



# The response-oriented mechanism for delay tolerant network

Banumathi P<sup>1</sup>, Suriya Priya N<sup>2</sup>, S. Yuvalatha<sup>3</sup>

<sup>1,2</sup>Student, Sree Sakthi Engineering College, Karamadai, Tamil Nadu

<sup>3</sup>Assistant Professor, Sree Sakthi Engineering College, Karamadai, Tamil Nadu

## ABSTRACT

*Broadcasting is a method of transferring data to all receiver devices simultaneously. In the proposed system utilizes multi server to store streaming data in which the video content are encoded using trap door hash algorithm and it generate a key for video content. After encoding it is fragmented by content distribution algorithm. The video content are fragmented into several blocks. When the user request the video content the Content Distribution Manager (CDM) send the fragmented data along with digital signature to the user. The sender send digitally signed data to receiver and receiver verify the data using hash of the message. The packet can be send without losses and delay.*

**Keywords:** Trap door, Content distribution, Wireless broadcast, Digital signature, Encoding.

## 1. INTRODUCTION

Network is a collection of computers and servers connected by switches and routers and used to share the resources. Switches are used to connect peers in the intranet and routers are used to connect the intranet to internet. The network classified into two type's wired and wireless network. The wired network use Ethernet cables to connect pc's and wireless is used avoid cabling in large organization, buildings, company's and home. Network security is used to provide security to unauthorized access, modification of content and malicious attacks to the files. Insecure transmission of content to the receiver may lead to attacks.

The type's attacks on the internet are,

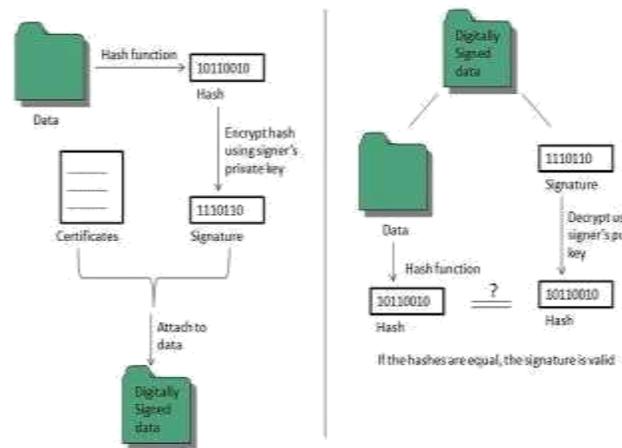
- Eavesdropping
- Modification of content
- IP address spoofing
- Denial of service attack

Wireless broadcast is used in many real time applications (RTA). Examples of real time applications are video conference, online-gaming, E-commerce transaction, Chatting, Instant messaging and video streaming. We focus on online video streaming and the network deliver the content to user.

Wireless network is used for users can move freely around within the area of network like laptop and handheld devices. Types of wireless networks are personal area network, Local area network, metropolitan area network, Wide area network.

Encoding is used to converts the data into another format and it does not require a key only the algorithm is used for both encode and decode. Encryption is used to converts data into another format and it requires a key which is kept secret. Plaintext is converted into cipher text using encryption operation and the cipher text is converted into plaintext using decryption operation along with the key.

Hashing ensures integrity. Hashing takes arbitrary input and produce a fixed-length of data and not possible to go back from output to input. Any modification in the input results to change in the hash. Digital signature works by taking input. Hashing it and then signing the hash by sender's private key. When the receiver receives a message then they validate the signature of hash with senders public key and then hash the message and compare it to hash that was signed by sender. If they match it is unmodified message.



Content distribution network also called content delivery network is consist of distributed networks of servers to deliver a web-content to wireless devices. Edge caching consist of a caching servers used to store the content which is closer to user.

