Selective Encryption Algorithm for Text Messages in Wireless Ad-hoc Networks

Ganesh Patil, Pankaj Gaikwad and Nitin Mane

August 16, 2018

Selective Encryption Algorithm for Text Messages in Wireless Ad-hoc Networks

Mr. Ganesh G. Patil[1], Mr. Pankaj G. Gaikwad[2], Mr. Nitin S. Mane[3]
[1,2,3] Assistant Professor, Department of Computer Science and Engineering, SVERI's College of Engineering, Pandharpur, Solapur, Maharashtra, India

Abstract. Security is one of the most challenging aspects in internet and network applications domain. In this domain the major issue is to provide security to the data which is travelling on the communication link. Data encryption is the primary solution to protect the data confidentiality and integrity between any pair of node. Using symmetric key algorithms fast and efficient cryptosystems can be built as they have significant applications. For a wireless ad hoc network with constraint computational resources, the cryptosystem based on symmetric key algorithms is extremely suitable for such an agile and dynamic environment along with other security strategies. The selective encryption algorithms are preferred by wireless networks because they are energy efficient for wireless devices..Probabilistic methodology and proposed algorithm enable a sender to include proper uncertainty in the process of message encryption so that only entrusted receiver can decrypt the cipher text and other unauthorized nodes have no knowledge of the transmitted messages on the whole.

Keyword: Wireless security, Selective cryptographic algorithm.

I. INTRODUCTION

A fundamental method of data protection in the area of information and network security is cryptography. It has been widely accepted as a traditional platform of data protection for decades. The application of cryptography is particularly prevalent today as it is exhaustively used today in homeland security, military communications, financial transactions and so on [3]. The method of data encryption and decryption are divided into symmetric encryption and asymmetric encryption [4]. Through the data encryption and decryption the protection of data confidentiality and integrity are achieved. However, a wireless ad hoc network based on the features of wireless devices has special security and efficiency requirements for conventional cryptographic algorithms. At present, there are a variety of methodologies to provide protection for data confidentiality and integrity. As one of the mainstream cryptographic methods, symmetric key algorithms are widely used due to their efficiency and capability of data protection. Typically, a symmetric key cryptosystem employs a secret key for both encryption and decryption. This secret key is the only shared by sender and receiver and kept confidential to other irrelevant entities. The protection of secrecy of the message depends on the confidentiality and secure distribution of the secret key. The selective encryption algorithms are used just to encrypt certain portions of the messages with less overhead consumption but simultaneously sufficient messages are encrypted to provide reliable safety to secure the confidentiality of the transmitted message. There is no need to encrypt all messages in selective encryption algorithm while the entire data transmission can be viewed to be secure on the whole. Selective encryption algorithm improves the scalability of data transmission and reduces the processing time. The primary application of selective encryption algorithms is found in the realms of energy-aware environments or large scale data transmission like multimedia communications, mobile ad-hoc networks and wireless sensor networks etc [5].

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 [3] 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[4] 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[5] 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[7] 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[10] 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[12] analyzed different radio propagation models implemented in NS-2 simulator in detail and applied two-ray ground propagation and ricean 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[13] 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.

III. SELECTIVE ENCRYPTION ALGORITHMS

The selective encryption algorithms are to just encrypt certain portions of the messages. They can reduce the overhead spent on data encryption/decryption, and improve the efficiency of the network. Algorithm aims to involve sufficient uncertainty into the encryption process, while providing satisfactory security protection to communicating nodes. The design of a selective encryption algorithm with less processing time but with relatively high security level is extremely significant.

The existing methods for selective encryption algorithms are as follows:

A. A Toss-a-Coin Selective Encryption Algorithm

All transmitted messages are divided into two groups: the odd number messages and the even number messages. For instance, messages *M1, M3, M5 ... M(2n-1)* represent the odd number messages; messages *M2, M4, M6, ... M(2n)* represent the even number messages. When the sender needs to decide which group should be encrypted, it makes use of a toss-a-coin method to determine whether the even number messages or odd number messages are to be encrypted. Hence, the value of encryption ratio here is tentatively determined to be 0.5, which means that approximately 50% of the communicated data will be encrypted.

B. A Probabilistic Selective Encryption Algorithm

A Probabilistically selective encryption algorithm 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, in order to increase the uncertainty in the process of message selection.

