I J C T A, 9(40) 2016, pp. 375-382
© International Science Press

Crypto Video Multicast based on QDM

Shaikh Ashfaque R. and P. B. Gosavi

ABSTRACT

Video Multicast in Multi-Rate wireless network attracted significant research, heterogeneity in clients, different bitrate of video data cause clients to adjust with video quality prior work defined for clients who expect differentiated qualities of video security issue with multicast deals like the packet to be multicast is replicated for each client. This transmission cause data packet to be received by other users who have access of network (directly attached to transmission media) and reduce the security and robustness of network. Here we present a novel content aware secured video multicasting protocol for quality differentiated video multicasting. It works in simple two steps 1) Frame analysis 2) Key Embedding & Steganography for QDM. Frames are extracted from the Video data and analyzed and then embedding the key message in that frames to continue processing steganography.

Keywords: Index Terms— Data Embedding, Steganography, QDM, CVM.

I. INTRODUCTION

Wireless broadcast nature is amazing concept to manage bandwidth requirement while multicasting video over multiple bitrate network , devices have different modulation schemes[1], this will waste bandwidth if a member in multicast is having higher bit rate which desire good quality. To overcome this problem Dynamic Rate Adaptation scheme with quality differentiated feature proposed (QDM) [1].

In this paper we are dealing with the information security on specified approach of QDM and dynamic rate adaptation. To secure data this paper proposed simple algorithms based procedure. This procedure include two major steps step-1: Frame analysis in which we divide the video data into n frames to multicast. Step-2: Embedding Message and Steganography. The proposed method deals with the information security i.e. video data to provide security we have embedded text on selected frames of video data. The text we are embedding is simple message string. Steganography is applied to embed data into the video frames.

II. RELATED WORK

In Network Information Flow [3] Rudolf Ahlswede, Ning Cai, Shuo-Yen Robert Li stated with one information source, and they got simple types of the admissible coding rate region. their result can be followed as the Max-flow Min-cut Theorem for network information flow. Contrary to one’s intuition, their proposal shows that it is in general not optimal to esteem the information to be multicast as a “fluid” that can simply be sent or replicated.

Radhika Gowaikar, Ravi Palanki, Babak Hassibi, Michelle Eros stated in Capacity of wireless erasure networks [4] at multicast problems over these networks.The capacity under the hypothesis that erasure places on all the links of the network are provided to the destinations is acquired. It depicts that the capacity region has a nice max-°ow min-cut interpretation. The definition of cut-capacity in these networks integrates the broadcast ability of the wireless medium. It is further shown that linear coding at nodes in the network sources to achieve the capacity region.

[*] Department of Computer Engineering, GF’s Godavari COE jalgaon, Maharashtra, India, *E-mail: sk.ashfaque.shaikh@gmail.com; Gosavi.pramod@gmail.com*

In Secure Routing for Mobile Ad hoc Networks [5] Panagiotis Papadimitratos and Zygmunt J. Haas present a route discovery protocol that eases the damaging effects of such malicious behavior, as to provide precise connectivity data. Our protocol guarantees that invented, compromised, or replayed route answers would either be rejected or never reach back the querying node. Also, the protocol sensitivity is secured under different types of attacks that exploit the routing protocol itself.

In “Weakly Secure Network Coding” [6] Kapil Bhattad and Krishna R. Narayanan illustration that under the new security requirements communication is possible at the multicast capability. A lined alteration is provided for networks with a given linear code to mark the system safe. The transformation required to be done solitary at the source and the operations at the intermediate nodes remain unaffected.

“The SecureRing Protocols for Securing Group Communication” Kim Potter Kihlstrom, L. E. Moser, P. M. Melliar-Smith describe here SecureRing, a suite of group communication protocols that provide protection against Byzantine faults. These protocols multicast messages to groups of processors within an asynchronous distributed system, impose a consistent total order on messages, and maintain consistent group memberships.

