

PERFORMANCE OF CIPHERING AN AUDIO AND VIDEO IN ADHOC NETWORK

M. Radha¹, S. Irudhaya Ananthi², K. Rani³

¹Dept of Computer Science, Jayaraj Annapackiam College for Women (autonomous), Periyakulam (Taluk), Theni (Dt)

^{2,3}Assistant Professor, Dept of Computer Science, Jayaraj Annapackiam College for Women (Autonomous), Periyakulam, Theni(Dt)

Abstract - Security is one of the most challenging aspects in the internet and network applications. Symmetric key algorithms are a typically efficient and fast cryptosystem, so it has significant applications in many realms. For a wireless ad hoc network with constraint computational resources, the cryptosystem based on symmetric key algorithms is extremely suitable for such a lively and dynamic environment, along with other security strategies. The majority of today's information hiding systems use multimedia objects like image, audio and video files. However, based on the features of wireless devices, a wireless ad hoc network has special security and efficiency requirements for conventional ciphering techniques. In this paper analyze performance of ciphering an audio and video in adhoc network.

Keywords - wireless security, Selective Cryptographic algorithm. Ciphering audio and video

I. INTRODUCTION

Ciphering technique is a new kind of secret communication technology. The majority of today's information hiding systems use multimedia objects like image, audio and video files. However, based on the features of wireless devices, a wireless ad hoc network has special security and efficiency requirements for conventional ciphering techniques. In this proposed paper it will provide technique, which gives us more secure in information hiding system using ciphering methods. In company, there is no proper security for sharing files among them. Because it is stored on centralized system and any unauthorized people will theft the information. So this paper will help them to protect information using ciphering. For example, project leader sends text, audio or video file to the project members. First session, they use the method of converting plaintext into cipher text. The messages are converted into an encrypted format in the sender side and then this cipher text is hidden for the security purpose. In sender form, It has 2 question with answer and we send files which either or text, audio or video to the receiver, then answer will be automatically send to the receiver mail-id. Then the second session, destination side, they decrypting the file using the password that sent to their e-mail id and then they do work on it.

Through selective encryption, not all messages are necessary to be encrypted while the entire data transmission can be viewed to be secure on the whole. Selective encryption is able to improve the scalability of data transmission and reduces the processing time. For multimedia communications, it often requires real-time data transmission, so tremendous audio and video data need to be transferred securely. Selective Encryption algorithm reduces computation time and power without compromising the security of the transmission.

II. RELATED WORK

Through selective encryption, not all messages are necessary to be encrypted while the entire data transmission can be viewed to be secure on the whole. Selective encryption is able to improve the scalability of data transmission and reduces the processing time.

Yonglin Ren, Azzedine Boukerche ,Lynda Mokdad [1] presents the principle of selective encryption and proposed a probabilistically selective encryption algorithm based on symmetric key. By utilizing probabilistic methodology and stochastic algorithm, a sender includes proper uncertainty in the process of message encryption, so that only entrusted receiver can decrypt the ciphertext and other unauthorized nodes have no knowledge of the transmitted messages on the whole. Selective encryption is one of the most promising solutions to reduce the cost of data protection in wireless and mobile networks. K.VetriVel, Dr. C.Senthamarai[2] analyzed a comparative study of computing resources such as speed, block size, key size and security level of most commonly used block ciphers in the symmetric encryption method and hence block Cipher algorithms a good choice for communication Security. The use of block cipher in symmetric key encryption algorithm for any type of file will impact on the levels of security and memory consumption. In this paper the authors presents a comparison study of block ciphers such as AES, DES, 3DES, Blowfish, RC2, and RC6 on the basis of block size, key size, and speed. S.Kala [3] implement the concept of selective encryption algorithm for wireless ad hoc network with the Quadrature Mirror Filters and Lossless compression techniques.

