journal homepage: www.ojs.sabauni.net

Saba Journal Of Information Technology And Networking (SJITN)

All Rights Reserved© 2019 Saba Journal of Information Technology and Networking, Published by Saba University.

journal homepage: www.ojs.sabauni.net

Saba Journal Of Information Technology And Networking (SJITN)

EDITOR IN CHIEF
Ibrahim Ahmed Al-Baltah

ADVISORY BOARD

Dr. G. Radhamani, India
Dr. Nidhal K. El-Abbadi, Iraq
Dr. Emad Abu-Shanab, Jordan
Prof. Gerald Robert Midgley, UK
Dr. Tawfiq S. Barhoom, Palestine
Dr. Wesam Bhaya, Iraq
Dr. Ahmad M. Aznaveh, Iran
Dr. Mohamed M. Elammari, Libya
Dr. Hisham Abushama, Sudan
Dr. Ali Al-Dahoud, Jordan
Dr. Mohammad Ibraheem, Egypt
Dr. Ahlal H. Montaser, Libya
Dr. Safaa Ahmed Hussein, Egypt
Dr. Maha Ahmed Ibrahim, Egypt
Dr. Basem Mohamed Elomda, Egypt
Dr. Alaa El-din Mohamed Riad, Egypt
Dr. Rehab Fayez Sayed, Egypt
Dr. Iyad M. Al-Agha, Palestine
Dr. Enas Hamood, Iraq
Dr. Assad norry, Iraq
Dr. Amjad Farooq, Pakistan
Dr. Sanjeev Gangwar, India
Dr. Waleed Al-Sitt, Jordan
Dr. N.Sudha Bhuvaneswari, India
Dr. Ali . Al-Sharafi, Saudi Arabia
Dr. Essam Said Hanandeh, Jordan
Dr. Ramadan Elaiess, Libya
Dr. Izzeldin M. Osman, Sudan
Dr. Rasha Osaman, United Kingdom
Dr. Eiman Kanjo, Saudi Arabia
Dr. Huda Dardary, USA

All Rights Reserved© 2019 Saba Journal of Information Technology and Networking, Published by Saba University.

journal homepage: www.ojs.sabauni.net

Saba Journal Of Information Technology And Networking (SJITN)

Table of Contents

All Rights Reserved© 2019 Saba Journal of Information Technology and Networking, Published by Saba University.

journal homepage: www.ojs.sabauni.net

S.J.I.T.N Saba Journal of Information Technology and Networking

Article

A New Symmetric Key Encryption Scheme for Binary Images

Abdullah Jaafar[1]*, Abdul-Gabbar Tarish Al-Tamimi[2]

[1] Department of Computer Science, Faculty of Computers and IT, Tai University, Taiz, Yemen.

2 Department of Computer Science, Faculty of Applied Science, Taiz University, Taiz, Yemen.

Article info

Article history:

Accepted: Aug. 2019

Keywords:

Diffie-Hellman (DH) Key Exchange Scheme, Shadow Image, Boolean Operation, Binary Inner Product,, Non-Invertible Matrix Problem

Abstract

Generally, symmetric key encryption schemes need to use a key exchange scheme for generating more secure session key between two parties. Diffie-Hellman (DH) key exchange scheme is a method to ensure the confidential construction of a shared secret key between two parties in real-time on an unsecure channel. Therefore, DH key exchange scheme is attached to existing symmetric key encryption scheme. In real implementation, normally, the shared secret key that is being established by DH key exchange scheme is used to encrypt and decrypt the subsequent communications using faster symmetric key encryption scheme. However, DH key exchange scheme is based on the difficulty to solve discrete logarithm, which is a hard mathematical problem and requires computationally heavy and complex operations. Since the Boolean operations are simple, quick, and very adaptive to be implemented to an image cryptography scheme, we propose in this paper a new symmetric key encryption scheme based on Boolean operations for binary images. The proposed scheme starts by establishing a shared secret key between two communicating parties and after that this shared secret key is then used as secret key to encrypt and decrypt the subsequent communications. The security of our scheme is based on the difficulty of solving the unsolvable non-invertible matrix problem. The performance results show that the total execution time of our scheme is better and smaller than the total execution time of the conventional scheme (DH with AES) for different sizes of data (image) files. Our scheme is fast, easily implemented and secure.

* Corresponding author: Abdullah Jaafar
E-mail: dr.abdullahjaafar@yahoo.com

All Rights Reserved © 2019 Saba Journal of Information Technology and Networking, Published by Saba University.

1. Introduction

Today digital information can be distributed via the Internet to a large number of people in an easy and simple way. Information security is a field that protects and secures sensitive digital information and its systems from unauthorized access, disclosure, disruption, modification, or destruction. Information security provides many services such as data confidentiality, authentication, data integrity and non-repudiation in order to keep the distribution of sensitive digital information and its systems works reliably [1]-[3].

Information security in the present era is becoming very important in communication and data storage. Data transferred from one party to another over an insecure channel (e.g., Internet) can be protected by cryptography. The main purpose of cryptography is to provide confidentiality by converting the sensitive private information from its normal form (known as plaintext) into an unreadable and useless form (known as ciphertext). The encrypting technologies of traditional and modern cryptography are usually used to avoid the message from being disclosed [4]-[8]. There are, in general, two main types of conventional cryptography which are controlled by keys, symmetric key cryptography and asymmetric key cryptography. Symmetric key cryptography which is also known as secret key cryptography, uses the same key (only one key) for both encryption of plaintext and decryption of ciphertext. The most common symmetric key encryption schemes are DES, 3DES, Blowfish, and AES. Advanced encryption standard (AES) is faster and more efficient than other symmetric key encryption schemes [9], [10]. Unlike symmetric key cryptography, asymmetric key cryptography does not use the same key to encrypt and decrypt a message. Instead, asymmetric key cryptography uses two different keys but related mathematically; the public key which is known to everyone is used for encryption, and the corresponding private key which is kept secret is used for decryption [9], [10]. Symmetric key encryption schemes are much faster computationally than asymmetric key encryption schemes, because asymmetric key encryption schemes require more computational processing power [9]. Symmetric key encryption schemes need to use a key exchange scheme for generating more secure session key between two parties [11]-[15].

In 1976, Diffie and Hellman [16] introduced the first concept of asymmetric (public) key cryptography to solve the secret key exchange problem in the symmetric (secret) key cryptography. Diffie-Hellman (DH) key exchange scheme is a method to ensure the confidential construction of a shared secret key between two parties, in real-time on an unsecure channel (open network) like Internet. A shared secret key then could enable the two parties, who may not have had any previous communication, to encrypt their communications [17]-[19]. The security of the DH key exchange scheme is established under the assumption that calculating discrete logarithms is a hard problem, which require heavy and complex cryptographic computations. The task of calculating discrete logarithms for large prime numbers is considered unfeasible, where the large prime numbers exceed 1024 bits [11], [16], [17], [20], [21]. Therefore, although the hybrid cryptographic schemes (such as the scheme which is resulting of combination of DH key exchange scheme with AES encryption scheme) give the strong security requirements, the performance of the hybrid scheme can be degraded due to increasing total execution time. In addition, many hybrid cryptographic schemes have complex structures and require more computing resources for implementations on images such as binary images. Until now, creating a hybrid scheme with high security and without heavy and complex cryptographic computations has been a great challenge. Therefore, it is important to investigate new key exchange primitive beside to encryption and decryption primitive that require less heavy and complex cryptographic computations but relatively secure.

In this paper, we propose a new symmetric key encryption scheme for binary (black-and-white)

images with easy and secure exchange key, encryption/decryption algorithms and a comparatively low computation complexity. In other words, a novel symmetric key encryption scheme for binary images is proposed, which is based on Boolean operations, to overcome the problem of complex and heavy cryptographic computations as in most of the existing conventional hybrid cryptographic schemes. The proposed symmetric key encryption scheme begins to establish a shared secret key between two communicating parties and after that this shared secret key is then used as the secret key during the proposed encryption and decryption processes.

2. Methods

In this section, we propose a new approach to symmetric key encryption scheme based on Boolean operations for binary (black-and-white) images. Our proposed scheme generates shadow images and manipulates them by using simple Boolean OR, AND, and XOR operations. The OR, AND, and XOR operations of the matrices (images) could be easily implemented by any simple and low computational device.

The proposed approach uses the binary inner product of two $N_{Row} \times N_{Column}$ binary matrices, denoted as $A \odot B$ which is computed by using simple Boolean OR ($\vee$) and AND ($\wedge$) operations as follows:

$$C = A \odot B = \left[\bigvee_{k=1}^{N} (a_{ik} \wedge b_{kj})\right], i = 1, \dots, N_{Row}; j = 1, \dots, N_{Column}.$$

The expression $C = A \odot B$ means that the *ij*-th element c_{ij} of matrix C is equal to $(a_{i1} \wedge b_{1j}) \vee (a_{i2} \wedge b_{2j}) \vee \cdots \vee (a_{iN} \wedge b_{Nj})$, where a and b are the binary elements of matrices A and B, respectively.