In CASM [2], A Content Aware Secure Multicast defined three modules 1) a scalable light-weight algorithm for group key management; 2) a content-aware key embedding algorithm that can make video quality distortion imperceptible and is reliable for clients to detect embedded keys 3) a smart two-level video encryption algorithm that can selectively encrypt a small set of video data only, this paper ensure the video as well as the embedded keys unrecognizable without a genuine key. The implementation of the CASM protocol is independent of the underlying multicast mechanism and is fully compatible with existing coding standards. Performance evaluation studies built upon a CASM prototype have demonstrated that CASM is highly robust and scalable in dynamic multicast environments. Moreover, it ensures secure distribution of key and video data with minimized communication and computation overheads. The proposed content-aware key embedding and encryption algorithms are fast enough to support real-time video multicasting.

QDM [1] propose a rate scheduling model that selects the optimal transmission bitrate for each video frame to maximize the total visual quality for a multicast group focus to the minimum-visual-quality-guaranteed limit. We then propose a practical and easy-to-implement protocol, called QDM, which makes a cluster-based structure to divide node heterogeneity and adjusts the transmission bit-rate to network dynamics based on video quality observed by the representative cluster heads. Since QDM selects the rate by a sample-based method, it is appropriate for real-time communication streaming even without any preprocess. We demonstrate that QDM can adjust to network dynamics and variable video-bit rates competently, and yield a gain of 2-5 dB in relations of the average video quality as related to the leader-based approach.

III. PERFORMANCE PARAMETERS

(a) **Loss Probability:** Packet loss occurs when packet fails to reach its destination. The probability of packet loss can also affect multicasting.

(b) **Time:** Time required transmitting subset of frames over the network as we are working with the Multirate network hence bandwidth heterogeneity of client effect time.

(c) **Video Quality:** Video quality or visual quality is quality of video to be transmitted. As we have clients whom bandwidth requirements may vary and therby our motive is to maintain the maximum quality as per their bandwidth requirement.

(d) **Visual Degradation:** This norm calculates the perceptual distortion of the video data with respect to the plain video. In some applications, it could be desirable to achieve enough visual degradation, so that an attacker would still recognize the data however favor to pay to access the unencrypted content. However, for sensitive data, high visual degradation could be desirable to completely disguise the visual content [8].

(e) **Encryption Ratio:** This criterion measures the ratio between the size of encrypted part and the whole data size. Encryption ratio has to be minimized to reduce computational complexity [8].

(f) **Speed:** Encryption and decryption algorithms should be fast enough to meet real time requirements [8].

IV. METHODOLOGY

The security of video data is very important concept which leads to paper propose a novel approach of video security with optimum speed as described in figure 4.7. The input to the system is the video data. QDM [1] protocol proposed the Cluster based multicasting in wireless multirate network. In which authors described the efficient method of multicasting in this paper we dealing on QDM[1] to provide security. The Security comes in various ways like traditional methods which deals with only authentication and authorization using UserID and passwords. Those are traditional methods of providing security by which the data still persist on the channel as in the case of multicasting in the result unauthorized user may get access to the data. In this paper we proposed the novel method of providing security in video multicasting based on QDM. This technique embed text directly into the video by which the video frames will get encrypted and the users which are knowing the text can retrieve the data. The process of CVM (Crypto Video Multicast) is carry out in two steps step 1. Frame Analysis, 2. Encryption and Steganography.

