Increase the Security Level for Real-Time Application Using New Key Management Solution

Obaida Mohammad Awad Al-Hazaimeh

**Department of Information Technology, AL-BALQA Applied University/
AL-Huson College, Irbid, Al-Huson, 50, Jordan**

Abstract

A real-time application Voice over Internet Protocol (VoIP) is the technology that enables data packets transmission over internet protocol (IP). Security is of concern whenever open networks are to be used. In general, the real-time applications suffer from packet latency and loss due to the nature of IP network. Cryptographic systems may be used to achieve the security goals, but their impact on the Quality of Services (QoS) should be minimized. Most of the known encryption algorithms are computationally expensive resulting in a significant amount of time added to packet delay. A real-time application Voice over IP (VoIP) is usually used by public users resulting in a key exchange problem and a trusted intermediate authority normally takes this responsibility. In this paper, the security goals were enhanced via a proposed cryptographic system to maintain the security on VoIP. The proposed solution consists of a simple, but strong encryption/decryption algorithm as well as an embedded method to exchange the keys between the users.

Keywords: *VoIP, QoS, DIEHARD Test Suite, NIST Test Suite.*

1. Introduction

Real-time application Voice over Internet Protocol (VoIP) refers to the technology that transfers voice data over Internet Protocol (IP) networks. It conveys real-time audio information such as human voice, in a manner that emulates traditional telephone service [1]. The VoIP technology relies on the fundamental internet architecture principle which allows any computer with an IP address to send any kind of data to any other computer with an IP address. In general, the VoIP technology only requires an Internet connection and a program on the endpoint computer capable of encoding and transmitting speech [2, 3].

Among the advantages of the VoIP technology over the traditional Public Switch Telephone Network (PSTN) are lower cost, integration with other media services, portability, and bandwidth utilization. For instance, the network and service providers consider the VoIP technology as a mean of reducing the cost of offering existing voice-based services and new multimedia services. In addition, the VoIP infrastructure is viewed as an economical base in building new revenue-generating services. Most importantly, the deployment of VoIP technology is becoming widespread and forming part of a shared competitive landscape [4].

Despite of all the benefits, the VoIP technology is facing some challenges such as latency, packet loss, and security. Therefore, appropriate strategies or techniques are needed to carefully manage these challenges to ensure the quality service of VoIP technology [2]. An example of VoIP security challenge is the threat of intruders and hackers over the networks. The obstructions or attacks by these culprits have become a great concern since there are various sniffing tools that can be used to compromise a VoIP conversation. In handling a security problem, cryptography plays a major role in helping to maintain data secrecy [3].

Cryptography is the science of using mathematics to encrypt and decrypt data. It provides a way to store sensitive information or transmit it across insecure networks (i.e. the Internet) so that it cannot be read by anyone except the intended recipient [5]. This technique is widely used to protect data that traverses over open networks. However, there is a drawback in this technique where most of the encryption algorithms are built to handle text data. These algorithms will consume a significant amount of time because it involves extensive computation. Therefore, these algorithms are not suitable for VoIP since the technology has already suffered latency [6].

2. VoIP Security

The VoIP security performance is measured mainly according to the following factors: the security level, encryption delay, message delay, and processing power. The complexity of the security algorithm seems to have an impact on these measurement factors. For any real-time applications without compromising the accuracy, the delay can cause significant voice degradation and interfere with call establishment. Since the delay is not suitable for real-time VoIP applications, it should be minimized [3, 7].

The current data encryption and decryption techniques that are used with VoIP usually cause unnecessary delay [8, 9]. Even though there are various data encryption and decryption techniques being applied to the VoIP, the delay overload problem still exists during the encryption and decryption processes [6, 10]. Therefore, this paper

proposes a new encryption and decryption technique that will reduce the overhead delay to a voice packet in the VoIP applications. In addition, the new encryption and decryption technique will secure the VoIP packets that would avoid a significant overhead delay.

3. Proposed Technique

Available data within a network environment are generally regarded as valuable asset. In such case, it is believed that such data should be handled in a secured manner in terms of storage and transmission to avoid undue access by unauthorized person. The most applicable security concept in this regard is called cryptography as mentioned in the introduction which emphasizes the significance of creating and managing keys.