In addition, the XOR ($\oplus$) Boolean operation was used in the encryption and decryption processes of the proposed symmetric key encryption method. The XOR of two $N_{Row} \times N_{Column}$ binary matrices could be described by the following formulae:

$$D = A \oplus B = [a_{ij} \oplus b_{ij}], i = 1, \dots, N_{Row}; j = 1, \dots, N_{Column}.$$

The expression $D = A \oplus B$ means that the ij-th element dij of matrix D is equal to $a_{ij} \oplus b_{ij}$, where aij and bij are the ij-th elements of matrices A and B, respectively.

2.1 Shared Secret Key Generation Phase

This phase performs by any two parties (user A and user B such as Alice and Bob, respectively) and consists of the following steps:

1. Both parties agree on a binary public shadow image PuS of 0's and 1's (black-and-white) and in the form of $N \times N$ random pixels, where PuS must be a non-identity and a non-invertible matrix used to avoid information leakage.
2. Alice generates a binary private key (private shadow image) PrK_A of 0's and 1's (black-and-white) and size $N \times N$ pixels. Bob generates a binary private key (private shadow image) PrK_B of 0's and 1's (black and white) and size $N \times N$ pixels.
3. Alice computes her public key PuK_A, as follows: $PuK_A = PrK_A \odot PuS$ (note here the first matrix of binary product must be PrK_A and the second matrix must be PuS). Bob computes his public key PuK_B, as follows: $PuK_B = PuS \odot PrK_B$ (note here the first matrix of binary product must be PuS and the second matrix must be PrK_B).
4. Alice sends her public key PuK_A to Bob. Bob sends his public key PuK_B to Alice.
5. Alice computes the shared secret key SK, as follows: $SK = PrK_A \odot PuK_B$ (note here the first matrix of binary product must be PrK_A and the second matrix must be PuK_B). Bob computes the shared secret key SK, as follows: $SK = PuK_A \odot PrK_B$ (note here the first matrix of binary product must be PuK_A and the second matrix must be PrK_B).

Note that PuK_A (or PuK_B) is the binary product of PuS and PrK_A (or PrK_B), respectively. Note as well that PuS is a bon-invertible matrix which makes recovering PrK_A (or PrK_B) impossible, given PuK_A (or PuK_B) and PuS. The derivation of PuK_A (or PuK_B) is to help in transporting PrK_A (or PrK_B) to user B (or user A), respectively securely.

After performing the above steps, Alice and Bob can obtain a shared secret key SK. That is

$$\begin{aligned} SK_{Alice} &\equiv PrK_A \odot PuK_B \\ &\equiv PrK_A \odot PuS \odot PrK_B \\ &\equiv PuK_A \odot PrK_B \equiv SK_{Bob} \end{aligned} \quad (1)$$

Alice and Bob keep the shared secret key *SK* for later encryption and decryption processes.

2.2 Encrypting (Encoding) Phase

Because the first party's shared secret key *SK* is equal to the second party's shared secret key *SK*, the shared secret key *SK* could serve as an encryption key for the sending party and as a decryption key for the receiving party. Suppose that the first party (such as Alice) has a black-and-white secret image *SI* of size $N \times N$ pixels and she wants to send it to the second party (such as Bob). The sender (Alice) must perform the following steps:

1. Generates the ciphered image *CI* by bitwise XORing the secret image *SI* with the sender's shared secret key *SK* (*SK* serves as an encryption key) which was established previously in the shared secret key generation phase as follows:
$$CI = SI \oplus SK \quad (2)$$
2. Sends the ciphered image *CI* to the receiver, Bob

2.3 Decrypting (Decoding) Phase

The receiver (Bob) must perform the following steps:

1. Receives the ciphered image *CI* from the sender, Alice.
2. Recovers the secret image *SI* by XORing the ciphered image *CI* with the shared secret key *SK* (*SK* serves as a decryption key) which was established previously in the shared secret key generation phase as follows:
$$RI = CI \oplus SK = SI \quad (3)$$

Note that the recovered image *RI* is in the form of $N \times N$ pixels and is equal to the original secret image *SI*. From Equations (2), (3) and because the XOR ($\oplus$) operation is commutative, and $SK \oplus SK$=zeros matrix (full white shadow image), we have:

$$RI = CI \oplus SK = (SI \oplus SK) \oplus SK = SI \oplus (SK \oplus SK) = SI \quad (4)$$

The process flow diagram of the proposed symmetric key encryption scheme is shown in Figure 1.

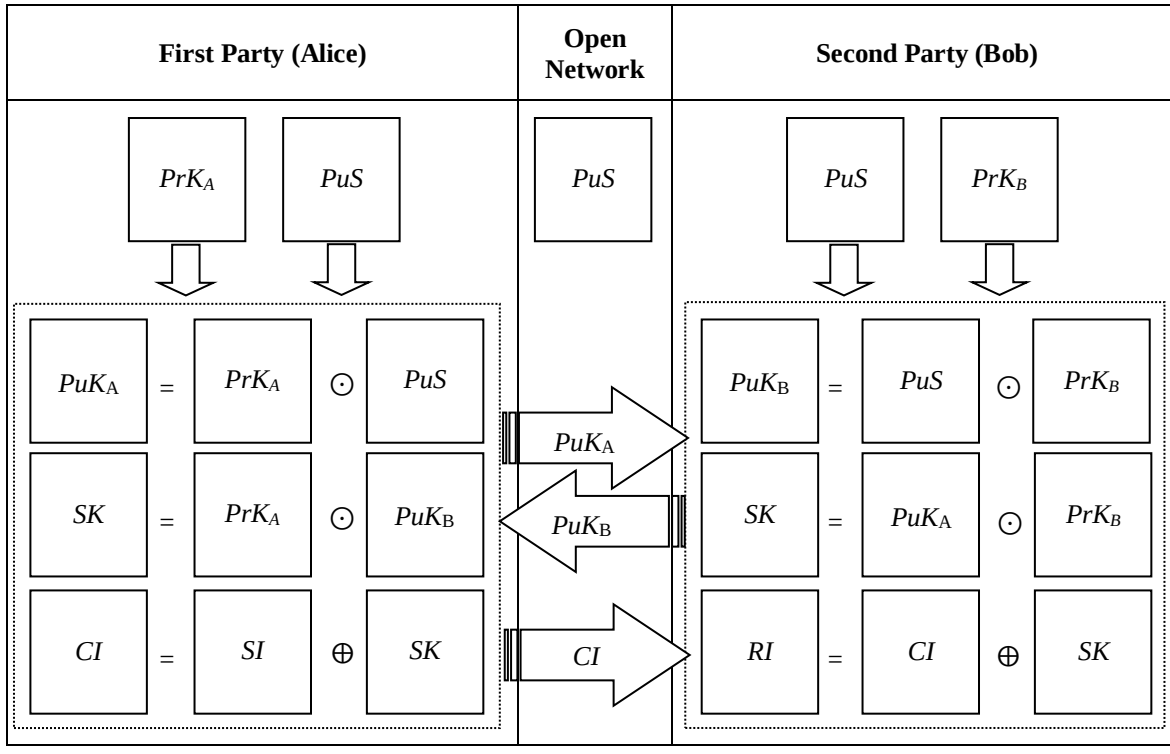


Fig 1. The process flow diagram summarizes the processes of the proposed scheme

3. Results and Discussion

3.1 Experimental Results

Figure 2 shows one of the experimental results of our scheme. In the beginning of the shared secret key generation phase, the first party (Alice) and the second party (Bob) agree on a public shadow image *PuS*. It is assumed that they chose a public shadow image *PuS* with size 302×302 pixels as shown in Figure 2(a). In addition, in the same phase, each party constructs his/her private key (i.e. PrK_A for Alice and PrK_B for Bob). Each party generates his/her public key (i.e. PuK_A for Alice and PuK_B for Bob) and sends it to the other party as shown in Figure 2(b)-(c) and then they establish the shared secret key *SK*, as shown in Figure 2(d). In the encryption phase, it is assumed that the sender takes a binary original image "Pierce Brosnan" with size 302×302 pixels as shown in Figure 2(e) as the secret image *SI*. The secret image *SI* encrypts into 302×302 pixels ciphered image *CI* as shown in Figure 2(f) by XORing the secret image *SI* with the sender's shared secret key *SK*, where *SK* serves as the encryption key. After that, the sender party sends the ciphered image *CI* to the receiver party. In the decryption phase, the ciphered image *CI* decrypts into 302×302 pixels recovered image *RI* as shown in Figure 2(g), which is equal to the original secret image *SI* as shown in Equation (4), by XORing the ciphered image *CI* with the receiver's shared secret key *SK*, where *SK* serves as the decryption key. Note that all the keys and (shadow, secret, ciphered and recovered) images in Figure 2 had been resized to fit into a page.