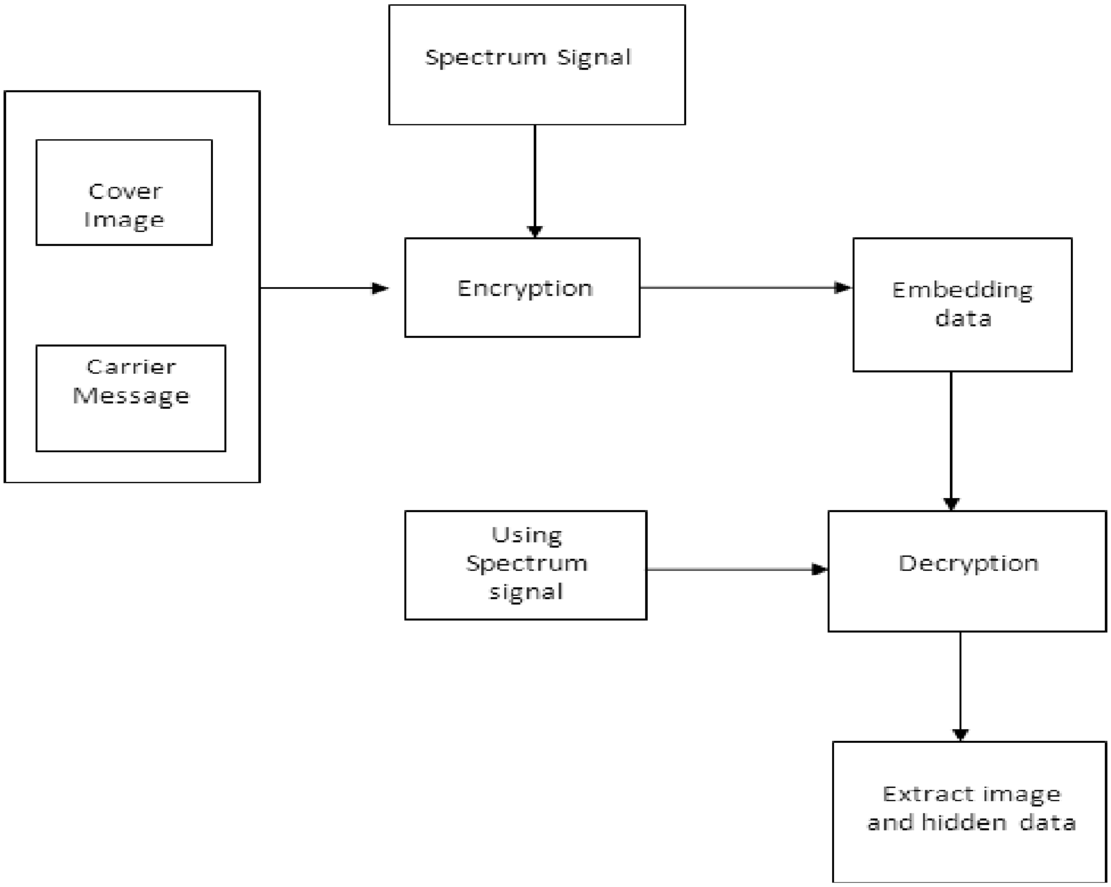

Figure 1: Functional block of CVM

4.1. Frame Analysis

Frames are images which compose the complete moving picture as video that means video data is made up of sequence of frames which is audio visual element [9]. In this proposed system we divide video into the frame Group say F= {f_1, f_2,…, f_n } where f denotes the frame and n indicates no if frames in the video data. The system having Members in m1ulticast M= {m_1, m_2, …, m_j} where m is the member of multicast group and j is the no of members in the group. The rate of multicast group is given by R= {r_1, r_2, …, r_k}. In CVM we have analyzed frames to provide security. For the reason mentioned in CVM steganography is applied on the frames to provide security the frames are then multicast through the channel and only member are able to retrieve the content those are having the secret message key which is embedded in frames.