It is based on online video streaming and packet recovery. Multi-slot max clique algorithm is used to preload one delay. Instantly Decodable Network Coding (IDNC) is used to finding packet losses using receiver feedback. The proposed system focusing on the distribution of content based on Content Distribution Network (CDN). Content distribution network consist of distributed servers used to deliver the content to user based on user location.

## 2. LITERATURE SURVEY

Consider a source broadcasting  $M$  packets to  $N$  receivers over independent erasure channels, where perfect feedback is available from the receivers to the source, and the source is allowed to use coding. Instantly Decodable Network Coding (IDNC) is a subclass of opportunistic network coding. IDNC, it cannot guarantee the decoding of a new packet at each receiver in each transmission, which may severely affect its completion delay. Second, it requires full feedback in order to operate properly

## 3. EXISTING SYSTEM

Existing system uses multi-slot max clique algorithm for preloading video content and concentrates on recovery of packet losses if packet lost due any error. The IDNC used for finding lost packet by sending feedback from receiver to sender. The receiver send acknowledgement if the packet correctly received and server store it as zero in the feedback matrix and if the receiver cannot receive packet it then send negative acknowledgement to the server and it store one in the matrix. Feedback matrix consists of set of receivers and packets. Server retransmits the packet corresponding receiver with the use of feedback marked as one.

Want set ( $W_i$ ): lost packets are stored in want set.

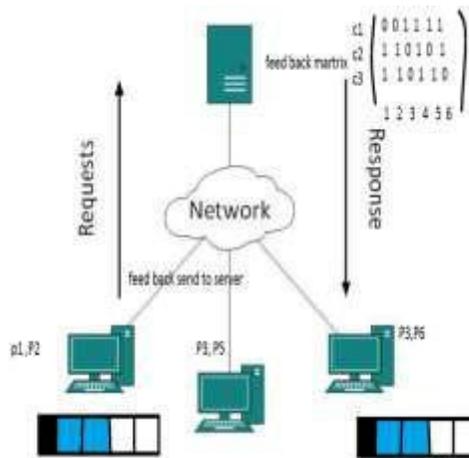
Has set ( $H_i$ ): Correctly received packets are stored in has set.

Has set and want set maintained by the receiver.

$$f_{ij} = \begin{cases} 0 & i \in H_i \\ 1 & i \in W_i \end{cases}$$

IDNC graph is related to information matrix A. let vertex  $V_{ij}$  if the user  $U_i$  wants packet  $P_j$  user index is  $i$  and packet index is  $j$  and there is an edge between two vertices  $V_{ij}$  and  $V_{kl}$  and one of the following conditions hold:

1.  $j=l$ , both user  $U_i$  and  $U_k$  want same packet  $p=p_j=p_l$ .
2.  $p_j \in H_k$  and  $p_l \in H_i$   $u_k$  has packet  $p_j$  that user  $u_i$  still wants and vice versa.

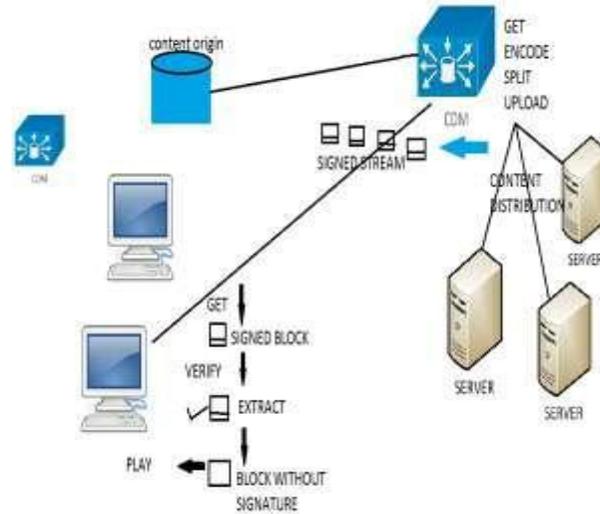


There is no proper authentication for data in peers and everyone can retrieve content without any security.