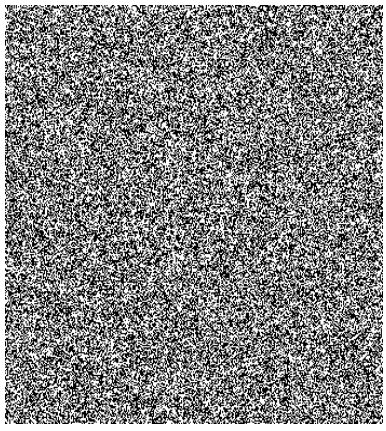
3.2 Security Analysis

The security of the proposed symmetric key encryption scheme is based on the security of Boolean operations and the difficulty of solving the unsolvable non-invertible matrix problem since the problem of inverting the non-invertible matrix is one of the hard mathematical problems that is impossible to solve mathematically (no solutions). In other words, the security of the proposed scheme is based on the security and properties of XOR Boolean operation and also based on the security of the proposed shared secret key *SK* which depends on the difficulty of solving the unsolvable non-invertible matrix problem, where it is impossible to obtain the shared secret key from the public information (i.e. *CI*, *PuS*, PuK_A and PuK_B). This is especially true when using a proper shadow image size, which leads to low probability of successful attack.

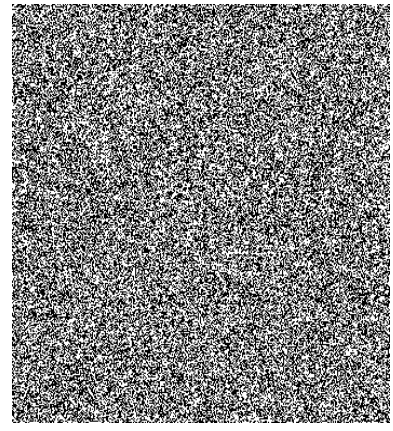
In order to decrypt the ciphered image *CI*, that is, to recover the original secret image *SI*, attackers may try to generate the shared secret key *SK* from all information open to public (i.e. *CI*, *PuS*, PuK_A and PuK_B). Note that first of all, it is clear that the product of a non-invertible matrix with any other matrix must always result in a non-invertible matrix as mentioned in [22]. Therefore, the parties public keys (PuK_A and PuK_B) are non-invertible and non-identity matrices, since *PuS* is a non-invertible and a non-identity matrix which product with each party's private key (PrK_A, PrK_B) for producing the parties public keys (PuK_A and PuK_B) as earlier shown in Subsection 2.1. Secondly, it is practically impossible to determine the inverse of the party's public key (PuK_A, PuK_B) from the public shadow image *PuS*, since *PuS* is a non-invertible and a non-identity matrix as earlier mentioned in Subsection 2.1. Therefore, attackers would encounter difficulties when trying to determine the shared secret key, provided that the size of the shadow images are chosen to be large enough.

In the encryption phase, the sender (Alice) could encrypt the secret image *SI* by XORing it with the shared secret key *SK* has already been established between the two parties and here, serves as an encryption key. The sender(Alice) sends *CI* to the receiver (Bob).

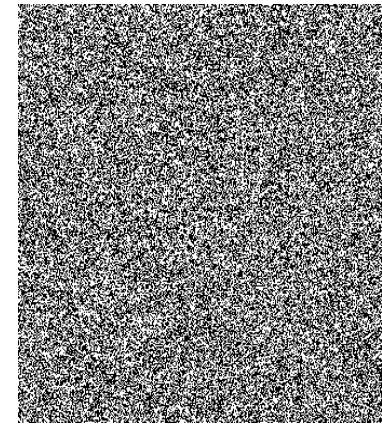
In decryption phase, the receiver (Bob) could recover the secret image *SI* by XORing the shared secret key *SK* (here *SK* serves as a decryption key) with the ciphered image *CI*, but ciphered image *CI* alone cannot disclose any information about the original secret image. In addition, if the ciphered image *CI* is changed and forged by an attacker, the recovered image *RI* is unclear and the secret is still unidentified. Therefore, the proposed symmetric key encryption scheme is considered very secure.



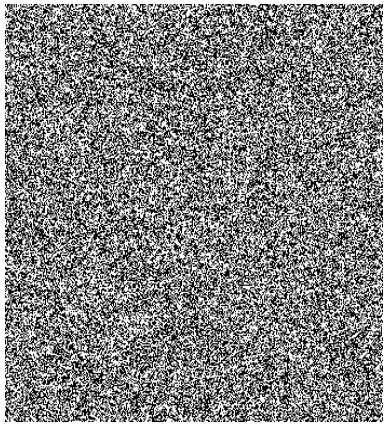
(a) Public Shadow Image (*PuS*)



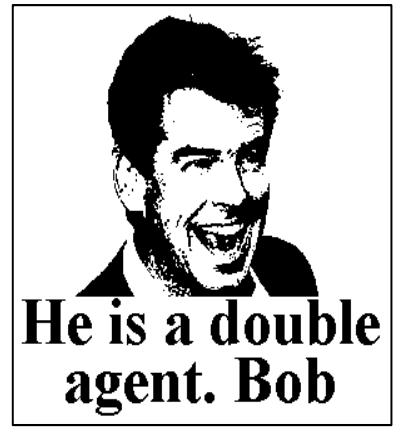
(b) Alice's Public Key (PuK_A)



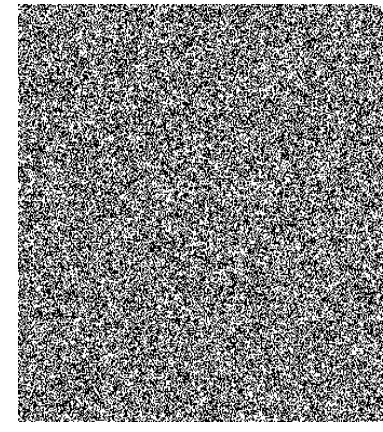
(c) Bob's Public Key (PuK_B)



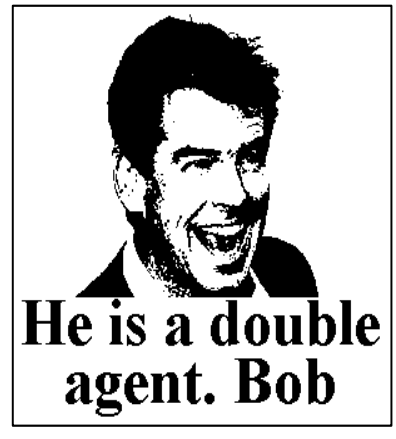
(d) Shared Secret Key (*SK*)



(e) Secret Image (*SI*)



(f) Ciphered Image (*CI*)



(g) Recovered Image (*RI*)

Fig 2. One of the experimental results of the proposed scheme

3.3 Computational Complexity

Two types of the complexity of the proposed symmetric key encryption scheme will be discussed in this section, algorithm complexity and brute-force attack complexity on the algorithm. Image encryption algorithm in the proposed symmetric key encryption scheme includes two things: first, obtaining the shared secret key *SK*, and then creating the ciphered image *CI* by XORing the shared secret key *SK* with the secret image *SI*. The shared secret key includes constructing two multiplication of two binary matrices on each party. The time complexity of constructing two multiplication of two binary matrices on each party is $O(N^3)$ + $O(N^3)$ = $O(N^3)$, if neglecting the constant and the multiplication is carried out naively (here multiplication means performing the OR and the AND Boolean operations of two binary matrices as shown in the beginning of Section 2). The time complexity of the ciphered image *CI* is $O(N^2)$. Therefore, the total time complexity for image encryption is $O(N^3)$ + $O(N^2)$ = $O(N^3)$, excluding the time needed to generate two distinct random shadow images (private keys); where the size of the shadow image is equal to $N \times N$ pixels. On the encryption side, generating the shared secret key *SK* requires $2N^3$of AND Boolean operations and $2(N^3\text{-}N^2)$ of OR Boolean operations. In addition, generating the ciphered image *CI* requires $N^2$of XOR Boolean operations. Image decryption algorithm in the proposed encryption scheme includes two things: first, obtaining the shared secret key and then XORing the shared secret key *SK* and the ciphered image *CI* for reconstructing the secret image *SI*. The time complexity for reconstructing the secret image *SI* is equal to the time complexity of the shared secret key which has already mentioned, is $O(N^3)$. On the decryption side, generating the shared secret key *SK* requires $2N^3$of AND Boolean operations and $2(N^3\text{-}N^2)$ of OR Boolean operations. In addition, generating the recovered image *RI* requires $N^2$of XOR Boolean operations. The proposed encryption scheme's time complexities analyzed above are the processes carried out by any two parties such as Alice and Bob. For brute-force attack, the attacker must find the private keys (PrK_A and PrK_B) from the public keys (PuK_A and PuK_B) to break the shared secret key and then decrypting a ciphered image *CI*. The time complexity of the attack is $O(2^Z)$, where *Z* is the total number of binary pixels in the image (image size in bytes), which is relatively a large number. Therefore, the effort and time needed for the brute-force attack to find private keys is too consuming especially when the size of those private keys are large.

3.4 Performance Results

Table 2 shows performance comparisons for the proposed encryption scheme against the conventional hybrid encryption scheme (DH + AES). The two schemes were coded in Turbo C++ 4.5 programming environment and run on a personal computer equipped with 2.80 GHz Intel® Pentium 4 CPU, 512 MB of RAM and Windows XP operating system. The execution times taken by the conventional hybrid and the proposed encryption schemes are calculated for different sizes of data (image) files. According to the comparison results, as shown in Table 2, it is found that the total execution time (key generation + encryption + decryption) of the proposed encryption scheme is faster than that of the conventional hybrid encryption scheme (DH + AES). From the same table, it is clear that the total execution time taken for our scheme decreases when the size of the image file is decreased.

