IJCAT - International Journal of Computing and Technology, Volume 1, Issue 10, November 2014
ISSN : 2348 - 6090
www.IJCAT.org

Novel Encryption Algorithm for Data Protection Mechanism in Wireless Ad- hoc Network

[1] Najim Sheikh, [2] Sagar Tete, [3] Ashish Mohod, [4] Rashmi Ganar

[1,2,3,4] M.Tech Scholar
[1] RGPV Bhopal, [2, 3, 4] RTMNU Nagpur

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 an agile and dynamic environment, along with other security strategies. We introduce the concept of selective encryption into the design of data protection mechanisms. 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 cipher text and other unauthorized nodes have no knowledge of the transmitted messages on the whole.

Keywords **- wireless security, Selective Cryptographic algorithm.**

1. Introduction

A fundamental method of data protection in the area of information and network security is cryptography, which has been widely accepted as a traditional platform of data protection for decades. The application of cryptography is particularly prevalent in nowadays information technology era and typical examples include the use of cryptographic techniques to homeland security, military communications, financial transactions, and so on. The method of data encryption and decryption are divided into symmetric encryption and asymmetric encryption. Encryption is the process of encoding plaintext into cipher text and decryption is the reverse process. Through the data encryption and decryption, the protection of data confidentiality and integrity are achieved. However, based on the features of wireless devices, a wireless ad hoc network has special security and efficiency requirements for conventional cryptographic algorithms. Selective encryption algorithms are primarily applied in the realms of energy-aware environments or large scale data transmission such as, multimedia communications, mobile ad hoc networks (MANETs), and wireless sensor. networks (WSNs) 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.

2. 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.

Youngling 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 cipher text 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] implements 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 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, Fang yang Sheen[6] analyzed different radio propagation models implemented in Ns-2 simulator in detail and applied two-ray ground propagation and rice an 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 Mush ell, 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.

3. 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:

3.1 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.

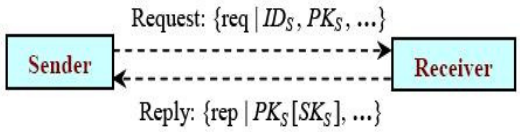

Fig. 1: The schematic diagram of key distribution

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 neighborhood 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 red 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.

3.2 A Toss-A-Coin Selective Encryption Algorithm

In order to provide sufficient security to data encryption, we choose a relatively high proportion as encryption ratio. Since the toss-a coin algorithm is a basic approach, little uncertainty is involved. For all transmitted messages, we divide them to two groups: the odd number messages and the even number messages. For instance, messages M1, M3, M5, and M (2n-1) represent the odd number messages; messages M2, M4, M6, and 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 encrypted. As an example, in which the even number messages are encrypted. After the method of toss-a-coin is applied, the sender makes the decision that only the even number messages M2, M4, M (2n) are encrypted. Thus, half of the whole messages are chosen to be encrypted and this approach shows a basic selective encryption algorithm with a semi-determined encryption pattern. The more data are encrypted, the more secure the communication is, but the more overhead is spent. Hence, the value of encryption ratio here is tentatively determined to be 0.5, which means that 50 percents of the communicated data will be encrypted.

3.3 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 *err*, 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).

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

2) 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.

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

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

3) Eventually, the sender selects the messages to encrypt based on the above pre-determined encryption ratio *err*. For example, once *S* finds out that the encryption probability *pi* is less than or equal to the encryption ratio *err*, it will encrypt the message *Mi* using its secret key *SK*. otherwise, this message will not be encrypted accordingly.

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

(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.

3.4 Proposed Selective Encryption Algorithm

Following is the proposed algorithm for selective encryption,

Where,

E = Entropy of message
Thr = 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 = 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 =-(N0*$\log_2$ (0) + N1*$\log_2$ (1))

Step 2: If this is the first message then,

Thr = E

Else If previously encryption percentage is less than equal to 50% then
Thr =Thr -Thr *1/10

Else If previously encryption percentage is more than 50% then
Thr =Thr +Thr *1/10

Step 3: If E > = Thr 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.

The entropy of a message gives us a measure of quantity of information contained in the message. For example a message containing all bits 1 does not have much information and same is the case with message containing all 0's. In selective encryption if we encrypt messages that have all 1's or 0's without encrypting messages that have higher entropy then security is reduced. The proposed method will selectively encrypt messages having higher entropy and pass messages having low entropy without encryption. Passing messages having lower entropy without encryption increases security of transmission when compared with normal selective encryption. This is so because when the transmission is intercepted; only that part of the transmission is accessible which has lower entropy and other higher entropy parts are encrypted.

4. Performance Evaluation

We propose to do a comparative study of three previous algorithms with our proposed selective encryption algorithm. Methods have used DES as the encryption cipher. The platform to used NS-2.

5. Conclusion

Selective encryption is one of the most promising solutions to reduce the cost of data protection in wireless and mobile networks. In this paper, we have presented a novel solution for selective encryption to achieve data protection effectively while with reasonably costs. They can reduce the overhead spent on data encryption/decryption, and improve the efficiency of the network. The factor of encryption probability involves the uncertainty to data encryption. We evaluate the performance of our approach based on an extensive set of simulation experiments.

6. Future Work

As compare to full encryption, a toss-a-coin & probability the proposed Selective Encryption algorithm will give better result in concern of time and security.

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] Stuart Kurkowski, Tracy Camp, Neil Mushell, Michael.