An Enhanced and Effective Encrypting Algorithm for High Volume Video Data Streaming Application on MANET

Saurabh Kumar
Dept. of E & CE, IIT Roorkee
Roorkee-247667, India

Sandeep Kumar
Dept. of E & CE, IIT Roorkee
Roorkee-247667, India

ABSTRACT
In this paper we are proposing an effective encryption technique for high volume streaming data which has been sent over various communication links throughout the network. Applications requiring high volume of streaming data transmission include audio-video conferencing or Voice over Internet Protocol (VoIP) and Internet Protocol Television (IPTV). In general, whenever we use these types of applications the emphasis is always to achieve transfer rate as high as possible between one peer node and another. As a matter of fact while taking these things into consideration security issues related to data are always overlooked and this can cause a big problem. Also, when the data is transmitted over wireless network such as MANET (Mobile Ad hoc Network), the limited wireless bandwidth and computational capability will lead to new security challenges. This paper is a solution to such security problems which are faced in case of streaming data transmission.

General Terms
Video Encryption, Security, Algorithm, MANET.

Keywords
Encryption, Decryption, Streaming, MANET, XORing.

1. INTRODUCTION
With the development of network multimedia system, systems will make continuous media streaming. It is very important to secure networked continuous media data from potential threats such as hackers, eavesdroppers etc. The applications for streaming are endless such as video conferencing, interactive web site etc. Some applications are Internet broadcasting (corporate communication), education (viewing lecture and distance learning) web based channel (IP-TV, internet radio) and video on demand (VOD). In all the streaming applications, high volume of data is transmitted over the network. Since traditional encryption algorithms often fail due to the extra high volume and latency sensitiveness of media data, security becomes a challenging task [1][2].

Sending a video stream (such as Video conferencing, VOD) over a network in real time requires that the transmitted frames are sent in a limited delay. Moreover, video frames needs to be display at a certain interval. The quality of video is directly proportional to the frame rate. So, if we want to achieve good quality video transmission it is required that a number of frames will transmitted over the network in a fixed time frame; therefore, sending and receiving encrypted packets must be sent in a certain amount of time in order to achieve quality video transmission over the network.

When playing a video streaming over a wireless network such as MANET [3], where wireless terminals (like PDAs, mobile phones, palmtops) access in video conferencing system, new challenges will be brought about [4]. First of all, a refactoring of the original system with security design should be considered because of limited wireless bandwidth of wireless terminals. In addition, a lightweight encryption algorithm to protect the media data should be given because of the limited battery power and the computational resource.

The goal of this paper is to propose a security scheme which reduces latency overhead by modifying existing approaches for encrypting video data using a probabilistic encryption of frames based on the hybrid of existing encryption scheme and the proposed XORing [5] scheme. The XORing scheme requires lesser time and its probabilistic application ensures that the overall security level is not degraded. This scheme can be efficiently used for communication in MANET. In addition, it is best suited for the communication between hand-held devices such as PDAs, mobile phones, palmtops etc. The algorithm can be used between the sites where the processing capacity and battery power are limited and efficient encryption is the main necessity.

2. FRAME BASED ENCRYPTION OF STREAMING DATA [6]
This algorithm encrypts video data frame by frame because a video is the sequence of the images (frames) which are presented in a sequence one after another in a constant time slice. That's why, the main concept of this algorithm is to perform encryption or decryption on an individual frames. That's why this algorithm is called Frame based Encryption of streaming data. This algorithm is a symmetric key encryption algorithm in which two keys are used. One is a static Key and another is dynamic. Static key is transferred before any data transmission is carried out by using a secure communication link (on connection oriented environment). And the dynamic key is send with encrypted video frame.