4. Conclusion

In this paper, we proposed a new symmetric key encryption scheme to protect binary images. The proposed scheme offers both key exchange and encryption/decryption processes. Therefore, it provides alternative method for two parties to establish the shared secret key between them and after that this shared key is then used as the secret key during the proposed encryption and decryption processes. The proposed scheme has several benefits compared to the conventional schemes such as more secure, has noise-like shadow images, uses only simple Boolean operations, less computational complexity, comparatively fast and easy to implement. Therefore, we can use and implement our scheme in many applications and

various fields like in military, defense and other places where the confidentiality of data should be must. our scheme can be extended for dealing with grayscale and color secret images.

References

[1] I. Ozturk and I. Sogukpinar, "Analysis and Comparison of Image Encryption Algorithms", International Journal of Information Technology, 1(2), pp. 64-67, 2005.

[2] M. S. Anoop, "Public Key Cryptography– Applications Algorithms and Mathematical Explanations", Tata Elxsi Ltd., 2007. http://www.tataelxsi.com/whitepapers/pub_key2.pdf?pdf_id=public_key

[3] C. Chan and Y. Wu, "A Visual Information Encryption Scheme Based on Visual Cryptography and D-H Key Agreement Scheme", International Journal of Computer Science and Network Security, 8(4), pp. 128-132, 2008.

[4] Y. C. Hou and S. F. Tu, "A Visual Cryptographic Technique for Chromatic Images Using Multi-pixel Encoding Method", Journal of Research and Practice in Information Technology, Tamkang University, Jung Li, Taiwan, vol.37, no.2, pp. 179-192, 2005.

[5] Y. C. Hou, "Visual cryptography for color images", Pattern Recognition 36 (7), pp. 1619-1629, 2003.

[6] A. Houas, Z. Mokhtari, K. E. Melkemi and A. Boussaad, "A novel binary image encryption algorithm based on diffuse representation", Engineering Science and Technology, an International Journal 19, pp. 1887-1894, 2016.

[7] I. Ozturk and I. Sogukpinar, "Analysis and Comparison of Image Encryption Algorithms", International Journal of Information Technology, vol.1, no.2, pp. 64-67, 2005.

[8] C. Chan and Y. Wu, "A Visual Information Encryption Scheme Based on Visual Cryptography and D-H Key Agreement Scheme", IJCSNS International Journal of Computer Science and Network Security, vol.8, no.4, pp. 128-132, 2008.

[9] N. K. Barpanda, M. Panda and A. Panda, "Image File Encryption using Symmetric Key Algorithms", International Journal of Advance Research in Science and Engineering, vol. 07, no. 07, 2018.

[10] M. Islam, M. Shah, Z. Khan, T. Mahmood and M. J. Khan, "A New Symmetric Key Encryption Algorithm using Images as Secret Keys ", 13th International Conference on Frontiers of Information Technology, pp. 1-5, 2015.

[11] W. Stallings, "Cryptography and Network Security-Principles and Practices", Prentice Hall, Inc, 4th Ed, 2006.

[12] C. S. Laih and K. Y. Chen, "Generating visible RSA public keys for PKI", Int. J. Secur. 2. 2, Springer, Berlin, pp. 103-109, 2004.

Scheme	Size of Data (Image) File	Brute-Force Complexity	Total Execution Time (ms)
DH (n=1024 bit) [23] + AES-128 bit [24]	1 KB	2^{80} [21]	247.327
	16 KB		248.152
	64 KB		250.792
	256 KB		261.354
Our Scheme	32×32 pixel (1 KB)	2^{1024}	0.059
	128×128 pixel (16 KB)	2^{16384}	3.813
	256×256 pixel (64 KB)	2^{65536}	30.504
	512×512 pixel (256 KB)	2^{262144}	244.032

Table 1: Performance Comparison between the conventional hybrid encryption scheme (DH + AES) and the proposed symmetric key encryption scheme (millisecond)

[13] J. J. Amador and R. W. Green, "Symmetric-Key Block Cipher for Image and Text Cryptography", IJIST (15), no.3, pp. 178-188, 2005.
[14] I. Muecke, "Greyscale and Colour Visual Cryptography", M.S. thesis, Dalhousie University, USA, 1999.
[15] W. D. Shun, Z. Lei, M. Ning and H. L. Sheng, "Secret Color Images Sharing Schemes Based on XOR Operation", Tsinghua University, Beijing, China, 2005.
[16] W. Diffie and M. Hellman, "New Directions in Cryptography", IEEE Transactions in Information Theory, vol. IT-22, no.6, pp. 644-654, 1976.
[17] D. A. Carts, "A review of the Diffie-Hellman algorithm and its use in secure internet protocols", SANS Institute Reading Room, 2001.
[18] K. Palmgren, "Diffie and Hellman key exchange: a non-mathematician's explanation", Expert Reference Series of White Papers, 2005.
[19] Y. XUE, "Overview of public-key cryptography", CS 291: Special Topics on Network Security, Vanderbilt University, 2007.
[20] J. Rothe, "Complexity Theory and Cryptology: An Introduction to Cryptocomplexity". Berlin: Springer, 2005.
[21] E. Barker W. Barker, W. Burr, W. Polk and M. Smid, "Recommendation for Key Management-Part 1: General (Revised)", NIST Special Publication 800-57 (Computer Security), pp. 58-63, 2007.
[22] A. E. Coulson, "Introduction to Matrices", London: Longman Group Limited, 5th impression, 1974.
[23] Code Taken From: http://www.example-code.com/vcpp/dh_key_exchange.asp
[24] Code Taken From: http://www.hoozi.com/post/0m3lb/advanced-encryption-standard-aes-implementation-in-c-c

journal homepage:ojs.www.sabauni.net

S.J.I.T.N
Saba Journal of Information Technology and Networking

Article

An Analytical study to Calibrate Quality of Service and Security Parameters of Voice Transmission over IPSec (QSVoIP) for Maximum Number of Calls with Acceptable Voice Quality

Ammar Thabit Zahary[1]*, Anwar Omar Adam[2]

[1]Faculty of Computer and Information Technology, Sana'a University, Sana'a, Yemen

[2]The Arab Academy for Financial and Banking Sciences, Sana'a Branch, Yemen

Article info

Article history:

Accepted: Oct. 2018

Keywords:

Voice-over-IP (VoIP), IP Security (IPSec), Voice-over-IPSec(VoIPSec), Encapsulating Security Payload (ESP), Encryption, Authentication, Quality of Service (QoS).

Abstract

Security in Voice-over-IP (VoIP) concerns protecting both the content, by encryption, and speaker identification, by authentication. IP Security (IPSec) technique can be used for this purpose. In addition, IPSec is usually applied with Encapsulating Security Payload (ESP) using tunnelling protocol. However, security strengthen of Voice-over-IPSec (VoIPSec) may affect Quality of Service (QoS) during VoIP transmission. This paper conducts approach called QSVoIP that calibrates QoS and Security parameters of Voice transmission over IPSec for maximum number of calls with maintaining acceptable voice quality that can be heard clearly by the listener. QSVoIP tries to reduce human threat in many aspects, such as packet sniffers, middle attacks, and several types of voice traffic analysis. QSVoIP conducts a developed method that estimates number of voice calls that can be applied in IPSec network with subject to maintain acceptable voice quality. This paper also presents performance analysis of VoIP communication over IPSec network, which has been executed for different scenarios using OPNET simulator in terms of end-to-end delay, jitter, and packet loss. The simulation results' analysis shows that transmitting voice over IPSec dramatically deteriorates the quality of VoIP. Results have shown that QSVoIP approach can effectively help network administrators and designers to determine the number of voice calls that can applied for a particular network with acceptable voice quality.

* Corresponding author: Ammar Thabit Zahary
E-mail: aalzahary@gmail.com

All Rights Reserved © 2019 Saba Journal of Information Technology and Networking, Published by Saba University.

1. Introduction

Recently, there is a growing interest can be observed clearly in the voice transmission using Internet Protocol (IP). The transmission of voice and data over packet networks is rapidly changing the way of communication for both businesses and individuals. However, security issue remains a challenge in packet networks. If confidentiality and authenticity usually protect privacy and accuracy of voice and data communications, they also have to be preserved against malicious activities such as spying, viruses, and spoofing that can highly occur with the increasing use of the Internet [1].

Nowadays, voice communication over IP (VoIP) is transforming the telecommunication industry. VoIP technology provides several opportunities for users such as simpler deployment, lower call fees, and more convergence of voice and data networks. Additionally, VoIP technology can make greater integration with multiple multimedia applications. However, VoIP also brings up new challenges despite the existence of all the technological and economic opportunities mentioned above. Security is perhaps the most compelling [1], thus, security is considered a major issue in VoIP networks.

