ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Expedient Activity in ARQ Model Packet Repudiate In Content Delivery Networks

Velidi Saibaba
M.Tech Student
Sri Vatsavai Krishnam Raju College of Engineering and Technology,
Bhimavaram, AP.

Dr.Penmetsa Vamsi Krishna Raja, M.Tech
Principal
Sri Vatsavai Krishnam Raju College of Engineering and Technology,
Bhimavaram, AP.

Abstract:

Recently increasing use of multimedia model applications and services applications is trusted video sources to dentations undesirable data loss is critical problem The model is used to generate a minimum number of test packets to exercise every link in the network exercise every rule in the network Test packets is sent periodically and detected failures trigger a separate model to localize the fault Packets through a mechanism called ARQ If several clients are connected to the same AP currently the only way to achieve reliable communication for all clients is by applying this model different for each client using multiple uncast flows instead exploiting the nature of the physical model in present the proposes a more packets efficient reliability method using network coding The results in network coding is to improvements in a single client model with multiple clients is a proposed reliability method using network coding take 25% reduction of redundant packets transmitted This gives significant improvement in the throughput as compared to ARQ the results is based on different experiments and theory the model is commercial use is discussed and followed up by giving suggestions for future work

Index Terms: ***Streaming content, leakage detection, traffic pattern, degree of similarity Fault detection;,PCA, boilers, loss data ,XSS.***

1. INTRODUCTION

They serve number of population users from the world with systems contents ranging from daily news feeds to entertainment feeds including example data music[1][7], videos, sports, and so forth, by using scams transmission models In addition real-time data streaming connected such as websites in intra company networks in online with XSS model differently deployed in a large number of corporations as a powerful means of efficiently thinks business applications without different costs A crucial concern data model services is the protection of the bit stream[4][8] from different peoples use duplication and sharing One of the most popular approaches to prevent undesirable contents sharing to insipiently users to protect authors' copyrights is the digital rights management (DRM)models. Most DRM techniques employ cryptographic or digital watermark model we mainly on the illegal redistribution of streaming content by an authorized user to external network[14][18]s The existing proposals and monitor information obtained at different nodes in the middle of the streaming locations The retrieved data are used to generate traffic patterns which appear as single content just like signatures The generation of traffic pattern no require any information on the packet header and therefore preserves the user's privacy loss data detection is then performed by comparing the generated traffic patterns the existence of data of different length in the network locations causes a considerable degradation in the leakage detection results then developing an different loss data detection model robust to the variation data lengths indeed required by balancing different length data[16][19] we determine a relationship among the length of data to be compared and their behaviorist. Based on this relationship we determine decision threshold different accurate loss detection even in an environment with different length data Initially the inputs from the user will be take and stored in the database for the standard for steam the data from the source to the destination The sender sending the packets of data of information. Every data from the source is sent via packets to reach the destination of the receiver The loss of packets will be checked and evaluated based on the sent data's of packets[10][7] translations then the data is lost during packet transfer then user there will be an intruder changing the content in the data packets Information has been loss and changed by the intruder or because of any different reasons will be checked in the information leakage check module In information loss check module packets will be checked on the traversal of source to destination of the indent users accordingly The packet Monitoring will be emphasized with the checking up of the data loss during the packet transfer from the sender side to the destinations side data exchange Real time example of our project is “data streaming of Data The overall performance of our system will be checked and evaluated in the results evaluation module based on the original packet data transfer from the user to the receiver of the traffic network model