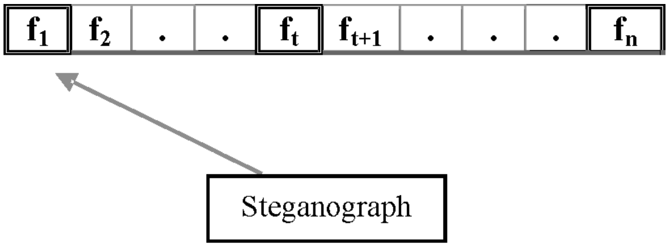

Figure 2: Selective Encryption in CVM

4.2. Steganography and Encryption

The main objectives of CVM are to encrypt data and reduce the encryption time. The proposed system will use steganography to achieve the objectives. Steganography is the art of hiding text behind the other object like image, video etc. Video steganography using TPVD [11] uses all frames to embed data in it but their motive is just to embed data in the video. In this paper we are dealing to provide security by means of steganography. CVM is using steganography for providing the security by means of hiding text behind the analyzed frames. We consider here the text to be embed into the frame f_t is T. Syndrome trellis code can be emerged here to provide the steganography. The compressed technique STC we could use to embed data behind the text. We hide the T message into video, by using this we eliminate the need of another communication process which traditional methods use to authenticate and authorize data and reduce the time and durability of system. Digital watermarking is a mostly studied data embedding. As a result. For consistent data embedding, Alattar et al. [12] have suggested that the original compressed stream can be partially decoded to uncover its syntactic items such data as Discrete Cosine Transform (DCT) coefficients can then be modified to insert the watermark. The CVM is motivated by this technique. It lets the frames average size value of certain regions in f_t-frames to embed data.

The video data has high data rate and long playback duration thus video have huge volume of data. It is not feasible to encrypt the entire video, thus selective encryption is advocated. The selective encryption algorithm in CVM uses for few frames F'={f_1,f_2,..f_t} where t<n, and F' is the subset of F. This algorithm is quicker because of selective encryption.

Therefor the steps in this paper include three major existing algorithms. 1. Steganography algorithm syndrome trellis algorithm to embed the data into the selected frames. 2. DCT algorithm to provide digital watermarking on the video data. 3. Selective encryption to provide encryption of video data

Then finally this process is applied to the QDM [1] protocol

4.3. The QDM

The Kate Ching-Ju Lin, Wei-Liang Shen, Chih-Cheng Hsu, and Cheng-Fu Chou, proposed a novel method of multicasting video in multirate wireless network called QDM-Quality Differentiated Video Multicasting.

They used efficient algorithm to provide multicasting in multirate wireless network. Use of cluster again strengthen their algorithm. In this paper we will provide the video security in QDM by applying the above described method of security process. Video quality in QDM is given by where PSNR is the expected quality of video as per the QDM protocol which is described in QDM[1].

Video Quality = PSNR_{exp}

While the Mean Square Error is given by

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[f(i,j)] - f'(i,j)]^2$$

$$PSNR = 10\log\frac{p^2}{MSE}$$

Where p is Maximum pixel value f ( ) is frames and f' ( ) is distorted frames. Quality of video is calculated by means of PSNR.

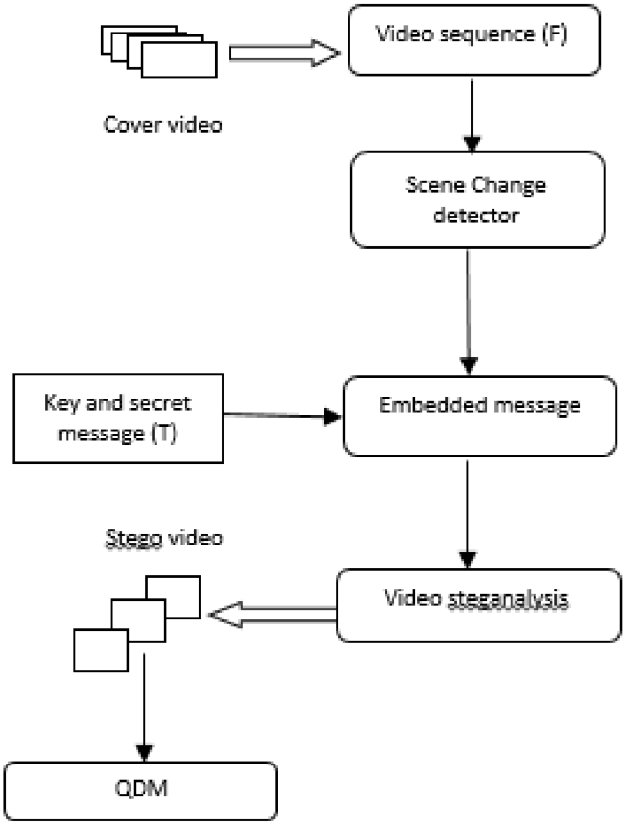

Figure 3: Architecture of CVM

The CVM works in the way it first analyze frames as shown in section 4.1 means simple as a part of coding the we divide video data into n frames e.g. say n is 100 then video is divided in the 100 frames and based on size of frames further processing is performed. In the next step we have to select the frames on which we have to embed secret key as the proposed part we are embedding secret keys on selected frames as mentioned in section 4.1. This embedded key is the core concept of this proposed work after multicasting this key is to be match with the receiver if found correct the video data is allowed then otherwise this system will deny the video data. In the next step hiding data into the frame is done using syndrome trellis coding and key exchange process is performed using DCT Discrete Cosine Transform