VoIP security concerns with both encryption and authentication. Encryption is used for protecting what a person says whereas authentication is used to authorize the person who is speaking. IPSec technique can be used to achieve goals, encryption and authentication. In addition, IPSec usually applied with ESP and tunnelling protocols which can be used to secure the identities of both endpoints and protect voice data from the potential prohibited users once packets leave the intranet of a particular enterprise. However, to increase availability of encryption, IPSec is usually incorporated with IPv4. Voice-over-IPSec (VoIPSec) can help reducing human threats, such as the middle attacks, packet sniffers, and many types of voice traffic analysis.

As mentioned above, IPSec can be used to achieve both encryption of the content and authentication of the user. In addition, it can be applied with ESP using tunnel method. However, security strengthen of VoIPSec may affect QoS during VoIP transmission. Therefore, there is a need to address the effect of applying security protocols to evaluate the performance and efficiency of VoIP communications. Furthermore, there is a need to have the ability to determine the maximum number of calls that can be maintained in VoIPSec networks. Thus, the aim behind this paper is to study the performance effect adding IPSec to VoIP networks.

This paper proposes a new approach called QSVoIP that calibrates QoS and Security parameters of Voice transmission over IPSec for maximum number of calls with acceptable voice quality. QSVoIP tries to reduce human threat in the middle attacks, packet sniffers, and the analysis of many voice traffic types. QSVoIP estimates number of voice calls that can be maintained in IPSec network with acceptable voice quality. Moreover, the paper introduces performance evaluations of voice transmission over secure communication links by implementing IPSec with different simulation scenarios using OPNET Modeler simulator. The simulation results shows that transmitting voice over IPSec dramatically deteriorate quality of VoIP. As shown by the results, QSVoIP approach can effectively help network administrators and designers determining the number of voice calls that can be maintained for a given network with acceptable voice quality in terms of end-to-end delay, jitter, and packet loss.

The paper is organized as follows: Section 2 presents an overview of VoIP and IPSec technologies. Section 3 presents the related work of VoIP and IPSec technologies related to voice quality. The proposed approach, QSVoIP, is described in Section 4. Section 5 presents QSVoIP implementation and simulation environment. Section 6 presents simulation results and performance evaluation. Finally, Section 7 concludes the paper.

2. RELATED WORK

There are several researches that have been carried related to this topic such as [3, 37, 38, and 39], which revealed the QoS issues associated

with VoIPSec.

In [3], researchers presented an experimental study of voice traffic transmitted over IPSec. They have executed a series of experiments on a real testbed to evaluate the impact on performance with a particular attention to bandwidth usage and transmission delay. Authors aim to increase the packet size stemming from IPSec usage. A version of IPSec called cIPSec has been implemented in [3] to compress the internal header of a packet down to approximately four bytes. This can be achieved because much of data in the internal headers of a packet remains constant or duplicated in the outer header. However, authors in [3] did not consider the actual time required to perform the compression which may take much longer than the time saved in crypto-engine. Moreover, a shortcoming point is that the compression scheme used in IPSec can compress only the packet header. In addition, this scenario is not applicable to the compression QoS issues associated with codec because only IP headers are considered not the actual media. Alternatively, for more compression, QoS changes according to the change in codec.

In [12], researchers proposed an approach of an IPSec approach to secure SIP based VoIP network. They have executed different configurations of IPSec for VoIP networks and evaluated the performance through a series of experiments. Results have shown that encryption is the more expensive operation in end-to-end delay, jitter, and packet loss when employing IPSec encryption and authentication services for VoIP signaling and media streams. Whereas, if both encryption and authentication services are employed, it is clearly remarked that a dramatically increase in call setup times is achieved. It is remarked that an increase of about 200% in jitter value, about 170% in media stream delay. Moreover, an exponentially increase has been remarked in the SIP call setup time and media stream delay with remarkable increase in the network call density. A crucial shortcoming of the simulation results in [12] is that transmitting voice over IPSec using their proposed approach increases packet loss, delay variation (jitter), and end to end delay.

In [33], authors proposed a model that tries to ensure secure call for VoIP Quality of service using SRTP protocol. Authors argued the common approaches of VoIP telephony that try to ensure protection and the impact of employing SRTP. Authors aimed to evaluate how it can ensure the secure stream of VoIP service and provide satisfactory quality of service. Moreover, SRTP simulation results have shown that the voice packets delay does not exceed critical 150 millisecond (ms) value and so they certainly supposed that quality of service can be essentially ensured for encrypting voice packets.

In [34], authors proposed an IPSec approach for VoIP network based on secured session initiation protocol SIP. Authors addresses some security issues using SIP protocol with IPSec, however they did not address voice quality issues.

In [40], authors addressed the effects of the security parameters on the VoIP QoS and proposed a QoS-oriented method that allows the deployment of secured VoIP networks without adversely affecting the provided quality of service.

In [41], authors brought a detailed view of video streaming performance over an IP-based network. They compared video quality with both packet loss and encryption. The measured results demonstrated the relation between the type of video codec and bitrate of the final quality of video.

In [42] authors tested consequently, the impact of IPSec encryption on CPU utilization of the router, the required bandwidth and quality of voice. All parameters were depending on the number of performed calls. They concluded that setting the appropriate period of voice payload can change the number of packets that are simultaneously transmitted and processed, and also affects CPU utilization and bandwidth.

Researchers in [43] proposed a multipath solution for the major security threats of VoIP communications, especially for low bandwidth networks. Results show that security affects VoIP quality especially for a large distance communicating nodes and also for large packet size. The proposed multipath solution seems outperforms single routing protocols in low bandwidth networks, especially in terms of reducing packet loss.

Recently authors in [45] the performance of VoIP on IPv4, IPv6 and 6in4 protocol with and without

IPsec is compared. RTT (Round Trip Time), Throughput, Jitter and CPU usage are compared in VoIP networks. The results for throughput are almost same for both operating systems. CPU usage was higher on both operating systems with IPsec enabled and the results for RTT and Jitter were inconsistent. In general, the results indicated that Fedora 16 performance was better than Windows 7. The results show that although IPSec can add security, it can reduce the VoIP performance in terms of higher delay and higher CPU usage. The main drawback of the paper is that it did not address the voice quality issues.

In [46], authors discuss about site-to-site IPsec VPN which communicate in the intra-nets. The implementation of IPsec VPN is done with security protocols for exchanging key management, authentication and integrity using Graphical Network Simulator 3 (GNS3). The encryption of data packets when information is transferred between different sites is tested and verified using tools like Ping, IPerf and Wireshark. The performance in terms of delay, bandwidth consumption, jitter and the data rate of the proposed method with and without Firewalls is analyzed. It is obvious that our proposed method can provide the security and prohibit the attackers to attack the network. However, authors did not address voice quality issues in this paper.

Most recent, authors in [47] assessed the quality of voice call in terms of lost packet ratio, latency and jitter with and without SCIP algorithm. However, they did not estimate the maximum number of calls that can be considered a threshold value of good voice quality.

2. QSVOIP APPROACH

This section presents the idea behind our approach QSVoIP which has been developed in this paper and executed using simulations of secure VoIP networks. As mentioned previously in Section 2, there are several methods that have proposed by many researchers related to this topic, which revealed the QoS issues associated with VoIPSec. However, all of these researches considered only study of VoIP traffic.

This paper tries to address the effect of peer-to-peer voice calls on the voice quality. It focuses mainly on examine the impact of apply IPSec to the quality of transmitting voice traffic. In addition, the paper investigates how the performance of voice communication can be affected when QoS is considered. The proposed approach will assist network operators and designers to determine the number of VoIP calls that can be maintained in a particular network with acceptable voice quality. The proposed QSVOIP approach, has been executed and comparatively evaluated using OPNET modeller with four different scenarios as well explained in Section 4.3.

Simulation results comparatively analysed and the performance of the proposed approach will be evaluated in terms of packet loss, voice jitter, and end-to-end delay, packets sent and packets received. Results are presented in Section 5 with a discussion of the implications of these results for designers who are interested to the implementation of real secure VoIP networks.

4. SIMULATION IMPLEMENTATION

This section describes in details the simulation model, various simulation scenarios, as well as traffic model. The simulation experiment is carried out using OPNET Modeller simulator 14.5.A PL8 (Build 7808 32-bit) under Windows as a platform.

4.1 Simulation Environment

To fulfil the aim of the research, we have divided the simulation execution into two parts.

Part 1: VoIP traffic is send from source to destination in four scenarios. The goal of this task is to examine the effect of adding IPSec on the quality of transmitting voice over communication links, and to compare the performance of voice traffic in terms of throughput, packet loss, voice jitter, and packet End-to-End delay.

Part 2: The approximate maximum number of calls that can be maintained with acceptable voice quality are estimated in the four scenarios using our approach. QSVOIP approach can be used in a real network to estimate the maximum number of calls and calibrating it with acceptable voice quality. This can be done by designing the real network in OPNET Modeler and make the needed simulations. End-to-End delay performance metric is used in this paper to estimate the

approximate maximum number of calls maintained in the four network scenarios.

The network model used for the simulation in this paper is shown by Figure 4. This network model consists of two LANs connected via Internet through Router_1 and Router_2. Link speed is 100Mb/s between LANs and routers and 2Mb/s between routers and Internet.