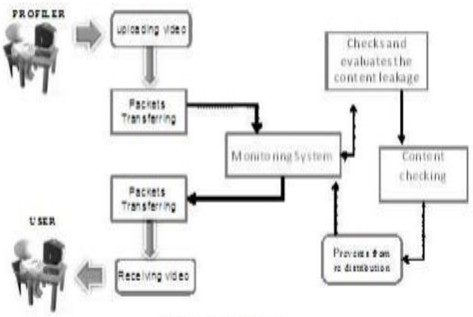


Figure 1.1 Web Monitor

2. EXISTING SYSTEM

We first take any typical data loss scenario and we present over all existing traffic pattern-based loss detection models these popularity of streaming delivery of movies development of P-to-P streaming[7] software has attracted some models These technologies change the distribution of any type of information in online[3][7] A typical content-leakage scenario can be described by the following steps as depicted a regular user in a secure network receives streaming content from a content server these with the use of a P-to-P streaming software the regular yet small user different distributes the streaming content to a non regular user outside its network[2]. Such content-loss is hardly detected or blocked by watermarking methods and DRM models An overview of the network models of the proposed leakage detection system This model consists of two main components namely the traffic pattern generation engine embedded in each router and the traffic pattern matching engine implemented in the management server then each router can observe its traffic volume and generate traffic pattern Meanwhile the traffic patter matching engine computes the similarity between traffic patterns through a matching model[9] and based on specific criterion detects contents loss The result is then notified to the target edge router to block leaked traffic[11]

A. Pattern Generation Algorithm

We describe the traffic pattern generation[8][5] model performed in observable methods Traffic pattern generation model is depended time slot-based algorithm a packet size-based algorithm The traffic pattern generated is expressed Time slot-based algorithm is a straight forward solution to generate traffic patterns by summing the amount of traffic arrival during a certain period of time In case some packets are delayed they may be stored over the delay and jitter of packets distorts the traffic pattern, and as a consequence, decreases the accuracy in pattern matching time slot-based algorithm is affected by packet loss Packet size-based algorithm defines[9] a slot as the results of amount of arrival traffic until the observation of a certain packet size This algorithm only make use of the packet arrival order and packet size therefore is robust to change in environment such as delay and jitter packet size-based algorithm shows no robustness to packet loss.

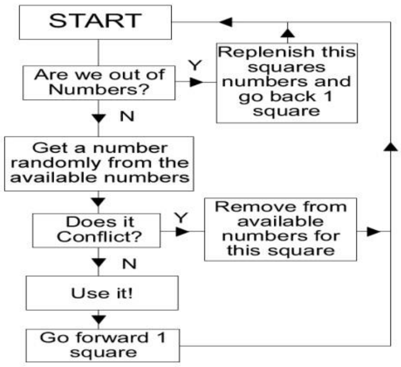

START
Are we out of Numbers?
Y
Replenish this squares numbers and go back 1 square
N
Get a number randomly from the available numbers
Does it Conflict?
Y
Remove from available numbers for this square
N
Use it!
Go forward 1 square

Fig no 2 pattern algorithm

B. Pattern Matching Algorithm

In model identify the degree of similarity is defined to be the similarity measure between patterns The server-side traffic patterns represents the original traffic model and is expressed The user-side traffic model is expressed as On the other hand the DP matching algorithm is performed on traffic model generated through packet size-based algorithm a fixed predefined value is used as the decision threshold different patterns are similar is decided by comparing the distance computed through DP matching with the decision threshold the distance less than the threshold indicates that the compared traffic patterns are similar[8][3]

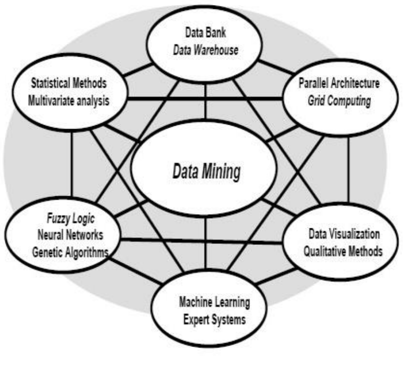


Fig. 2. Data mining process.

Fig no 3 Pattern Matching Algorithm

3. PROPOSED SYSTEM:

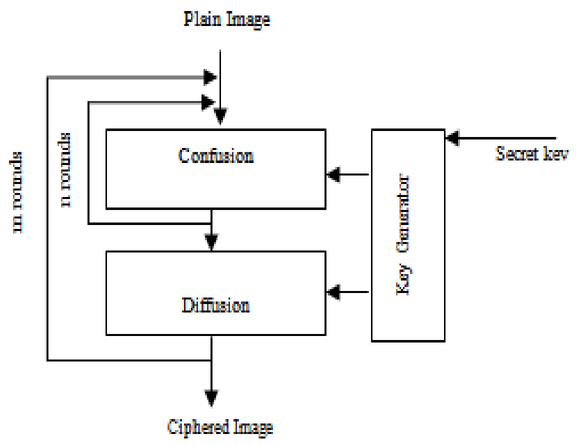
1. Automatic Repeat Re Quest (ARQ)