Algorithm

```
1. [Frame Analyze]
   Repeat for s=0 to n [where n is number of frames]
   f[s]=extractframe.
2. Select frames for encryption f'[s]={$f_1$, $f_2$, ..$f_t$}
3. [AES encryption]
   3.1 Byte substitute state[16][16]=frames(f')
   3.2 Shift rows
             Repeat for r=1 to 16
                   Repeat for c=16 to 1
                   Swap state[r][c] to state[r][c-1]
   3.3 Mix column and add round key key[x]+state[r][c]
4. Apply Syndrome Trellis Codes and DCT
   4.1 Emb (x,m)=D(x,y)
   4.2 For Extraction Ext(y)=Hy
5.  Proceed with QDM.
```

The algorithm shown depicts the general architecture for CVM and proposed system.

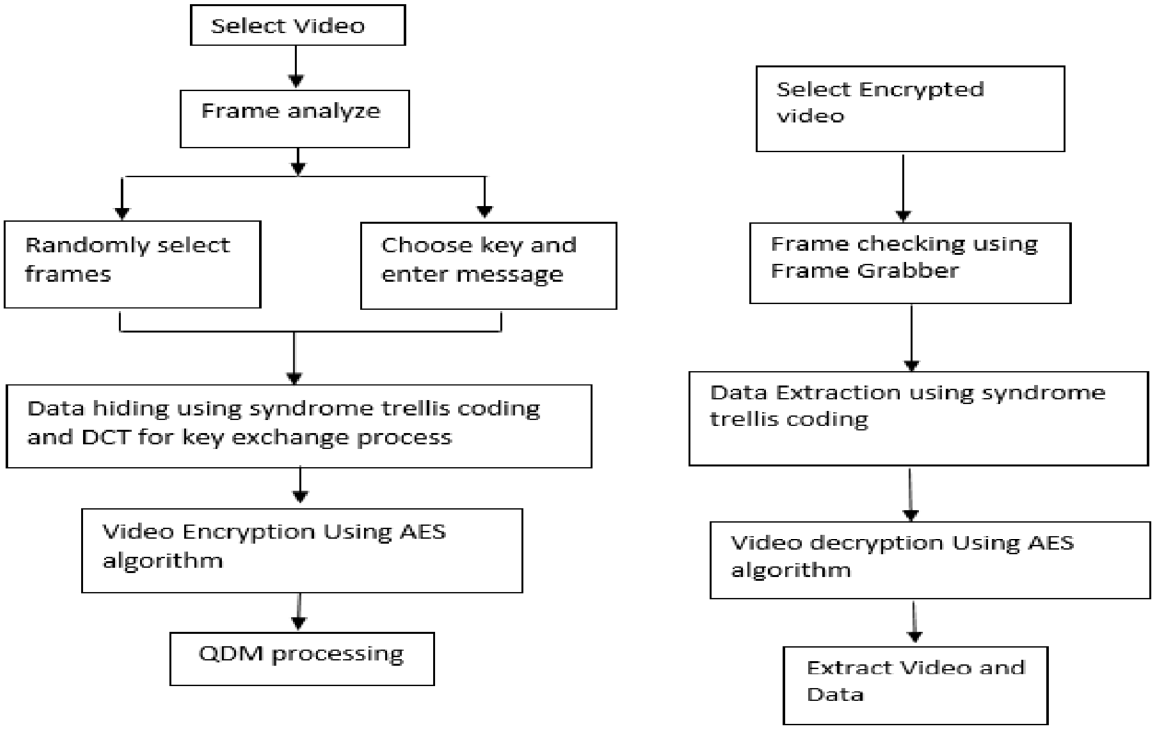
Select Video
Frame analyze
Randomly select frames
Choose key and enter message
Data hiding using syndrome trellis coding and DCT for key exchange process
Video Encryption Using AES algorithm
QDM processing
Select Encrypted video
Frame checking using Frame Grabber
Data Extraction using syndrome trellis coding
Video decryption Using AES algorithm
Extract Video and Data