3.1 Encryption Algorithm

The cryptographic process usually involves encryption algorithms. These algorithms execute many iterations of substitutions and transformations on original data (known as plaintext), in order to complicate the process of identifying the data by a hacker or intruder [11].

The proposed encryption algorithm consists of the following processes as shown in Figure 1.

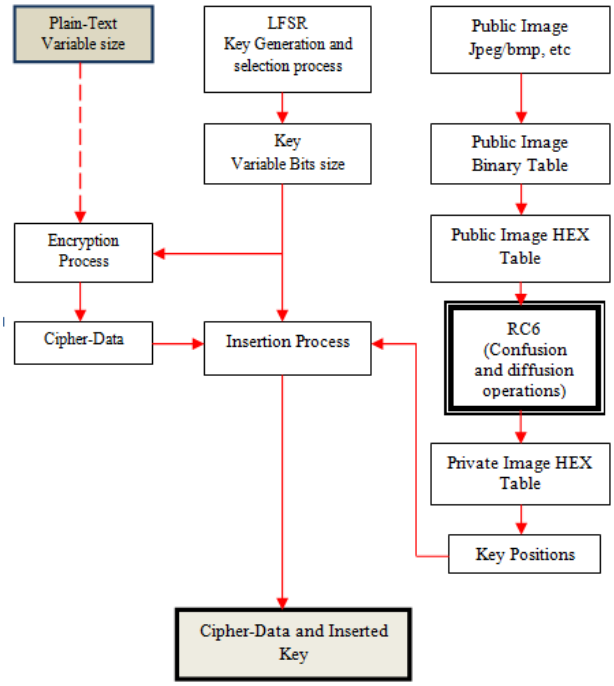

Figure 1: Encryption process architecture

A. Public Image: The image should be available at sender and receiver side. Since the image is not secret, it can be announced to the public.

B. Public Image Binary Table: Convert image to binary image table.

C. Public Image HEX Table: Convert public image binary table to HEX image table.

D. RC6: Confusion and diffusion operations set as an act of establishing possible complex relationship between the public image HEX Table and the private image HEX table in an attempt to frustrate the attackers. These operations done according to the secret value between sender and receiver.

E. Private Image HEX Table: is generated after performing RC6 algorithm.

F. Key Position: The key positions are generated from the values in the private image HEX table.

G. LFSR: Linear Feedback Shift Register- based pseudo-random number generator used to generate a random keys with a variable bits size.

H. Plain-Text: The data to be sent (source data).

I. Encryption Process: XOR process for the encryption of the voice data.

J. Insertion Process: Insert the key inside the Cipher-data according to the key position table.

3.2 Decryption Algorithm

Decryption is a process of reversing all that has happened in the encryption process. It involves converting the encrypted data back to its original form for the receiver's understanding. The same process is performed at the beginning of the encryption and decryption process (connection established) as described in the encryption part at the sender side to generate the same private table at the receiver side. As shown in Figure 2, the proposed decryption algorithm consists of the following processes:

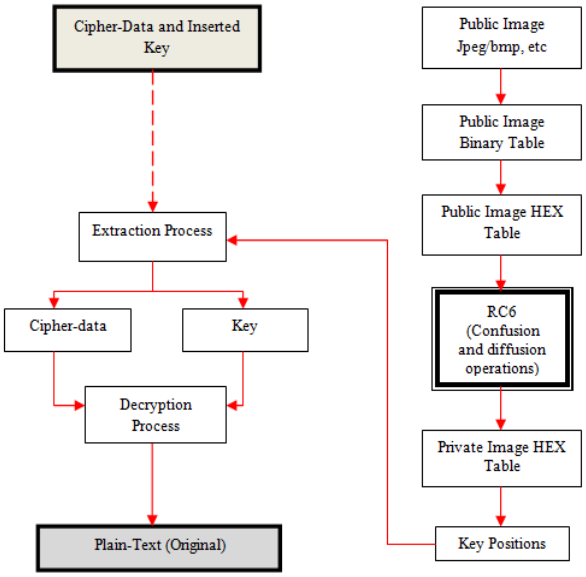

Figure 2: Decryption process architecture

1. Extraction process: Extract the key from the Cipher-data and inserted key according to the key position table since the key position table is made available at both the sender and receiver side.
2. Decryption process: involves a XOR operation between the encrypted data and the extracted key, and the end result of such operation is the plain text data (original text).