2.1 Encryption Phase [6]
[6] proposes a frame based encryption technique for encryption of audio, video data. In this technique encryption of individual RGB video frames, of sizes such as 640 X 480, of a video transmission is considered. Steps involved in the encryption phase are described as follows:

Step1: First a row matrix P is calculated. The row matrix is shown in (1) and its elements are the number of 1s that are present at the m^{th} bit of the m-sized byte segment.

$$P = [p_m\ p_{m-1}\ p_{m-2} \ldots\ldots\ldots\ldots\ldots\ldots p_1] \quad (1)$$

The row matrix P consists of frequency of 1s occurring in a single image frame based on reading m bytes at a time.

Step2: m^2 bytes of data are read at a time and each byte is placed in a square matrix Q of dimension m X m. This matrix is the one which is encrypted and send to the receiver.

Step3: Hadamard product is performed between each row of matrix Q and the row matrix P. After performing the hadamard product, we will get a hadamard product matrix Q_H.

If r and s are two sets on which Hadamard product is performed then

Hadamard product (r.s) = $r_{i,j} . s_{i,j}$

Step4: Diagonal Exchange: exchange the left diagonal element with right diagonal element and right diagonal element with left diagonal element of the resulted hadamard product matrix. After performing the diagonal exchange we will get a diagonal exchanged matrix Q_D.

Step5: Rotate Anticlockwise: After performing diagonal exchange, the remaining elements of matrix are rotated in Anticlockwise with the angle θ radian. θ is calculated with the following equation:

$$\theta = m * \pi /2 \qquad (2)$$

where m >=1.

The procedure for rotating remaining elements of the matrix Q_D anticlockwise is as follows:

[6]RotateAntiClock(θ)

m= θ / (π/2)

For every i=1…....m

For every j=2…..m-1

Buff1[j]= Q_D 1,j

Buff2[j]= Q_D j,1

Buff3[j]= Q_D m,j

Buff4[j]= Q_D j,m

End For

For every j=2…..m-1

Q_D 1,j=Buff4[j]

Q_D j,1=Buff3[j]

Q_D m,j=Buff2[j]

Q_D j,m=Buff1[j]

End For

End For

End RotateAntiClock

After rotating anticlockwise operation on the matrix Q_D, it will generate a new matrix called Q_θ.

Step6: XOR operation: Firstly a matrix X is generated randomly whose value ranges from 0 to 2^{m-1} and the size of this randomly generated matrix is equal to the size of the matrix Q_θ and the determinant of the matrix X is not equal to 0. After generating random matrix X, XOR operation is performed in between X and Q_θ. After performing XOR operation, Q_{PE} matrix is generated. The element of the matrix X is generated using procedure given in [6].

Step 7: Matrix Multiplication: A matrix multiplication is performed between randomly generated matrix X and the matrix Q_{PE} comes from the XOR operation performed in step 6. The result of this operation is encrypted matrix E.

2.2 Key Distribution [6]

As discussed earlier, the key set for encryption is divided in two sets that are static key set and the dynamic key set. The static key set is (m, θ, X, f), where m is the dimension of data matrix Q, θ is the anticlockwise rotation angle for the rotating non-diagonal elements, X is the randomly generated matrix whose value ranges from 0 to 2^{m-1}, and the f is the framing sequence which is used to determine the position of the dynamic key in the upcoming data. The value of f is either -1 or 1. A 1 will signify that the dynamic key P is appended at the top of the encrypted frame and -1 will indicate that the key P is appended at the bottom of the frame.

2.3 Decryption Phase [6]

The decryption process is just the reverse of the encryption process. The process of decrypting a frame is as follows:

Step1: From the frame count, find the value of f and extract the dynamic key P.

Step2: Find the inverse of X using the method described in [7] or [8].

Step3: Matrix multiplication of the encrypted frame E with the inverse of X called EX^{-1}.

Step4: Perform XOR operation of EX^{-1} with the X.