In a Toss-A-coin algorithm only 50% of communicated data will be encrypted and remaining 50% will be unencrypted and, it is transferred as it is. It requires more bandwidth. Here the unencrypted data is compressed by a Quadrature Mirror Filters and Lossless compression techniques. Only the intended receiver can decrypt and decompress the message and other unauthorized nodes have no knowledge about the transmitted messages on the whole. Here 50% of data is encrypted and remaining 50% data is compressed. M. Abomhara, Omar Zakaria, Othman O. Khalifa, A.A Zaidan, B.B Zaidan[4] presents a new system of video encryption. The proposed system aim to gain a deep understanding of video data security on multimedia technologies, to investigate how encryption and decryption could be implemented for real time video applications, and to enhance the selective encryption for H.264/AVC. The system includes two main functions; first is the encoding/encryption of video stream, through the execution of two processes (the input sequences of video is first compressed by the H.264/AVC encoder, and the encoded bit stream (I-frame) is partially encrypted using AES block cipher) and the second function is the decryption/decoding of the encrypted video through two process (specify the encrypted I- frame stream, decryption of the I-frame, and decoding with H.264/AVC decoder). Yajun Wang, Mian Cai, Feng Tang[5] presents the technology of H.264-based video data security becomes increasingly important. A new selective encryption scheme based on H.264, it combines the AES OFB mode with the sign encryption algorithm, and encrypts DCs and parts of ACs respectively. This method not only keeps advantages of former selective encryption algorithms in computational complexity and error-propagation prevention, but also efficiently make up for the deficiency in security and compression performance. Bing Qi, Fangyang Shen[6] analyzed different radio propagation models implemented in Ns-2 simulator in detail and applied two-ray ground propagation and rician

fading model to evaluate the effectiveness of current routing metrics, such as Shortest Path metric(HOP), Expected Transmission Count(ETX), Expected Transmission Time (ETT) and Interference aware Expected Transmission Time metric(iETT). Stuart Kurkowski, Tracy Camp, Neil Mushell, Michael Colagrosso[7] presents a new visualization and analysis tool for use with NS-2 wireless simulations. The Network Simulator 2 (NS-2) is a popular and powerful simulation environment, and the number of NS-2 users has increased greatly in recent years. Although it was originally designed for wired networks, NS-2 has been extended to work with wireless networks, including wireless LANs, mobile ad hoc networks (MANETs), and sensor networks; however, the Network Animator (NAM) for NS-2 has not been extended for wireless visualization.

III. SELECTIVE ENCRYPTION ALGORITHMS

In this section, we will present the design of a probabilistic selective encryption algorithm step by step, which not only reflects the idea of probabilistic encryption, but also uses both of symmetric key and asymmetric key. Specifically, algorithm aims to involve sufficient uncertainty into the encryption process, while providing satisfactory security protection to communicating nodes. The links between wireless nodes are always bidirectional and every wireless node has enough computational power to finish these operations. There are three methods for Selective Encryption Algorithms:

A. Secure Key Distribution (Full Encryption)

Nevertheless, due to the constrained computational power of wireless devices, it is not realistic to encrypt all information always using the public key algorithms (PKI). Hence, all official data communication between two nodes will be encrypted through symmetric key, and in the meantime, these symmetric keys will be distributed by public key encryption algorithm.

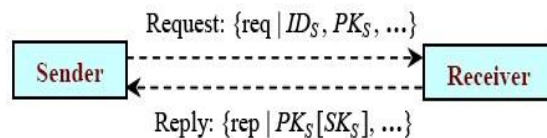


Fig. 1: The schematic diagram of key distribution

In a network, when a node wants to communicate with another node, a secret key (symmetric key) will be generated for their communication. Let us denote the initiating node as S and receiving node as R. If an initiating node S moves into the neighbourhood of node R, it will inform the node R of its public key for the authentication between them. The receiving node R then assigns a secret key to the initiating node S for the purpose of encryption/decryption. In order to distribute the secret key securely, R will encrypt this secret key using the public key of node S before sending it. Furthermore, R generates different secret keys for different initiating nodes. Thus, each sender has a unique secret key for

communicating with the receiver and all information is encrypted using the corresponding secret key. The figure.1 illustrates the procedure of secret key distribution between a pair of nodes. The message's sender composes a communicating request message req which contains not only its identifier IDs, but also its public key PKs, for the purpose of their later mutual authentication. Once the receiver gets such a communication request, a secret key (symmetric key) SKs will be generated by the receiver and encrypted using the public key PKs of the requester, which is included in the communicating request message. Later, the receiver composes a communicating reply rep message and replies it to the communicating sender, in order to indicate that their communication has been successfully established. After the sender obtains the response from the receiver, it will use its corresponding private key PRs to decrypt the secret key SKs issued from the receiver.