Figure 4: Module Flow of System : Encryption(left), Decryption(right)

The flow of proposed system is described with the help of module flow diagrams as fig 4.4. Shows the algorithm flow chart of encryption phase as depicted in the algorithm aforementioned while the fig 4.4 depicts the decryption phase.

V. SIMULATION AND RESULTS

We have conducted experiments over a variety of video sequences to investigate the fmeasures. Fig 5.1 shows a video frame with a 60 bit secret message embedded (left) and original frame (right), as well as the encrypted frame in 5.1 c. This sequence containing 100frames is taken from a sample cookie video

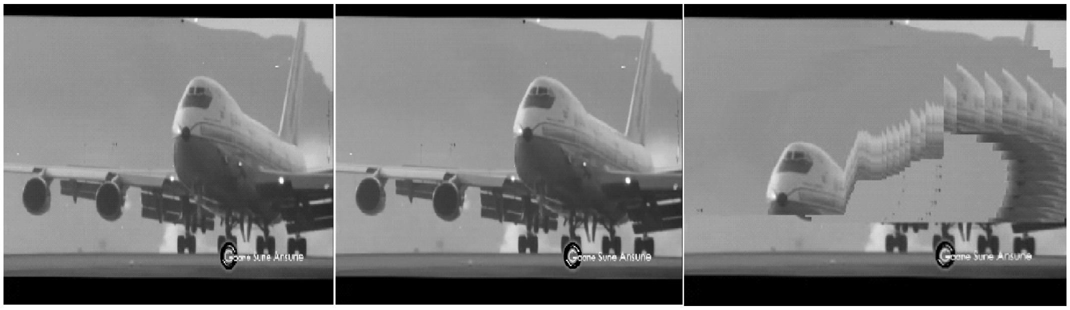

Figure 5.1: Video frame a) Stego Frame b) Original frame c) encryptd frame

The Loss probability indicates the loss of packets in transmission in CVM the loss probability as same as QDM as we are dealing with security phase only hence two more parameters are same as QDM in CVM the video quality is same as QDM and the Time of transmission for the video in multicasting. The rest parameters are related to video encryption which we can improve to demonstrate the CVM. The video cryptography is broadly characterized in several algorithms enlist Fully Layered video cryptography permutation based video cryptography selective encryption. In CVM we used selective encryption as mentioned in section 4.1 we have selected any of four frames and applied encryption on the selected frames. Below table shows the comparison table of algorithms the parameters for fully layered and permutation based algorithms are referenced from the research of jolly shah and vikas saxena [8] and CASM content aware secure multicast algorithm parameters are referenced from the Hao Yin and other authors [2] and CVM parameters are calculated by the experiment performed. Where VD stands for Visual degradation, ER for Encryption ratio and Speed of Encryption denoted by Speed

Table 5.1
Parameter comparison in algorithms

Algorithm	*VD*	*ER*	*Speed*
Fully Layered	H	100%	Slow
Permutation Based	H	100%	Fast
CASM	V	100%	Fast
Selective CVM	V	4-10%	Fast

CONCLUSION

Broadcasting nature can allow the video streaming to be accessed by the unauthorized user hence here we can secure video by emerging digital signature to the video data by means of steganography over the network so that no unauthorized user can able to decrypt the video. QDM provide the best multirate multicasting of video and we can provide security in the QDM. Data embedding, Group key management and Selective encryption can be emerged into the QDM protocol we embed rekey message to avoid separate control channel for key transmission for the clients. We encrypt motion vectors and DC components only. Modified version of these combined algorithms can provide extreme quality based multirate multicasting of QDM with the great security based on Content aware secure multicasting of video.