Step5: Perform θ operation clockwise using following procedure:

[6] RotateClockWise(θ)

m= θ / (π/2)

For every i=1…....m

For every j=2…..m-1

Buff1[j]= Q_D 1,j

Buff2[j]= Q_D j,1

Buff3[j]= Q_D m,j

Buff4[j]= Q_D j,m

End For

For every j=2…..m-1

Q_D 1,j=Buff2[j]

Q_D j,1=Buff3[j]

Q_D m,j=Buff4[j]

Q_D j,m=Buff1[j]

End For

End For

End RotateClockWise

Step6: Diagonal Exchange: exchange the right diagonal element with the left diagonal element and the left diagonal element with the right diagonal element.

Step7: Divide each row of the matrix obtained from step 6 element by element by using P. It will give the original data frame.

3. MODIFIED FRAME BASED ENCRYPTION ALGORITHM

We made modification in the encryption phase and the decryption phase. In this, we use existing encryption and decryption algorithm with the hybrid of XORing on the probability basis. The key distribution is the same as the existing algorithm. In this strategy, there is a need for saving previous frame for the encryption of newly arrived frame. If F_i is the current processing frame then F_{i-1} (previous frame) is stored on both the ends (sender and receiver). The modified encryption and decryption phase is as follows:

3.1 Encryption Phase

Modified encryption procedure is shown in fig 1. In this, first we generate a random number R in between 1 and 10 both inclusive. This random number is compared with a threshold T which will decide the encryption strategy to encrypt the current frame. If the value of R is greater than T, the original encryption algorithm (discussed in section 2.1) is used to encrypt the frame. Otherwise XORing is performed with the previous frame and all the elements of row matrix P are set to 0.

3.2 Decryption Phase

Modified decryption procedure is shown in fig 2. In this, first we extract the row matrix P from the upcoming data by using the frame sequence f. The elements of row matrix P decide the strategy of the decryption phase. If all elements of row matrix P are 0 than the XOR operation is performed between current encrypted frame and the previous decrypted frame at the receiver end.