For smooth decryption process to be achieved, the accuracy of the decryption key cannot be negotiated. In short, the accuracy of this algorithm is a function of the key extraction process as to whether the extracted key is correct or not.

4. Security Analysis

This study aims to propose a new algorithm to improve VoIP performance by minimizing a significant amount of delay time to maintain the security on VoIP. The performance and security analysis of the proposed algorithm were conducted in two phases: key positions phase and cipher data with the inserted key phase.

4.1 Key positions phase

As mentioned earlier in section 3, a public table should be available at the sender and the receiver side. Since the public table is not secret, it can be announced to the public. After performing a regular confusion and diffusion operations using RC6 algorithm, a private table was generated, and the key positions were generated from the values in the private table.

The strength of the key positions depends on the relation between the public table and the private table. When there is no relation between the public and the private tables, the key positions are stronger. However, when a relation exists, this can help attackers to trace between the public and the private tables to re-generate the key positions. To examine the relation between the public table and the private table, correlation analysis was performed.

4.1.1 Correlation analysis

To analyze the correlations between the public and the private tables, the following equation is used to calculate the correlation coefficients in horizontal, vertical and diagonal directions [12, 13].

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \quad , r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}},$$

Where,

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad , D(x) = \frac{1}{N}\sum_{i=1}^{N}(xi - E(x))^2$$

E (x) is the estimation of the mathematical expectation *of x, D (x)* is the estimation of variance x and *cov (x, y)* is the estimation of covariance between *x* and *y*.

The strength of the relationship between the public and private tables is determined by a correlation coefficient, which ranges from -1 to +1. The closer the coefficient is to +1/-1, the stronger is the relationship. This means that the tables are related and are the same. In other words, if the correlation coefficient is equal to zero, then the public and the private tables are totally different. If the correlation coefficient is perfect correlation then the public table and the private table are same [14,15].

In correlation analysis, we randomly choose different values in the public table and private table. The correlation coefficients of the public and the private tables in vertical, horizontal, and diagonal directions were calculated and listed in Table1, and the corresponding distribution is shown in Figures 3-4.

Table1: Correlation coefficients in public and private tables

Direction	Public Table	Private Table
Horizontal	1.0000	0.0424
Vertical	1.0000	- 0.074
Diagonal	1.0000	- 0.0663

It is clear from Table1 that the correlation coefficients for the three dimensions in the private table are close to zero, while the coefficients for the three dimensions in the public table are 1.00. This indicates that the public and private tables are not correlated, as suggested by Tao Sang et al. [12].

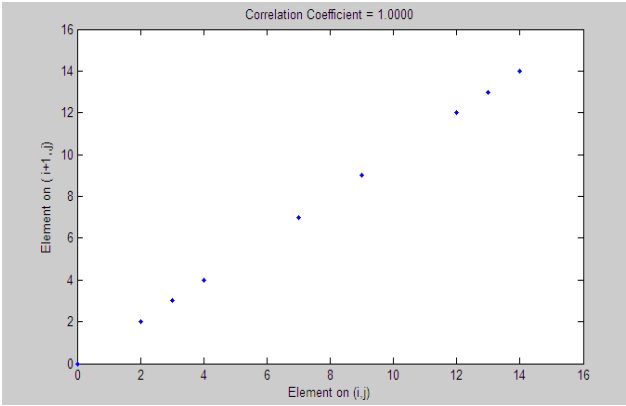

Figure 3: Correlation analysis of public table (Horizontal)