The way 802.11n ensure reliable communication in the presence of packet loss is by using a mechanism called ARQ. This mechanism is designed for only a single sender and receiver, so it is only used in uncast streams in WiFi, and not in broadcast streams. The mechanism works by getting feedback through acknowledgements from the receiver regarding packets that were correctly received and which were not correctly received. The receiver can verify whether a packet is received successfully by using the Cyclic Redundancy Check (CRC) code provided in the packet. By using the concept of acknowledging packets, there have emerged a few commonly known versions of ARQ. The most common are called Stop-and-wait, Go-back-N and Selective Repeat. WiFi uses the simplest version of ARQ called Stop-and-wait, which is explained in detail in the following section.

Stop-and-wait ARQ: This version of ARQ ensures both recoveries of lost packets as well as in-order reception of packets. The Stop-and-wait ARQ mechanism ensures in-order delivery by forcing each packet in turn to be received at the receiver, and it provides this reliable communication as follows:

1. Send current packet and start the local timer.

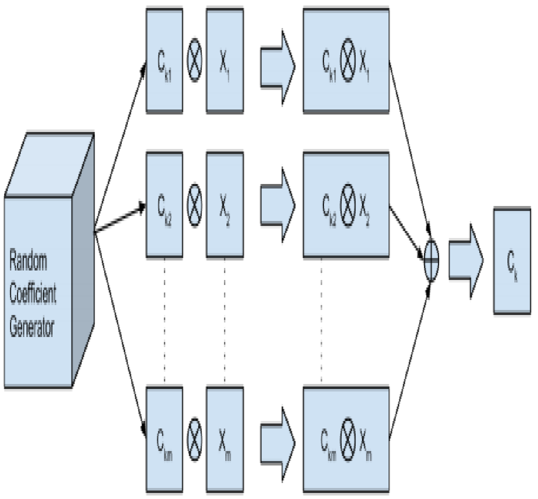
2. Wait until you either receive an Acknowledgement (ACK), NACK or the local timer expires If ACK received; continue with the next packet, knowing that the packet is received successfully. If NACK is received



2. Random Linear Network Coding (RLNC)

RLNC is a type of linear network coding where the coefficients for encoding the coded packets are chosen at random from a Galois field. This has been shown to allow close to optimal throughput [HKM+], yet with less complexity at the sender. Field theory is not covered in detail in this thesis, but is explained in great detail in a book called Finite Fields for Computer Scientists and Engineers [McE87].

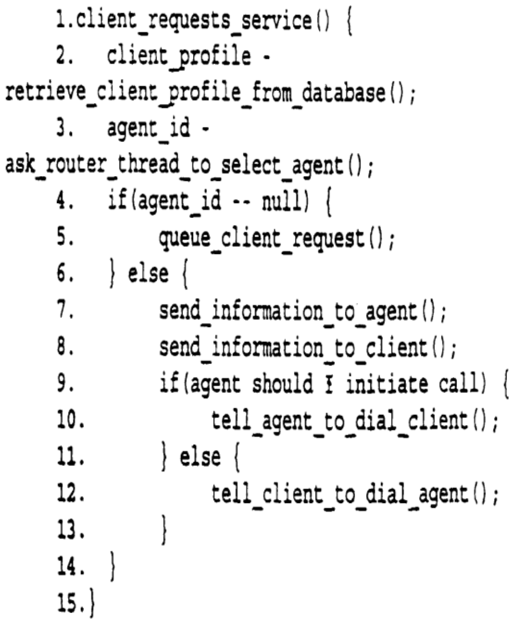
By choosing the coefficients randomly also allows the sender and receiver to generate coded packets with little overhead. Since both encoder and decoder must use the same coefficients, it is sufficient for the encoder to transmit only a seed together with the coded packet, and both encoder and decoder can use the seed to generate the same psudo-random coefficients



3. Custom Rate Adaption Algorithm

The author developed a custom rate adaption algorithm for both drivers. This rate adaption algorithm ensures a fixed modulation and coding scheme regardless of loss patterns.