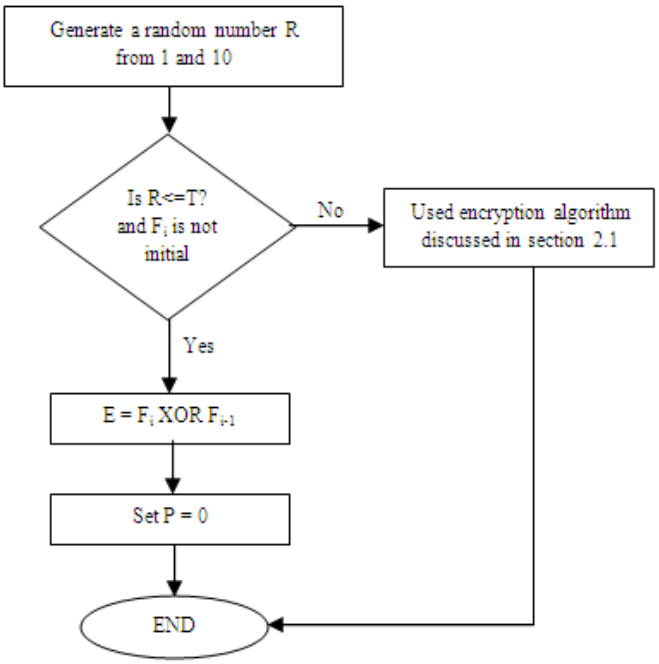

Fig 1: Modified Encryption Procedure

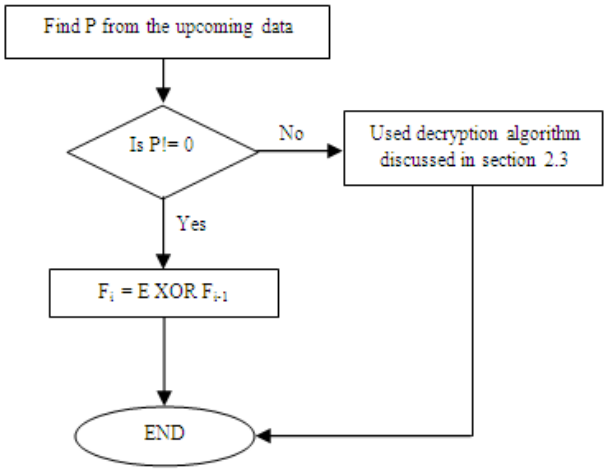

Fig 2: Modified Decryption Procedure

4. ANALYSIS AND COMPARISION

As our finding, in the original encryption and decryption phase, a lot of matrix operations are involved. Matrix operations are time consuming. If these operations are performed on handheld devices such as palmtops, mobiles, PDAs etc, which have low computation capability and are commonly used in MANETs; a lot of processing time will be consumed. If XOR operation is used, it will take less amount of time because it is implemented in hardware. If only XOR operation is used to encrypt data then data is less secure, and also predictable. After understating all these facts, this paper represents a hybrid of both XORing and the previous frame based algorithm to encrypt data.

The time reduction in encryption and decryption phase is directly proportional to the threshold value T. The value of T decides how many frames are encrypted using the XOR operation with the previous frame.

Suppose if a frame is encrypted with the XOR operation instead of original encryption algorithm, and it will take half of the time taken in original encryption algorithm. Here the random number R is in the scale of 10 and the value of threshold T also lies between 0 and 10. 0 means the hybrid algorithm works as original algorithm. So the number of frames that are encrypted or decrypted by XOR operation is directly proportional to the value of threshold T.

Let there is a 100 frames of video available to send. If original scheme takes t time to encrypt a frame, then using XOR it will take t/2 time. So the total amount of time taken by original algorithm in encryption phase is 100t and following table 1 shows the encryption time taken by the modified algorithm with the different value of T ranging from 1 to 6.

From table 1, it is clearly indicated that the value of T decides by how much percent this modified algorithm is faster than the previous algorithm.

Table 1. Time taken in modified algorithm

T	Encrypted frame by XOR	Encrypted frame by original algorithm	Total time
1	10	90	95t
2	20	80	90t
3	30	70	85t
4	40	60	80t
5	50	50	75t
6	60	40	70t

5. CONCLUSIONS

The security of the original encryption algorithm is not reduced after modifying the algorithm. The hybrid scheme is as secure as the original encryption technique because we do not change the key distribution technique. In the modified algorithm, only encryption and decryption phases are modified, and their probabilistic approaches ensure that it is not easily predictable. Predictability is low because in this modified algorithm the encryption strategy is decided randomly with the help of two values one is random number R and another one is threshold T.

6. REFERENCES

[1] Liu, X., and Eskicioglu, A. M. 2003 Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Direction., IASTED International Conference on Communications, Internet and Information Technology (CIIT 2003), Scottsdale, AZ, November 17-19,2003.

[2] Liu, F. W., and Koenig, H. 2005 A Novel Encryption Algorithm for High Resolution Video. NOSSDAV2005, Wash, USA, pp.69-74, 2005.

[3] Zhou, L., and Haas, Z. J. 1999 Securing ad hoc networks. Network, IEEE, vol.13, no.6, pp.24-30, Nov/Dec 1999.

[4] Gibson, J. D., Servetti, A., Dong, H., Gersho, A., Lookabaugh, T., and Martin, D. JC. 2004 Selective Encryption and Scalable Speech Coding for Voice Communications over Multi-hop Wireless Links. IEEE MILCOM04, 2004.

[5] Stallings, W. 2005 Cryptography and Network Security, Principles and Practice. Pearson education, Third Edition, 2005.

[6] Rahman, T.R. 2010 A Dynamic Encryption Algorithm for Multicast/Broadcast Streaming Applications, Fourth Asia International Conference on Mathematical/Analytical Modelling and Computer Simulation, 2010.

[7] Cormen, T. H., Leiserson, C. E., and Rivest, R. L. 1990 Introduction to Algorithms, First Edition, 1990, MIT Press and McGraw-Hill, Cambridge, MA, USA.

[8] Steven, C., and Canale, R. 2003 Numerical Methods for Engineers, 2003, Tata McGraw-Hill India.