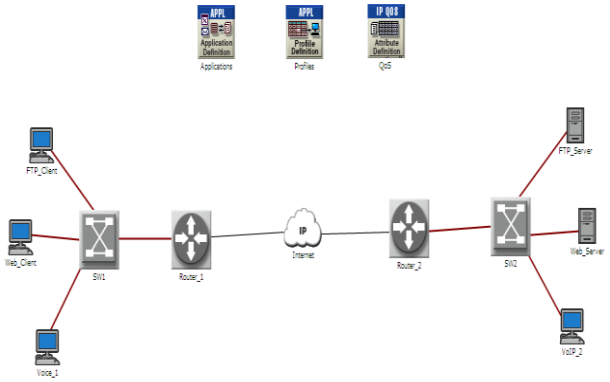


Figure 4. Network simulation model.

Table 1. Components of network model

Component	Model	Type	Qty
Applications	Application Config	Utilities	1
Profiles	Profile Config		1
QoS_Config	QoS Attribute Config		1
Internet	ip32_cloud	Internet Cloud	1
Router_A	Ethernet4_slip 8_gtwy	Router	3
Router_B			
SW1	Ethernet16_s witch	Switch	3
SW2			
FTP_Server	Ethernet_server	Server	2
Web_Server			
FTP_Client	Ethernet_wkstn	Workstat ion	4
Web_Client			
Voice_T			
Voice_R			
Connection	PPP_ E1(2.048 Mbps)	Link	2
	100BaseT	Link	6

As shown in Figure 4, the first LAN on left side, consist of one router represents Router_1, one an Ethernet switch represents SW1 and three designated Ethernet workstations represent FTP_Client, Web_Client and Voice_1. FTP_Client, Web_Client workstations are a source for generate the background traffic while Voice_1 is a source for sending VoIP calls. The second LAN on right side, consist of one router represents Router_2, one an Ethernet switch represents SW2 and three designated Ethernet servers represent FTP_Server, Web_Server and one workstation represent Voice_2. The Ethernet Servers will support FTP traffic, HTTP traffic and generate the traffics needed to study. Voice_2 is a sink for receiving VoIP calls from Voice_1.

The cloud symbol represents the Internet. The IP cloud is responsible for routing the incoming packets to the appropriate destination based on the packet header information. The network model has been build up with the main components listed in Table 1.

4.2 Modelling Assumptions

The following assumptions are considered when building the Tcl script:

1. Because of the traffic in a network varies from source to destination at any time, so it is hard to predict the traffic behavior in the network.
2. VoIP model has been simulated in this paper by considering the worst case scenario (when we need to estimate the maximum number of VoIP calls that a network can support with acceptable voice quality).
3. The background traffic is considered to be as 50% of link capacity excluding the VoIP traffic. To protect it from bursts, 60% link capacity is the maximum utilization allowed of a link [16].
4. It is required that end-to-end packet delay should not exceed 150ms for VoIP applications in order to ensure acceptable quality of a particular VoIP call.

Modelling assumptions of our simulation can be summarized as follows:

1. Local area networks operate at 100Mb/s throughout the simulations.
2. Simulation time of each simulation experiment is 8 minutes.
3. There is no voice conferencing throughout the simulation, only peer-to-peer voice calls are applied.

4.3 Simulation Scenarios

A simulation study is carried out by the simulation of four network scenarios with the same network topology. Results have been analyzed in terms of same performance metrics. The simulation network model shown in Figure 4 consists of four scenarios described as follows:

- ***Scenario 1: Baseline (with no security services)***

In this scenario, no encryption is used by the source. Thus, voice data travels to and from the destination is unencrypted. In this scenario, when a workstation receives voice data from any end-party, it simply forwards it to its destination.

- ***Scenario 2: IPSec with Authentication only***

In this scenario, it provides authentication alone. Authentication Header (AH) does not provide data confidentiality (encryption) of packets. This mean no encryption it used, so the packet is transported unencrypted. In this scenario the modification is done by adding overhead value about 40 bytes (320 bits) to the packet.

- ***Scenario 3: IPSec with Encryption only***

In this scenario, it provides confidentiality alone. In this scenario the modification is done by adding overhead value about 44 bytes (352 bits) to the packet.

- ***Scenario 4: IPSec with both Encryption and Authentication***

In this scenario, it provides both encryption and authentication. In this scenario, the additional overhead value is about 52 bytes (448 bits) to the packet.

Cryptographic algorithms implemented in this scenario are as follows:

- For encryption: DES [28] has been implemented in CBC mode.
- For authentication: HMAC-MD5 [30] has been implemented with default configuration.

Processing latencies configured in model for MD5 and DES algorithms were based on values reported by [30] and [28], respectively.

Modifications made to the OPNET model are as follows:

1. Because security functions models are not provided by OPNET Modeler, we have modified the source code of the transceiver system models in order to apply additional overhead to represent the various solutions of security with simulating additional load of more security schemes. The simulation is done by changing the OPNET model compared to the normal packet flow that results from a one-to-one call over the network [42].
2. A modification has been made for Ethernet_wkstn nodes in the IPSec scenarios with adding more security overhead and payload to each packet generated prior to encapsulation.

5. Simulation Results Study

In this section, a detailed simulation results are analyzed and the performance of VoIP network is tested. Before running simulation, OPNET model should be configured with a number of VoIP network components such as switches, router, links, and VoIP traffic. This section presents the simulation results obtained from the various scenarios that have been executed to examine the performance and the effect of implementing IPSec on the quality of transmitting voice traffic using OPNET simulator. Simulation results have been comparatively analysed and the performance of our approach has been evaluated in terms of packet loss, voice jitter, and end-to-end delay, packets sent and packets received. Results are presented in this section with a discussion of the implications of these results for designers who are interested to the implementation of real secure VoIP networks.

The duration of simulation for each scenario is configured to 8 minutes (420 seconds). The generation of background traffic, started at 40 seconds from the start time of the simulation run. The VoIP traffic starts at the 100 seconds after the simulation is initially started, and stops at the 420 seconds of the simulation time. VoIP calls have been added at fixed time intervals in four scenarios (for every five seconds starting from 100 seconds till 420 seconds).

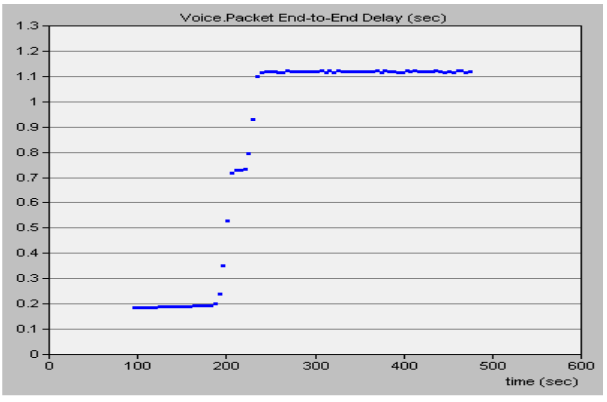
5.1 *Voice End-to-End Delay*

As explained in the Section 4, in order to establish VoIP calls with acceptable voice

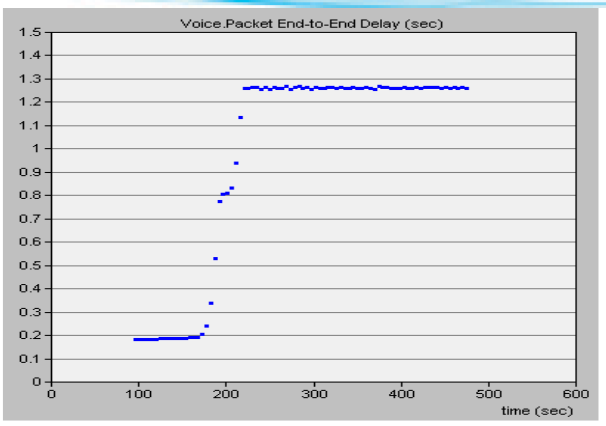
quality, end-to-end delay in a VoIP network should not exceed the threshold value of 150 milliseconds [27]. Figure 5 (a, b, c, d, and e) shows the results of end-to-end delay for four network models/scenarios, namely: 1) baseline, 2) IPSec with authentication only, 3) IPSec with encryption only and 4) IPSec with both encryption and authentication, respectively. It clear that in Figure 5(a), the average end-to-end delay in baseline scenario is 832.1 milliseconds which exceeds the threshold. In the second scenario as shown in Figure 5(b), IPSec with authentication only, the average end-to-end delay exceeds the threshold at 971.5 milliseconds. In the other hand, in the third scenario as shown in in Figure 5(c), IPSec with encryption only, the average end-to-end delay exceeds the threshold at 1023.3 milliseconds, and in the fourth scenario as shown in Figure 5(d), IPSec with both encryption and authentication, the average end-to-end delay exceeds the threshold at 1075.9 milliseconds.

VoIPSec networks reach the threshold earlier than Baseline network, is due to that encryption and authentication services are employed.