B. A Probabilistic Selective Encryption Algorithm

Here, a probabilistically selective encryption algorithm, which uses the advantages of the probabilistic methodology, aiming to obtain sufficient uncertainty. During the process of sending messages, the sender will randomly generate a value to indicate the encryption percentage, which represents how many messages will be encrypted among the transmitted messages. Then, the sender uses a probabilistic function to choose the already deterministic amount of messages to encrypt them. Moreover, this selective algorithm is comprised of the following three phases:

1) The sender of communicating parties S will first apply a random generator RNG to randomly obtain an encryption ratio er , which determines the percentages of encrypted messages among all messages. Here, in order to ensure that enough data are able to be encrypted so as to provide sufficient security protection, the generated encryption ratio should be higher than a pre-determined value of security requirement SR (SR means that data communication is secure if there are SR or more percents of messages are encrypted).

$$S \xrightarrow{RNG} er \mid \{er \geq SR\} \quad (1)$$

2) Then the sender S will employ a probabilistic function PF to generate an encryption probability p_i to determine if one message M_i will be encrypted or not.

$$S \xrightarrow{PF(M_i)} p_i \quad (2)$$

$$p_i = \frac{\text{Counts Encrypted Messages}}{i - 1}$$

3) Eventually, the sender selects the messages to encrypt based on the above pre-determined encryption ratio er . For example, once S finds out that the encryption

probability p_i is less than or equal to the encryption ratio er , it will encrypt the message M_i using its secret key SK . otherwise, this message will not be encrypted accordingly.

$$\begin{cases} S \rightarrow SK[M_i] & p_i \leq er \\ S \rightarrow M_i & p_i > er \end{cases} \quad (3)$$

Thus, the probabilistic selective encryption algorithm integrates both the probabilistic method and stochastic strategy, in order to increase the uncertainty in the process of message selection. The more uncertain the encryption algorithm is, the secure data communication is based on the assumption that sufficient data is encrypted to provide reliable security.

IV. RESULT AND DISCUSSION

Source Side

- **New User - Registration**



Fig 2. Registration

Figure 2 shows the new user registration. In this the user has to register the details by giving their name, gender, date of birth, contact number, email id, address for communication, and username to access and password to login into the system. Once all the details have been filled, the user has been allowed for further access of the system.

Audio and Video Upload

- **Upload Audio (with Customized Questions +Answers)**




Figure 3. Audio Upload

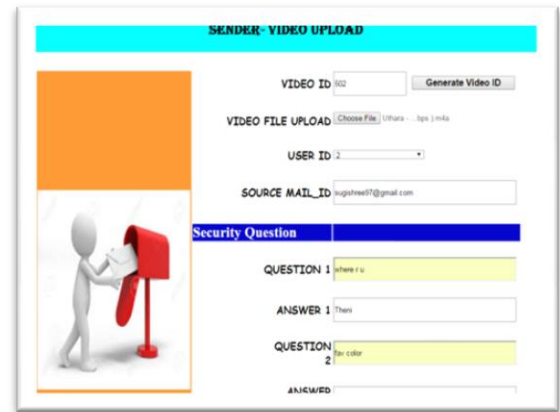


Figure 4. Video Upload

In Figure 3 the user has to enter into their login for each audio file uploading. The user has been allowed to browse the audio to upload, once the audio file has been chosen, then the user has to give 2 security questions with answers (where the questions and answers has been well know to the receiver already) and the receiver mail id.

- **Conversion - Convert Audio into Binary Format (Fix Security Constraints)**
 - After entering the primary details, then the server stores the user constraint details and using stream reader function, the uploaded audio file is converted to binary format with the help of byte allocation. The audio file extension has been stored separately. These details are organized together and finally updated into the database.
- **Upload Video (with Customized Questions +Answers)**
 - The Figure 4 shows the video file upload. The user has to enter into their login for each video file uploading. The user has been allowed to browse the video to upload, once the video file has been chosen, then the user has to give 2 security questions with answers (where the questions and answers has been well know to the receiver already) and the receiver mail id.
- **Conversion - Convert Video into Binary Format (Fix Security Constraints)**
 - After entering the primary details, then the server stores the user constraint details and using stream reader function, the uploaded video file is converted to binary format with the help of byte allocation. The video file extension has been stored separately. These details are organized together and finally updated into the database.