The probabilistic selective encryption algorithm is comprised of the following three steps:

i) The sender of communicating parties *S* will first apply a random number generator *RNG* to randomly obtain an encryption ratio *er*, which determines the percentage of encrypted messages among all messages. Here, in order to ensure that enough data is 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 is *SR* or more percentage of messages are encrypted).

$$\boldsymbol{S} \xrightarrow{\boldsymbol{RNG}} \boldsymbol{er} \mid \{\boldsymbol{er} \geq \boldsymbol{SR}\} \qquad (\mathbf{1})$$

ii) Then the sender *S* will employ a probabilistic function *PF* to generate an encryption probability *pi* to determine if one message *Mi* will be encrypted or not.

$$\boldsymbol{S} \xrightarrow{\boldsymbol{PF(M_i)}} \mathbf{p}_i \qquad (\mathbf{2})$$

$$\boldsymbol{p_i} = \frac{\textbf{Counts Encrypted Messages}}{\boldsymbol{i}}$$

iii) 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 *pi* is less than or equal to the encryption ratio *er*, it will encrypt the message *Mi* using its secret key *SK*, otherwise this message will not be encrypted accordingly.

$$\begin{cases} \boldsymbol{S} \rightarrow \ \mathbf{SK}[\mathbf{M}_i] & \mathbf{p}_i \leq \boldsymbol{er} \\ \mathbf{S} \ \rightarrow \ \mathbf{M}_i & \mathbf{p}_i > \boldsymbol{er} \end{cases} \qquad (\mathbf{3})$$

IV. PROPOSED SELECTIVE ENCRYPTION ALGORITHM

Our proposed selective encryption algorithm is based on message entropy. Using the message entropy the uncertainty in the process of message selection is increased. Following is the proposed algorithm for selective encryption,

where,
$\mathrm{E}(m)$= Entropy of message
$\mathrm{Thr}(m)$= Threshold value of message
N0= Number of 0's bits
N1= Number of 1's bits
N= Total number of bits

```
Step 0: Take messages one by one

Step 1: Calculate E(m) = Entropy of message
            1.1: Convert message to ASCII code.
            1.2: Convert the ASCII code to binary format.
            1.3: Find the number of 0's say N0 and the number of 1's say N1
            1.4: Calculate N0=N0/N, N1=N1/N.
            1.5: The entropy of the message will be,
                $E(m) = -(N0*\log_2(N0)+N1*\log_2(N1))$

Step 2:  This is the first message then,
                $Thr(m) = E(m)$
        If previously encryption percentage is less than equal to 50% then,
            $Thr(m)=Thr(m)-E(m)*1/100$

        Else If previously encryption percentage is more than 50% then,
            $Thr(m)=Thr(m)+E(m)*1/100$

Step 3: If  $E(m) >= Thr(m)$ then Encrypt the message
        else do not encrypt the message

Step 4: Calculate encryption percentage

Step 5: Take the next message till all messages to be sent are over.
```

In selective encryption, if messages that have all 1s or 0s are encrypted without encrypting messages that have higher entropy in that case the security reduces. The proposed method will selectively encrypt messages which have higher entropy and pass messages which have lower entropy without encryption. Passing messages having lower entropy without encryption increases security of transmission and reduce the power for wireless ad-hoc networks. The proposed method provide more security as compared to toss-a-coin and probabilistic methods.

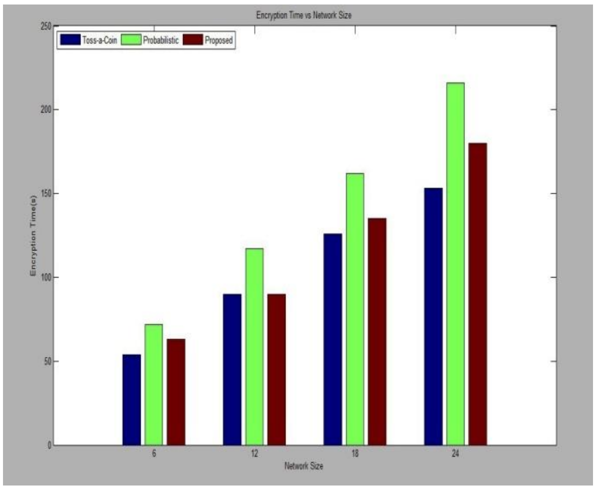

Figure 1: Encryption Time vs. Network Size

V. RESULTS

In this section, in order to study proposed selective encryption scheme and observe its characteristics, observation are noted on extensive set of experiments within a wireless environment based on Network Simulator-2(NS-2) [13]. In the setup of our experimental environment, the transmission range is set to 250*m* without fading effect. During the process of communications, the traffic is generated over UDP. The tclDES algorithm used for encryption/decryption of message blocks(the block size is 64bits). The DES algorithm is employed for communication between a pair of nodes and the secret keys have a length of 64 bits

Utilize the above two approaches as comparable models to our proposed selective encryption approaches. The first approach is the toss-a-coin approach and the second approach is the probabilistic approach. By comparing the performance and efficiency of the above approaches, above Figures 1 and 2 show the illustrated the comparison of encryption percentages and time based on three approaches. As compared to probabilistic method the toss-a-coin and our proposed method have an obvious lower encryption time percentages. In Figure 1, the time spent on encryption/decryption is compared to show that probabilistic method takes a longer time than toss-a-coin and proposed encryption methods. Table 1 shows the comparison of selective encryption algorithms.