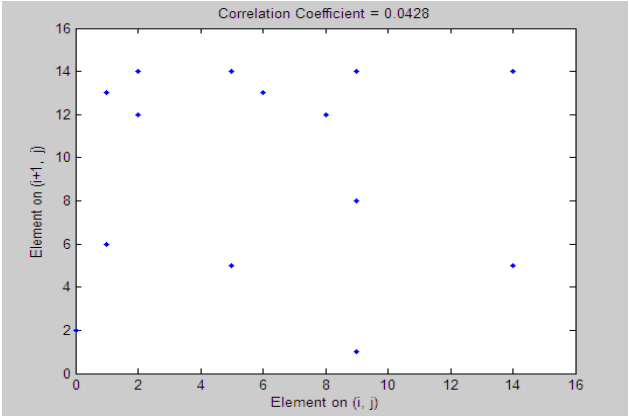

Figure 4: Correlation analysis of private table (Horizontal)

It is clear from the Figures 3-4, that the RC6 algorithm has covered all the public table characters and shown good performance.

4.2 Cipher-data with the inserted key phase

In terms of security analysis, we examined the strength of the cipher-data with the inserted key against cryptanalysis attacks and performed a different set of statistical tests known as DIEHARD, NIST test suite values and ENT test suite [16]. These tests are mainly designed to measure the randomness of a given sequence. These three tests were performed on file of 16MB cipher-data which is needed for these tests.

4.2.1 DIEHARD Test Suite

Diehard test suite is a group of statistical tests for measuring the quality of a set of random numbers [17-20], developed by Marsaglia and published in 1995 [16]. These tests consist of 18 core tests that produces a set of 215 p-value which should be uniform on [0,1).

DEHARD test is important because it seems to be the most powerful and difficult test suite to pass [21, 22]. The results presented in Table2 show that Cipher-date with the inserted key has successfully passed the Diehard tests suite. The p-value of each test shows that our proposed algorithm (Cipher-Data and inserted key) has passed all the tests within the success range of $0.01 < \text{p-value} < 0.99$, which means that the sequence is random with confidence level of 99% [21, 23- 25].

Table2: p-value and conclusion for diehard tests on cipher-data with the inserted key

	Test Name	*p*-value	Conclusion
1	Birthday Spacing Test	0.506655	Success
2	Overlapping 5-Permutation Test	0.342171	Success
3	Binary Rank Test for (31 x 31) Matrices	0.996311	Success
4	Binary Rank Test for (32 x 32) Matrices	0.351343	Success
5	Binary Rank Test for (6 x 8) Matrices	0.588188	Success
6	Bitstream Test	0.529975	Success
7	DNA Test	0.5860	Success
8	OPSO Test	0.4570	Success
9	OQSO Test	0.5427	Success
10	Count-The 1's Test on Stream of Bytes	0.430811	Success
11	Count-The-1's Test for Specific Bytes	0.516605	Success
12	Parking Lot Test	0.681327	Success
13	Minimum Distance Test	0.666815	Success
14	3Dspheres Test	0.344852	Success
15	Squeeze Test	0.697871	Success
16	Overlapping Sums Test	0.683819	Success
17	Run Test	0.694030	Success
18	Crap Test	0.07006	Success

4.2.2 NIST Tests Suite

The NIST test suite is a statistical package consisting of 15 tests that are developed to test the randomness of (arbitrarily long) binary sequences produced by either hardware or software based cryptographic random or pseudorandom number generators [23]. These tests focus on a variety of different types of non-randomness that could exist in a sequence. The results of the tests are called p-value, which means that their values are real, between 0 and 1 [26].

The results presented in Table3 show that Cipher-date with the inserted key has successfully passed the NIST tests suite. The p-value of each test shows that the proposed algorithm (Cipher-Data and inserted key) has passed the tests within the success range of 0.01 < p-value < 0.99, which means that the sequence is random with a confidence level of 99% [26].