Receiver Side

- **Security Credential Login**



Fig 5. Security Credential login

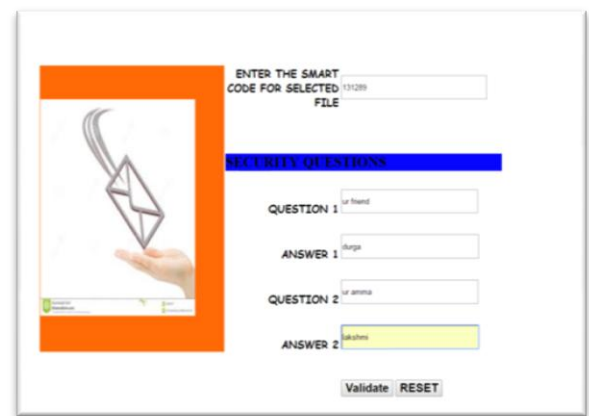


Fig 6. Download the file

Figure 5 & 6 are used to download the file in secured manner. Once the user entered the security pin received to their email id from the server, the server generates a One Time Password to the receiver email id again. The receiver has to get back the One Time Password and after validation, the receiver can get the audio and video for downloading.

Audio

- **Download Audio as binary format**

- The selected audio file has been converted from binary format to original file with the help of stream reader function.

- **Release Security constraints**

- Once the downloading completed, the user has to answer for the security questions fixed by the sender. Once the given answers has been validated and checked. Then the binary file format has been moved to final process.

- **Audio stream into original file from binary format**

- In the final process, the downloaded binary file has been converted into original file with the help of memory stream function.

Video

- **Download Video as binary format**

- The selected video file has been converted from binary format to original file with the help of stream reader function.

- **Release Security constraints**

- Once the downloading completed, the user has to answer for the security questions fixed by the sender. Once the given answers has been validated and checked. Then the binary file format has been moved to final process.

- **Video stream into original file from binary format**
 - In the final process, the downloaded binary file has been converted into original file with the help of memory stream function.

V. CONCLUSION

The proposed framework for the most part emerges keeping in mind the end goal to encode the critical sound and video substance of the organization. Since the organization is completely in light of media working procedure, their primary database comprises of sound and video speaking to the pioneers' meeting, squeeze meeting document. Yet at the same time now, there is no legitimate security requirements are taken after to shield these documents protecting from the working staff side or from different interlopers side. The current framework is altogether comprehended and the proposed framework is planned with encryption of sound and video utilizing SMTP server bolster and additionally remote SMS bolster. The primary center support of the venture is the web situated concentrated web server, where the scrambled document are permitted to store in the incorporated database and a similar record is unscrambled in the goal side later. A few modules are composed so as to scramble the sound and video from source side and download the records from the goal side.

VII. REFERENCES

- [1] Yonglin Ren, Azzedine Boukerche ,Lynda Mokdad, "Performance Analysis of a Selective Encryption Algorithm for Wireless Ad hoc Networks", IEEE WCNC 2011-Network.
- [2] K.VetriVel, Dr.C.Senthamarai, "A Study of Comparison of various Block Ciphers in Symmetric Key Encryption Algorithm", International Journal of Computer Information Systems, Vol. 1, No. 5, 2010.
- [3] S.Kala, "Enhanced Selective Encryption Algorithm For Wireless Ad Hoc Networks", International Journal of Computing Technology and Information Security Vol.1, No.2, pp.48-51, December, 2011.
- [4] M. Abomhara, Omar Zakaria, Othman O. Khalifa, A.A Zaidan, B.B Zaidan, "Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard", International Journal of Computer Theory and Engineering, Vol. 2, No. 2 April, 2010.
- [5] Yajun Wang, Mian Cai, Feng Tang, "Design of a New Selective Video Encryption Scheme Based on H.264", IEEE International Conference on Computational Intelligence and Security 2007.
- [6] Bing Qi, Fangyang Shen, " Propagation Models for Multi-hop Wireless Networks in Ns-2 Simulator ", 2011 Eighth IEEE International Conference on Information Technology: New Generations. <http://www.isi.edu/nsnam/ns/>
- [7] Alex Homer, "Professional ASP.NET 1.1", 2004 Edition, Wrox Publications