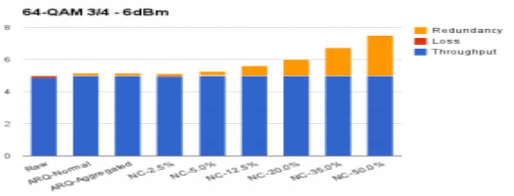
The modulation and coding scheme can be manually changed, but it will remain the same until it is manually changed again. In the rest of this thesis, it is referred to as the fixed rate adaption algorithm

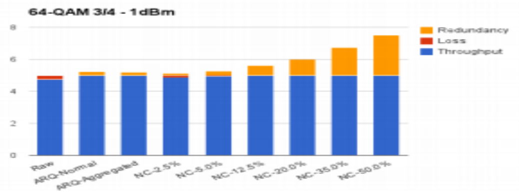


```
client_requests_service() {
    client_profile -
retrieve_client_profile_from_database();
    agent_id -
ask_router_thread_to_select_agent();
    if(agent_id -- null) {
        queue_client_request();
    } else {
        send_information_to agent();
        send_information_to_client();
        if(agent should I initiate call) {
            tell_agent_to_dial_client();
        } else {
            tell_client_to_dial_agent();
        }
    }
}
```

4. Results

Results Network engineers hunt down bugs using the most rudimentary tools and track down root causes using a combination of accrued wisdom and intuition Debugging networks is only becoming harder as networks are getting bigger and e faults into two categories action faults and match faults An action fault occurs when every packet matching the rule is processed incorrectly. Examples of action faults include unexpected packet loss a missing rule congestion, and miswriting On the other hand, match faults are harder to detect because they only affect some packets matching the rules.





5. CONCLUSION

The proposed reliability model using network coding is taking 25% reduction of redundant packets transmitted This gives significant improvement to compared to ARQ. the results is based on the experiments and The content leakage finding model based on the real fact that every streaming content has single traffic pattern is different solution to prevent The proposed model take flexible and accurate streaming content leakage detection independent of the length of the streaming content which changed secured and trusted content delivery rate Artificial Intelligence (AI) is one of the connections oriented research areas which can be utilized to find new ways for pattern generation Many technologies such as Machine Learning and Neural Networks could be applied to finding faults new types of web attacks We could employ these methods to develop more efficiently detection applications based on frame logs with long time taken the results.

6. FUTURE WORK

In addition to the web optimizations for leakage detection and analysis of the data model different ways the register users to redistribute the data in order to trusted networks the watermarking models and the video is embed the security of the sender the secret information to the register users of the trusted network In addition The number of applications in research further to finding necessary on how to detect new insufficient users of web applications more effectively Artificial Intelligence (AI) is one of the connections research areas which can be used to find new models for pattern cassations models such as Machine Learning and Neural Networks to be applied to detect new types of web attacks.

7. RFERENCES

[1] Y. Chu, S.G. Rao, S. Seshan, and H. Zhang, “Enabling Conferencing Applications on the Internet Using an Overlay Multicast Architecture,” Proc. ACM SIGCOMM, pp. 55-67, Aug. 2001.

[2] Z. Yang, H. Ma, and J. Zhang, “A Dynamic Scalable Service Model for SIP-Based Video Conference,” Proc. Ninth Int’l Conf. Computer Supported Cooperative Work in DE, pp. 594-599, May 2005

[3] Y. Chu, S. G. Rao, S. Seshan and H. Zhang, “Enabling conferencing applications on the Internet using an overlay multicast architecture,” in Proc. ACM SIGCOM, pp.55-67, California, USA, Aug. 2001.

[4] K. Su, D. Kundur, and D. Hatzinakos, “Statistical invisibility for collusion-resistant digital video watermarking,” IEEE Trans. Multimedia, vol.7, no.1, pp.43-51, Feb. 2005.

[5] Y Liu, Y. Guo, and C. Liang, “A survey on peer-to-peer video streaming systems,” Peer-to-Peer Networking and Applications, Vol.1, No.1, pp.18- 28, Mar. 2008.

[6] K. Matsuda, H. Nakayama, and N. Kato, “A Study on Streaming Video Detection using Dynamic Traffic Pattern,” IEICE Transactions on Communications (Japanese Edition), vol.J19-B, no.02, 2010.