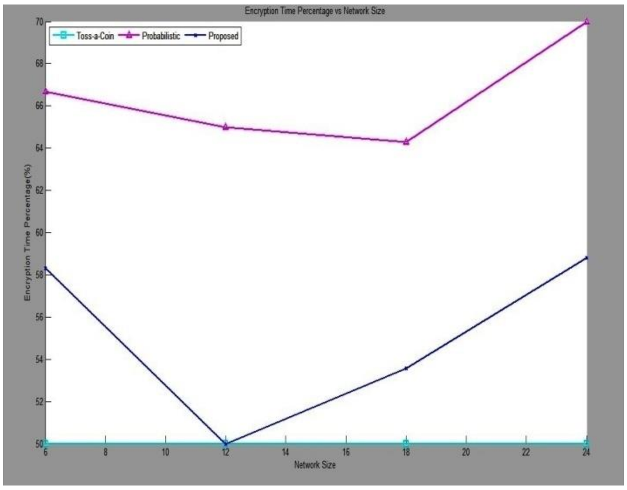

Figure 2: Encryption Percentage vs. Network Size

Table 1. Comparison of Selective Encryption Algorithms

Algorithms	Toss-A-Coin	Probabilistic	Proposed Selective Encryption
Characteristics			
1) Encryption Time Percentage	Approximate 50%	60% or More than 60%	50% to 60%
2) Encryption Time	Less	More	Medium
3) Saving Time	Approximate 50%	Less than 50%	40% to 50%
4) Security	Less Secure	Secure	More Secure

VI. CONCLUSION

Selective encryption algorithms is one of the most promising solutions to reduce the cost of data protection, reduce the computation time and power in wireless and mobile networks. They can reduce the overhead spent on data encryption/decryption and improve the efficiency of the network. As compared to a toss-a-coin and probability methods the proposed selective encryption algorithm is expected to give better results in terms of time and security.

VII. FUTURE WORK

The selective encryption algorithms can also be used for encryption of images and video.

VIII. REFERENCES

[1] Ahmed I. Sallam, El-Sayed M. EL-Rabaie & Osama S. Faragallah “HEVC Selective Encryption Using RC6 Block Cipher Technique”, IEEE 2017.

[2] Xiaoqiang Di,Yingzheng Wang, Jinqing Li*, Ligang Cong, Hui Qi and Yuxin Zhang “An Optimized Video Selective Encryption Algorithm”, CISP-BMEI 2017.

[3] Yonglin Ren, Azzedine Boukerche ,Lynda Mokdad, "Performance Analysis of a Selective Encryption Algorithm for Wireless Ad hoc Networks", IEEE WCNC 2011-Network.

[4] 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.

[5] 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.

[6] Priyanka Agrawal, Manisha Rajpoot, "Partial Encryption algorithm for Secure Transmission of Multimedia Messages", International Journal of Computer Science and Technology(IJCST), Vol.3, Issue 1, Jan-March 2012.

[7] 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.

[8] Bismita Gadanayak, Chittaranjan Pradhan, "Selective Encryption of MP3 Compression", International Conference on Information Systems and Technology (ICIST) 2011, Proceedings published by International Journal of Computer Applications® (IJCA)2011.

[9] Feng Bao, Robert H. Deng, "Light-Weight Encryption Schemes for Multimedia Data and High-Speed Networks", IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2007 proceedings.

[10] 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.

[11] Ayoub Massoudi , Fr´ed´eric Lef`ebvre, Christophe De Vleeschouwer , Franc¸ois-Olivier Devaux, " Secure and low cost selective encryption for JPEG2000 ", Tenth IEEE International Symposium on Multimedia 2008.

[12] Bing Qi, Fangyang Shen,"Propagation Models for Multi-hop Wireless Networks in Ns-2 Simulator ", 2011 Eighth IEEE International Conference on Information Technology.

[13] Stuart Kurkowski, Tracy Camp, Neil Mushell, Michael Colagrosso, " A Visualization and Analysis Tool for NS-2 Wireless Simulations: iNSpect∗ ", Proceedings of the 13th IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS’05).

[14] NS-2, available at http://www.isi.edu/nsnam/ns/, Information Sciences Institute, University of Southern California.