Table3: p-value and conclusion for NIST tests on cipher-data with the key inserted

	Test Name	*p*-value	Conclusion
1	The Frequency Test	0.654467	Success
2	Frequency Test within a Block	0.517442	Success
3	The Runs Test	0.931952	Success
4	Tests for the Longest-Run-of-Ones in a Block	0.619722	Success
5	Binary Matrix Rank Test	0.078086	Success
6	Discrete Fourier Transform (Spectral) Test	0.078086	Success
7	Non-overlapping Template Matching Test	0.534146	Success
8	Overlapping Template Matching Test	0.364146	Success
9	Maurer's "Universal Statistical" Test	0.204076	Success
10	Linear Complexity Test	0.422034	Success
11	Serial Test	0.035174	Success
12	Approximate Entropy Test	0.378138	Success
13	Cumulative Sums Test	0.689019	Success
14	Random Excursions Test	0.496841	Success
15	Random Excursions Variant Test	0.425817	Success

4.2.3 Information entropy

Information entropy is a mathematical theory of data communication and storage founded in 1949 by Claude E. Shannon [28]. To calculate the entropy *H(s)* of a source, we have:

$$H(s) = \sum_{i=1}^{2N-1} P(s_i) \log_2 \frac{1}{P(s_i)}$$

Where, *P(Si)* represents the probability of *Si*. In general, the entropy value of the source is smaller than the ideal value. When these messages are encrypted, their entropy should ideally be 8 [27]. If the output of such a cipher-data with the inserted key with entropy value is less than 8, then there exists a predictability which threatens its security.

In this paper, we have calculated the information entropy according to the ENT test. ENT test is a collective term for three tests which are Entropy, Chi-square, and serial correlation coefficient (SCC) as shown in Table4. The result shows the entropy value H (s) for the proposed algorithm is 7.999988. The obtained value is very close to the theoretical value 8. This means that information leakage in the encryption process is negligible, and so the encryption system is secure upon the entropy attack.

Table4: ENT test suite

Test Name	Max Grade	Result
Entropy	Close to 8.0	7.999988
Chi-square	Close to 127.5	127.5080
SCC	Close to 0.0	0.000103

5. Conclusion

In this paper, new cryptographic encryption and decryption techniques are proposed to enhance/add the security of real-time application VoIP call. Based on the results, it can be concluded that the proposed technique is secure because it has satisfied the ENT, DIEHARD, and NIST tests. Thus, we expect that the proposed technique will be efficiently used in real-time application VoIP calls or considered as a good alternative to other technique because of the high level of security.

References

[1] M. Hil. and G. Zhang, "A Web Services Based Framework for Voice over IP", *Proceedings of the 30th Euromicro Conference*, vol. 10, pp. 258 – 264, 2004.

[2] S. Bellovin, M. Blaze, E. Brickell, C. Brooks, V. Cerf, W. Diffie, S. Landau, J. Peterson, and J. Treichler, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP", *Information Technology Association of America*, 2006. [Online]. Available at: http://www.cs.columbia.edu/~smb/papers/CALEAVOIPreport.pdf.

[3] C. Hett, N. Kuntze, and A. Schmidt, "Security and Non-Repudiation for Voice-over-IP Conversations," Diploma of Science dissertation, Fraunhofer-Institut for Sichere Informations Technologie, 2006.

[4] S. Ahuja and R. Ensor, "VoIP: What is it Good for?", *Association for Computing Machinery Queue (ACM Queue)*, vol. 2, pp. 55-58, 2004

[5] P. Zimmerman, "*An Introduction to Cryptography"*, Doubleday & Company, Inc., United State of America, USA, 1999.

[6] T. Walsh and D. Kuhn, "Challenges in Securing Voice Over IP", *IEEE Security and Privacy* , vol. 3, pp. 44-49, 2005.

[7] D. Greenstreet and S. Scoggins, "Building Residential VoIP Gateways", *A Tutorial Part Four: VoIP Security Implementation*, 2004, [Online]. Available at: http://www. analogzone . com/nett0913. pdf.

[8] K. Werbach, "Using VoIP to Compete", *Harvard Business Review*, vol. 83, pp. 140-147, 2005.

[9] M. Wali and M. Rehan, "Effective Coding and Performance Evaluation of the Rijndael Algorithm (AES)", *in the Proceedings of the Engineering Sciences and Technology Conference*, vol. 7, pp. 1-7, Karachi, 2005.

[10] S. Chang, "The Design of A Secure and Pervasive Multimodal Web System", *in the Proceedings of the 17th International Conference on Advanced Information Networking and Applications (AINA'05)*, vol. 2, pp. 683 – 688, Taiwan, 2005.