[7]. A. Barron, "Universal approximation bounds for superpositions of a sigmoidal function", IEEE Trans. Inform. Theory, vol. 39, pp.930 -945 1993

[8]. M. Basseville and I. V. Nikiforov, Detection of Abrupt Changes: Theory and Applications, 1993 :Prentice-Hall

[9]. J. Chen and R. J. Patton, Robust Model-Based Fault Diagnosis for Dynamic Systems, 1999 :Kluwer

[10]. R. N. Clark, "Instrument fault detection", IEEE Trans. Aero. Eletron. Syst., vol. AES-14, pp.456 -465 1978

[11]. Chan-il woo1 and seung-dae lee2 (2013) international journal of smart home vol.7, no.5, pp.115-124,http://dx.doi.org/10.14257/ijsh.2013.7.5.12

issn: 1975-4094 ijsh “Digital Watermarking For Image Tamper Detection Using Block-Wise Technique”

[12]. David X. Wei Cheng Jin Steven H. Low Sanjay Hegde in(Dec 2006).in IEEE/ACM Transactions on Networking, Volume. 14, Issue no. 6, pp no.59,“FAST TCP: Motivation, Architecture, Algorithms, Performance.”

[13]. M. Almgren, H. Debar, and M. Dacier. A lightweight tool for detecting web server attacks. In ISOC Symposium on Network and Distributed Systems Security (NDSS), 2000.

[14].HTMLParser. http://htmlparser.sourceforge. net/, 2006.

[15]. Y.-W. Huang, S.-K. Huang, and T.-P. Lin. Web Application Security Assessment by Fault Injection and Behavior Monitoring. In 12th International World Wide Web Conference (WWW), 2003.

[16]. Y.-W. Huang, F. Yu, C. Hang, C.-H. Tsai, D.-T. Lee, and S.-Y. Kuo. Securing Web Application Code by Static Analysis and Runtime Protection. In 13th International World Wide Web Conference, 2004.

[17]. Java Q & A - Session State in the Client Tier. http://Java.sun.com/ blueprints/qanda/ client_tier/session_state.html, 2006

[18]. Injection Points in Real word XSS http://sandsprite.com/Sleuth/papers/RealWorld_XSS_2 .html

[19]. P. Vogt, F. Nentwich, N. Jovanovic, C. Kruegel, E. Kirda, and G. Vigna. ―Cross site scripting prevention with dynamic data tainting and static analysis‖, 14th Annual Network and Distributed System Security Symposium (NDSS), 2007.

[20] E. Gal´an, A. Alcaide, A. Orfila, J. Blasco, ―A Multi–agent Scanner to Detect Stored–XSS Vulnerabilities‖, IEEE International Conference on Internet Technology and Secure Transactions (ICITST), pp.332-337, June 2010

[21] M. James Stephen, P.V.G.D. Prasad Reddy, Ch. Demudu Naidu Prevention of Cross Site Scripting with E-Guard Algorithm‖, International Journal of Computer Applications Volume 22– No.5, pp. 30-34, May 2011.

[22] XSS Attack Vectors at http://ha.ckers.org/xss.html

[23] shar, l.; tan, h.; ―methods for defending against cross site scripting attacks

[24]StripeFramework,http://stripes.sourceforge.net/docs/current/javadoc /index.html

[25]. WEB4J Framework, http://www.web4j.com/UserGuide.jsp#XSS.

Author Details

Velidi Saibaba is one of the author received B.Tech (IT) Degree from JNTU Kakinada in 2012. He is studying M.Tech in Sri Vatsavayi Krishnam Raju College of Engineering & Technology, Bhimavaram, A.P.

Dr.Penmetsa Vamsi Raja, He did his PhD from JNTU Kakinada AP. He received M.Tech Post Graduation degree in C.S.T department from Andhra University, Visakhapatnam, A.P. He is presently working as Principal in Sri Vatsavayi Krishnam Raju College of Engineering & Technology Bhimavaram AP. He has authored more than 20 relevant publications in journals and Conferences. His Research areas include Computer Networks, Network Security, Cloud Computing, Big Data, Data Mining and Software Engineering.