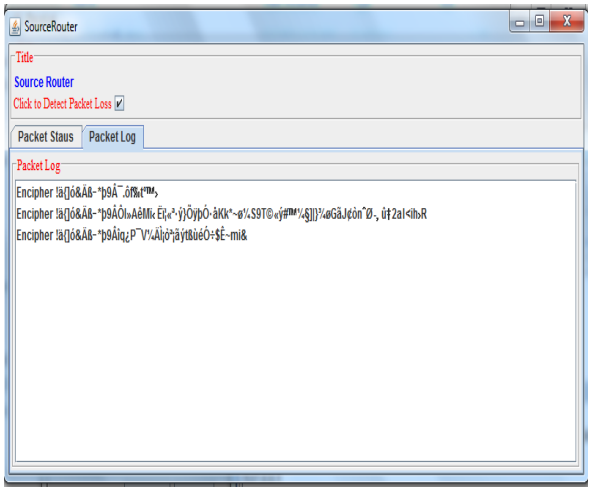

Fig 5: Encryption

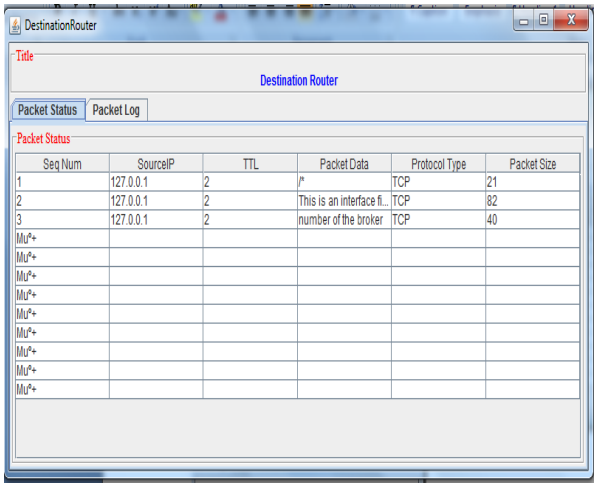

Fig 6: Destination Router

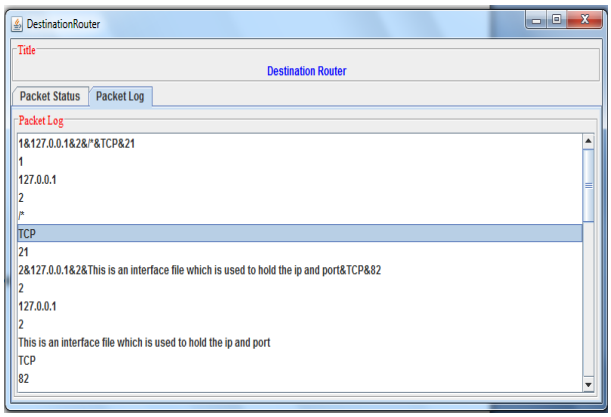

Fig 7: Decryption

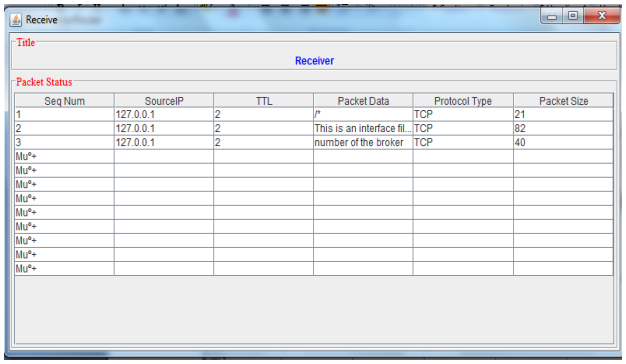

Fig 8: Receiver

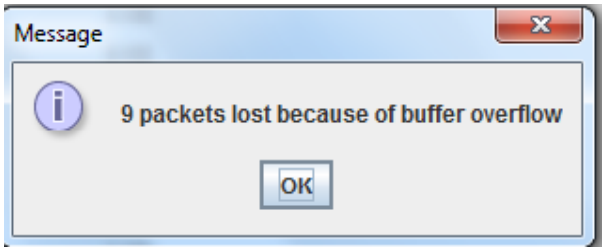

Fig 9: Packet Loss Measurement

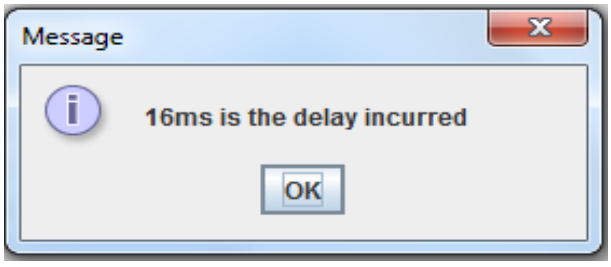

Fig 10: Delay Measurement

5. CONCLUSION

The work presented in this paper is oriented towards finding the accurate packet loss estimate and delay incurred in addition to providing security to the packets in transit. A modified version of the RSA algorithm has been used. Simulation results indicate the effectiveness of the method that has been used. This work was taken up not only to overcome the deficiencies of the traditional measurement tools but also provide the packets with more secure cryptographic algorithm.

6. ACKNOWLEDGEMENT

This paper would not have existed without my guide Assistant Professor Manjunath.S.S. I also would like to thank our head of the department Dr. Ramesh Babu D.R., Professor Bhaskar Rao and my colleague Shivamalini.L.

7. REFERENCES

[1] Joel Sommers, Paul Barford, Nick Duffield, Amos Ron, Volume 20, No.2, February 2009 Improving Accuracy in End-to end Packet Loss Measurement. In IEEE Transactions on Parallel and Distributed Systems.

[2] Yasuhiro Yamasaki, Hideyuki Shimonishi, Tutomu Murase, 2005. Statistical Estimation of TCP Packet Loss Rate from Sampled ACK Packets. Global Telecommunications Conference IEEE.

[3] Thaier Hayajneh, Prashant Krishnamurthy, David Tipper, Taehoon Kim, 2009. Detecting Malicious Packet Dropping in the Presence of Collisions and Channel Errors in Wireless Ad hoc Networks. In IEEE International Conference on Communications.

[4] Imadud Din, Nazar Abbas Saqib, 2008.Passive Packet Loss Detection and its Effect on Web Traffic Characteristics. International Conference on Computer and Electrical Engineering.

[5] Hemanta Kumar Kalita, Manoj K. Nambiar, Debadatta Mishra, 2007. A New Algorithm for Measuring Available Bandwidth in a Wide Area Network. In 15th International Conference on Advanced Computing and Communications.

[6] Rajaram, A., Dr. Palaniswami S., Detecting Malicious Node in MANET Using Trust Based Cross-Layer Security Protocol, 2010. In International Journal of Computer Science and Information Technologies, Volume 1 (2).

[7] Chinawat Wongvivitkul, Sudsanguan Ngamsuriyaroj, 2007. The Effects of Filtering Malicious Traffic under DoS Attacks. In Asia Pacific Advanced Network 2007, 27-31 August 2007, Xian, China, Network Research Workshop 2007, 27 August 2007, Xian, China.

[8] Padmalatha, R. and Sreedhar, G. 2010. A Novel Algorithm for Improving the End-to-End Active Packet Loss Measurements in Computer Networks. In International Journal of Computer Applications (0975-8887), Volume 6 No.1.