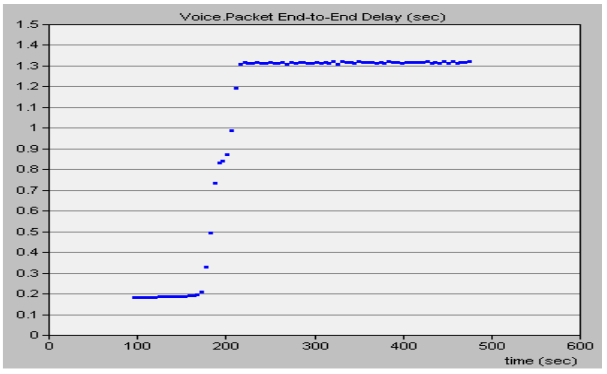
Also it is observed from Figure 5(e) that the delay of IPSec with encryption and authentication is higher than Baseline network, around 130%. This increasing in delay is happened due to that the encryption provided by IPSec provides an additional level of security for voice conversations. The average values of end-to-end delay for the four scenarios are shown in Table 2.



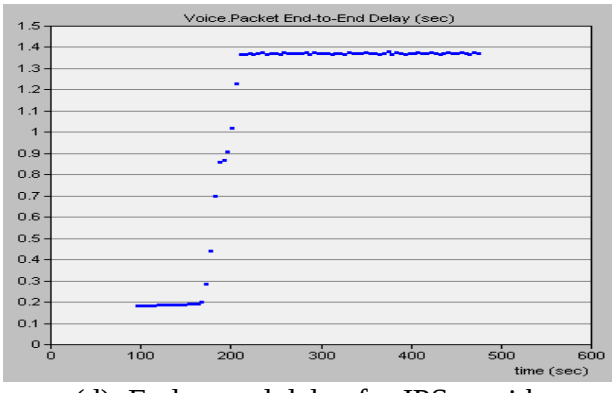
(a): End-to-end delay for baseline scenario



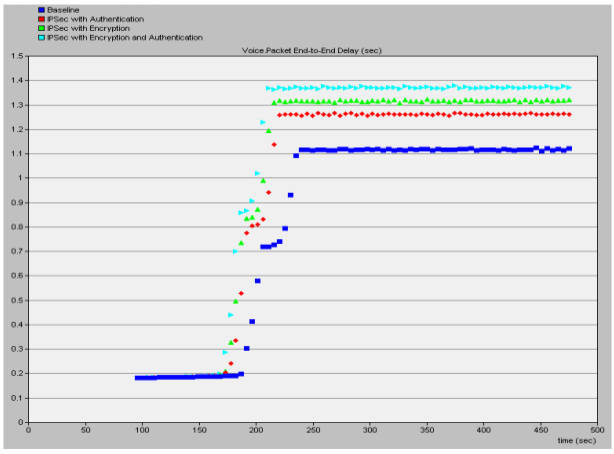
(b): End-to-end delay for IPSec with authentication scenario



(c): End-to-end delay for IPSec with encryption scenario



(d): End-to-end delay for IPSec with authentication and encryption scenario



(e): End-to-end delay for all scenarios

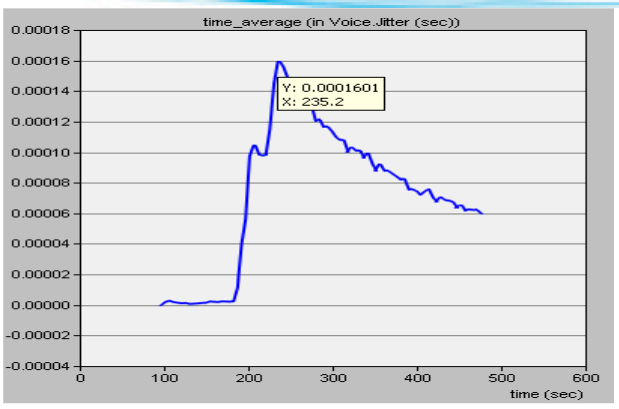
Figure 5. Voice Packet end-to-end delay for different scenarios

Table 2. The average values of end-to-end delay (sec)

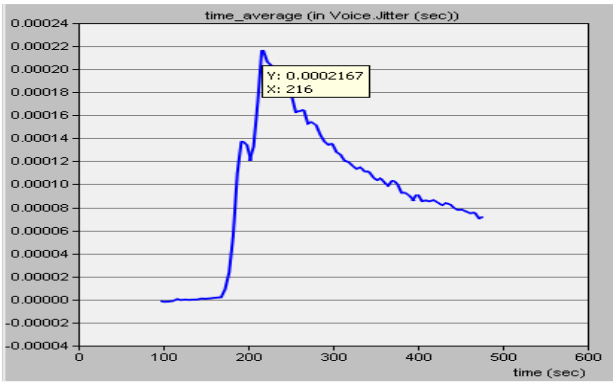
Scenario name	End-to-end delay
Baseline	0.8321
IPSec with Authentication	0.9715
IPSec with Encryption	1.0233
IPSec with Encryption and Authentication	1.0759

5.2 *Voice Packet Delay Variation (Jitter)*

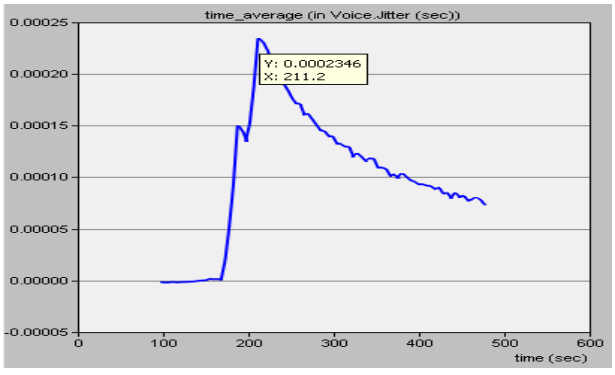
Figure 6 (a, b, c, d, and e) shows the results of voice packet delay variation (jitter) for four network models/scenarios, namely: 1) baseline, 2) IPSec with authentication only, 3) IPSec with encryption only and 4) IPSec with both encryption and authentication. It clear that the packet delay variation (jitter) starts to increase at 160 microseconds for baseline scenario. For IPSec with authentication only, it starts to increase at 216.7 microseconds. For IPSec with encryption only, it starts to increase at 234.6 microseconds. For IPSec with both encryption and authentication, it starts to increase at 250.3 microseconds. As shown in Figure 6e, it can be seen that the jitter of IPSec with encryption and authentication is higher than Baseline network by around 156%. The average values of jitter for four scenarios are shown in Table 3.



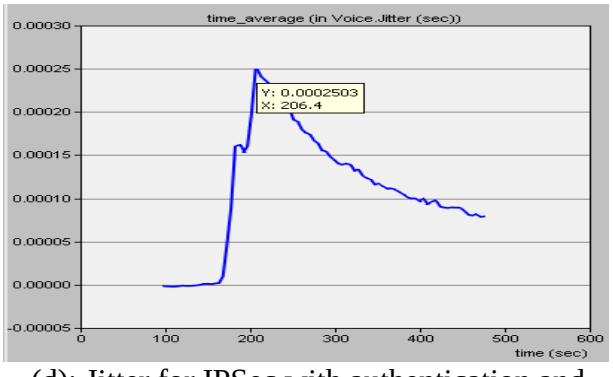
(a): Jitter for baseline scenario



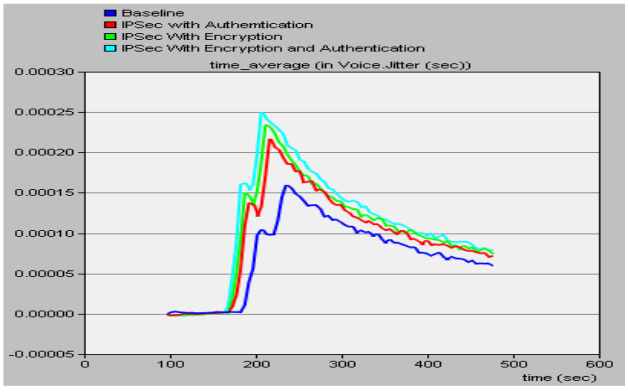
(b): Jitter for IPSec with authentication scenario



(c): Jitter for IPSec with encryption scenario



(d): Jitter for IPSec with authentication and encryption scenario



(e): Jitter for all scenarios

Figure 6. Voice Packet jitter for different scenarios

Table 3. The average values of jitter (sec)

Scenario name	Jitter
Baseline	0.0001600
IPSec with authentication	0.0002167
IPSec with encryption	0.0002346
IPSec with encryption and authentication	0.0002503

5.3 *Voice Packet Loss*

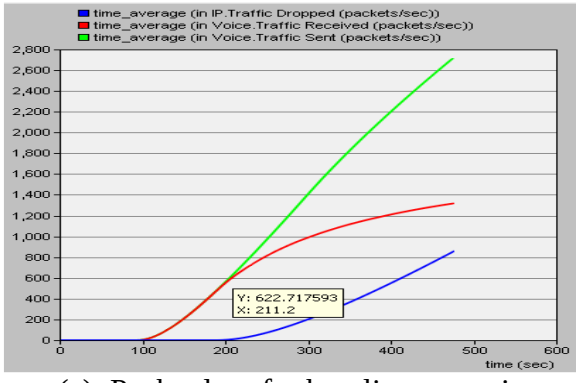
Figure 7 (a, b, c, d, and e) gives the average number of packet loss (sent, received, and dropped packets/sec) for four network models/scenarios, namely: 1) baseline, 2) IPSec with authentication only, 3) IPSec with encryption only and 4) IPSec with both encryption and authentication. It clear that the voice packets drop starts from 622.7 packets/sec in the Baseline scenario, and from 511 packets/sec in IPSec with authentication only scenario. In IPSec with encryption only scenario, it starts to drop from 476.8 packets/sec, and finally it starts to drop from 443 packets/sec in IPSec with both encryption and authentication scenario. So it observed the voice packet drop in VoIPSec network starts before Baseline network is due to the overhead that IPSec introduces for voice conversations, this decrease the throughput in VoIPSec networks.