[11] X. Lai, J. Massey, and S. Murphy, "Markov Ciphers and Differential Cryptanalysis", *Advances in Cryptology-EUROCRYPT'91*, Springer-Verlag, vol. 547, pp. 17-38. 2000.

[12] S. Tao, W. Ruli, and Y. Yixun, "Clock-Controlled Chaotic Key-Stream Generators", *Institution of Engineering and Technology Electronics Letters*, vol. 34, pp. 1932-1934, 1998.

[13] A. Masoun, "Cryptography Primitives Based on Piecewise Nonlinear Chaotic Maps", Master of Science dissertation, Universiti Sains Malaysia (USM), Pineng, Malaysia, 2008.

[14] Ahmed, H. Kalash, and OSF, "Implementation of RC5 Block Cipher Algorithm for Image Cryptosystems", *International Journal of Information Technology*, vol. 3, pp. 245-250, 2008.

[15] W. Emm, "Impact of Multiencryption in Data Security", *International Journal of Computer Theory and Engineering*, vol. 1, pp. 567-571, 2009.

[16] G. Marsaglia, "The Marsaglia Random Number CDROM Including The Diehard Battery of Tests of Randomness", 1995, [Online]. Available at: http://www. stat.fsu.edu/pub/diehard.

[17] J. Gleeson, "Truly Random Number Generator Based on Turbulent Electroconvection", *Journal of Applied Physics Letters*, vol. 81, pp. 1949-1952, 2002.

[18] E. John and J. Rubio, *Unique Chips and System*: Technology & Engineering, CRC Press, NY, USA, 2007.

[19] S. Lee, H. Jeong, and Y. Lee, "Application-Adaptive Pseudo Random Number Generators and Binding Selector", *in the Proceedings of the 23rd International Technical Conferance on Circuits/Systems Computers and Communication (ITC-CSCC'08)*, vol. 27, pp. 1561-1564, 2008.

[20] M. Stipcevice, "The Diehard Battery of Stringent Statistical Randomness Tests", 2001, [Online]. Available at: http:// random.com.hr/products/random/manual/html/Diehard.htiml.

[21] B.-H. Kang, D.-H. Lee, and C.-P. Hong, "High-Performance Psedorandom Number Generator Using Two-Dimensional Cellular Automata," *in the Proceedings of the 4th IEEE International Symposium on Electronic Design, Test & Applications*, vol. 46, pp. 597-602, Hong Kong, 2008.

[22] M. Alani, "Testing Randomness in Ciphertext of Block-Ciphers Using DieHard Tests", *International Journal of Computer Science and Network Security*, vol. 10, pp. 53-57, 2010.

[23] M. Robshaw, "Stream ciphers", *RSA Labratories Technical Report TR-701*. Version 2 ,1995.

[24] R. Baldwin, "Preliminary Analysis of The BSAFE 3. x Pseudorandom Number Generators", *RSA Laboratories Bulletin* No. 8, 1998, [Online]. Available at: ftp://ftp.rsa.com/pub/pdfs/bulletn8.pdf.

[25] X. Zhang, K. Tang, and L. Shu, "A Chaotic Cipher Mmohocc and Its Randomness Evaluation", *in the Proceedings of the Sixth International Conference on Complex Systems: The New England Complex Systems Institute*, MA, Boston, 2006.

[26] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, and A. Heckert, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", *NIST special publication 800-22*, 2001, [Online]. Available at: http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22b.pdf .

[27] C. Shannon, "Communication Theory of Secrecy Systems", *Bell Systems Technical Journal, MD Computing*, vol. 15, pp. 57-64, 1998.
[28] A. Ephremides, "The Collected Papers of Claude E. Shannon", *Proceedings of IEEE*, vol. 84, pp. 1570-1571, 1996.

Author

Obaida Mohammad Awad Al-Hazaimeh received the B.S. degree in Computer Science from Applied Science University (ASU), Jordan in 2004, the MSc in Computer Science/ Distributed system from University Science Malaysia (USM), 2005, and PhD in Computer Science/ Network security (Cryptography) for Real-Time Application from University Utara Malaysia (UUM), 2010.