In this paper we proposed a Secured video Multicasting for Quality differentiated video multicast based on selective encryption. We used selective encryption to demonstrate less use of encryption with strong support of steganography. This process is repeated for different number of frames to be encrypted. The encryption and decryption process are simple enough to be carried out on any large sized video data, but provides enough security.

REFERENCES

[1] Kate Ching-Ju Lin Wei-Liang Shen, Chih-Cheng Hsu, and Cheng-Fu Chou, "*Quality-Differentiated Video Multicast in Multirate Wireless Networks*", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 1, JANUARY 2013.

[2] Hao Yin, Chuang Lin, Feng Qiu, Jiangchuan Liu, Geyong Min, Bo Li "*CASM: Content-Aware protocol for secured video multicast*", IEEE Transactions on Multimedia (Volume:8 , Issue: 2).

[3] Rudolf Ahlswede, Ning Cai, Shuo-Yen Robert Li, Senior Member, IEEE, and Raymond W. Yeung, Senior Member **"***Network Information Flow*" IEEE Transactions on Information Theory (Volume:46 , Issue: 4)

[4] Danay, Radhika Gowaikar, Ravi Palanki, Babak Hassibi, Michelle E ros Amir F "*Capacity of wireless erasure networks*". IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 52, NO. 3, MARCH 2006

[5] Panagiotis Papadimitratos and Zygmunt J. Haas *"Secure Routing for Mobile Ad hoc Networks"* In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002

[6] Kapil Bhattad and Krishna R. Narayanan "*Weakly Secure Network Coding"*

[7] Kim Potter Kihlstrom, L. E. Moser, P. M. Melliar-Smith "*The SecureRing Protocols for Securing Group Communication"*

[8] Jolly shah and Dr. Vikas Saxena, "*Video Encryption: A Survey* ", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011.

[9] Aleksander Kostuch1, Krzysztof Gier³owski2, Jozef Wozniak2, "Performance analysis of multicast video streaming in IEEE 802.11 bgn testbed environment"

[10] Tomáš Filler, Jan Judas, and Jessica Fridrich "Minimizing Embedding Impact in Steganography using Trellis-Coded Quantization"

[11] Sherly A P and Amritha P "*A Compressed Video Steganography using TPVD"* International Journal of Database Management Systems (IJDMS) Vol.2, No.3, August 2010 DOI : 10.5121/ijdms.2010.2307 67

[12] Adnan M. Alattar, Member, IEEE, Eugene T. Lin, Student Member, IEEE, and Mehmet Utku Celik, Student Member, IEEE "*Digital Watermarking of Low Bit-Rate Advanced Simple Profile MPEG-4 Compressed Video"* IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 13, NO. 8, AUGUST 2003

[13] V .Venkatramani, R .Madhanmohan "*Rate Adaptive Video Multicast in Multirate Wireless Networks*" Volume 4, Issue 11, November 2014.

[14] O. Alay, T. Korakis, Y. Wang, and S. Panwar, "*Dynamic Rate and FEC Adaptation for Video Multicast in Multi-Rate Wireless Networks*" Mobile Networks and Applications,vol. 15, pp. 425-434, 2009.

[15] S. Lee and K. Chung, "*Combining the Rate Adaptation and Quality Adaptation Schemes for Wireless Video Streaming*" Visual Comm. and Image Representation, vol. 19, no. 8, pp. 508- 519, 2008.

[16] D.-N. Yang and M.-S. Chen, "*Bandwidth Efficient Video Multicasting in Multiradio Multicellular Wireless Networks*" IEEE Trans. Mobile Computing, vol. 7, no. 2, pp. 275 -288, Feb. 2008.

[17] S. Pal, S.R. Kundu, A.R. Mazloom, and S.K. Das, "*Video Rate Adaptation and Scheduling in Multi-Rate Wireless Networks*" Networking: Proc. Sixth Int'l IFIP-TC6 Conf. Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet, pp. 475-487, 2007.

[18] Desmond S. Lun, Muriel M´edard, Ralf Koetter, and Michelle Effros. "*On Coding for Reliable Communication over Packet Networks*" Physical Communication Volume 1, Issue 1, March 2008.