Delay is high in data transmission while retrieving the video content. There is no security for data owner who uploading video files.

#### 4. PROPOSED SYSTEM

To avoid the slow transmission of the content, the video content are divided into blocks and stored in multiple server and bring content as close as possible to the user. The content are encoded by trap door hash algorithm and it generate a key for the video content and then video content are fragmented by content distribution algorithm and stored in multi-server based on availability. The trap door algorithm decodes the data from the server. Content distribution manager manages the encoding and distribution content to servers. When the user request the video the CDM fetch the blocks from the servers and attach the digital signature to the each and every blocks and send to requested user. The user can play the video content after verify the signature. Digital signature provides the authentication of stream. If server goes down the request will be automatically routed to next server. The traffic and load on the host server is reduced.



The new user can register and previously registered user can enter into application it verifies the whether the authorized user or not. Client authentication is done by the registration. Registration requires a user name, mail and password. The authorized user can only request video uploaded in the content distribution network. Then the request send to nearest content distribution manager which is already do the uploading of video stream into multi-server as a block and the content distribution manager retrieve videos from the server. The content distribution manager defragment the video content and it tolerate out of order arrival block. The content distribution manager sends each and every block with digital signature and content displayed to user after the signature verification.

A content publisher in the CDN network can only enter and do the uploading of video files. Trap door hash creates unique key for the video content and the whole video stream is fragmented by the content distribution network after encoded. After the signature verification only the block stream will be delivered to end user. If individual peer tries to retrieve individual block stream the content will not displayed to the user. The receiver verify each block based on the contents of previously received block.

Our technique minimizes delays in transmitting a stream following the block-signing process and playback of the stream following the block-verification process.

## 5. CONCLUSION

The system reduces the downloading time of the video content. It provides security for the content from unauthorized access, modification, and so on. The receiver can verify the authenticity of data stream. The content stored in multiple server so dependency of single server is tolerated. Response time is increased and workload is decreased.

## 6. REFERENCE

- [1] Anhle, Saber Tehrani, Alexandros dimakis & Athina markopoulou, "Recovery of packet losses in wireless broadcast for real time application" IEEE/ACM transaction on network vol:25 year:2017
- [2] Long hai, Hongyu wang, jie wang "Instantly decodable network coding for multiple unicast retransmission in wireless point to multipoint network" IEEE transaction on vehicular technology. Vol: 65 year: 2016.
- [3] J.Araujo, F.Giroire, J.moulierac, Y.liu, R.modrzejewski, "Energy efficient content distribution"vol:5 year:2016
- [4] Lorenzokeller, Elenidrinea, Christinafragouli "Online broadcasting with network coding" 2008 fourth workshop on network coding, Theory and application. Year: 2008
- [5] Samesh sorour, shahrokh valaee "Minimum broadcast decoding delay for generalized instantly network coding" IEEE global telecommunications conference GLOBECOL, year: 2010
- [6] Samesh sorour, Shahrokh valaee" Completion delay minimization for instantly decodable network coding with limited feedback" IEEE international conference on communications (ICC), year: 2011
- [7] Valentino pacifici, Gyorgy dan"Distributed algorithm for content allocation in interconnected content distribution network"IEEE conference on computer communication year: 2015
- [8] L. Keller, E. Drinea, and C. Fragouli, "Online broadcasting with network coding,"in Proc. IEEE Int. Symp. Netw. Coding (NetCod), Hong Kong, Jan. 2008, pp. 1–6.
- [9] S. Katti et al., "XORs in the air: Practical wireless network coding," IEEE/ACM Trans. Netw., vol. 16, no. 3, pp. 497–510, Jun. 2008.
- [10] X. Li, C.-C. Wang, and X. Lin, "On the capacity of immediately decodable coding schemes for wireless stored-video broadcast with hard deadline constraints," IEEE J. Sel. Areas Commun., vol. 29, no. 5, pp. 1094–1105, May 2011.