As shown in Table 4, it can be seen that the voice packet loss of IPSec with encryption and authentication is lower than Baseline network by around 29%. The average value of jitter for four scenarios is given in Table 4.

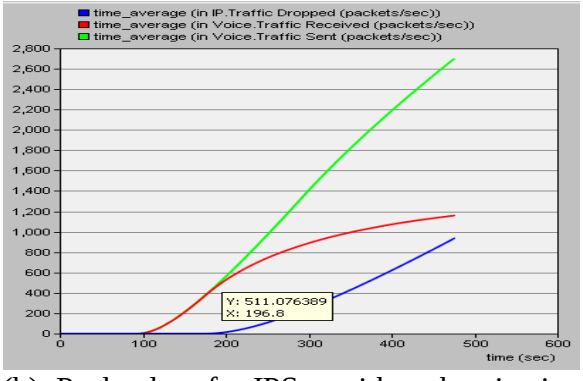
The early packet drops in VoIPSec networks, in which encryption and authentication services are employed, indicate that VoIP calls cannot be established with acceptable voice quality after 197, 192 and 187 seconds, respectively for the last three compound scenarios. VoIP calls that are established after 187 seconds almost suffer from information loss because of the packet loss which causes voice breaks and skips.

Table 4. The average values of voice packet loss (packets/sec)

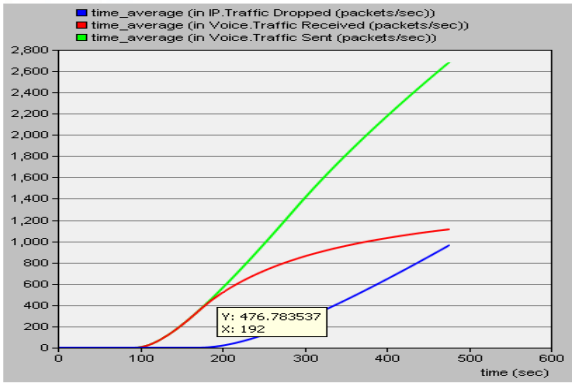
Scenario name	packet loss
Baseline	622.717
IPSec with authentication	511.076
IPSec with encryption	476.784
IPSec with encryption and authentication	443.010



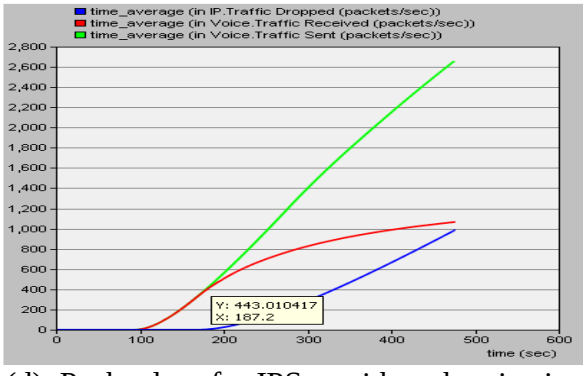
(a): Packet loss for baseline scenario



(b): Packet loss for IPSec with authentication scenario



(c): Packet loss for IPSec with encryption scenario



(d): Packet loss for IPSec with authentication and encryption scenario

Figure 7. Voice packet loss for different scenarios

5.4 *Calculating Maximum Number of VoIP Calls*

As explained in the Section 4, in order to establish VoIP calls with acceptable voice quality, end-to-end delay in a VoIP network should not exceed the threshold value of 150 milliseconds [27]. For this purpose, we need to estimate the maximum number of VoIP calls that can be maintained with acceptable voice quality. We used the end-to-end delay graph shown in Figure 5 to estimate the number of VoIP calls that can be maintained in the four scenarios. Figure 5 (a, b, c, and d) shows the end-to-end delay of four scenarios.

As shown in Figure 5a, the baseline scenario, it is clear that the end-to-end delay crosses the threshold value of 150ms at 226 seconds. From the Figure 5b, the second scenario, it is clear that the end-to-end delay crosses the threshold value of 150ms at 197 seconds. From the Figure 5c, third scenario, it is clear that the end-to-end delay crosses the threshold value of 150ms at 192 seconds, and from the Figure 5d it is noticed that in IPSec with encryption and authentication, the end-to-end delay crosses the threshold value of 80ms at 187 seconds.

In the simulation of this paper, the Application Definition and Profile Definition have been configured with VoIP calls that have been added to the network by this configuring. According to that, each call is added every 5 seconds. The addition of calls begins at the second number 100 of the simulation and continue to end of simulation. This starting point has been chosen because the start time of applying VoIP application between source and destination starts at the second number 100 of the simulation. In each scenario the total number of established calls is given by calculating total simulation time (e.g. from 100 to 475 seconds). Since one call is added to the network every 5 seconds, the total number of calls maintained in the network can be estimated by Eq(1) as follows:

Number of total number of calls =total simulation time / 5 seconds Eq(1)

So, as Eq(1) the number of VoIP calls established in each scenario (475-100) / 5 = 75 VoIP calls.

Furthermore, the maximum number of calls maintained in four scenarios with acceptable voice quality can be calculated as the following:

- ***In Baseline scenario***

Around 226 seconds (see Figure 5a) the threshold is reached (i.e., 80 milliseconds), VoIP calls calculated are from 100 to 226 seconds, as a VoIP call for every 5 seconds is added. Therefore, the maximum number of VoIP calls maintained with acceptable voice quality in baseline scenario is: (226 - 100) / 5 = 25 VoIP calls with acceptable voice quality.

- ***In IPSec with authentication scenario***

The maximum number of VoIP calls maintained with acceptable voice quality is (see Figure 5b): (197 – 100) / 5 = 19 VoIP calls with acceptable voice quality.

- ***In IPSec with encryption scenario***

The maximum number of VoIP calls maintained with acceptable voice quality is (see Figure 5c): (192 - 100) / 5 = 18 VoIP calls with acceptable voice quality.

- ***In IPSec with encryption and authentication scenario***

As shown in Figure 5d, the maximum number of VoIP calls maintained with acceptable voice quality is: (187 - 100) / 5 = 17 VoIP calls with acceptable voice quality.

The maximum number of calls maintained for each scenario with acceptable voice quality is illustrated in Table 5.

Table 5. The maximum number of calls

Scenario name	Maximum Number of Calls
Baseline	25
IPSec with authentication	19
IPSec with encryption	18
IPSec with encryption and authentication	17

The calls calculated in the four network models scenarios are varied depending on traffic conditions and security services.

6. Conclusion

This paper conducts a new approach for QoS of VoIP over IPSec network. The approach called QSVoIP calibrates QoS and security parameters of Voice transmission over IPSec to determine the maximum number of calls with acceptable voice quality. The QSVoIP approach has been implemented and executed using OPNET simulator and the performance of the approach has been evaluated and compared for different simulation scenario in terms of end-to-end delay, jitter, and packet loss. Simulation results show that transmitting voice over IPSec dramatically deteriorate quality of VoIP. As shown by the results, QSVoIP approach can effectively help network administrators/designers determining the number of voice calls that can be maintained for a given network with acceptable voice quality. As a future work, researchers can the network support and readiness of deploying other popular real-time network services such multimedia, video, and web conferencing. Finally, experiments can be performed with other types of real-time traffic to see whether the results presented in this paper can be generalized to all real-time traffic are part of future work.

References

[1] Sotillo S. Zfone: " A New Approach for Securing VoIP Communication" , ICTN 4040, 2006. - P. 13.

[2] K. Bhumip, " Implementing voice over IP" . John Wiley & Sons, Inc, 2003.

[3] Jong-Moon Chung, Elie Marroun, Harman Sandhu, and Sang-Chul Kim " VoIP over MPLS Networking Requirements" , ICN 2001, LNCS 2094, pp. 735– 744, 2001.

[4] BUR GOODE, " Voice Over Internet Protocol (VoIP)" , PROCEEDINGS OF THE IEEE, VOL. 90, NO. 9, SEPTEMBER 2002.

[5] D. Rizzetto, & C. Catania, " A Voice over IP Service Architecture for Integrated Communications" , IEEE Internet Computing, Volume 3, Issue 3, Pages: 53 – 62, 1999.

[6] Skype official website: http://about.skype.com/

[7] Google Talk URL: http://www.google.com /talk/

[8] Skype official website: http://about.skype. com/

[9] S. K. Das, E. Lee, K. Basu, & S. K. Sen, " Performance Optimization of VoIP Calls over Wireless Links Using H.323 Protocol Computers" , IEEE Transactions, Vol. 52, No. 6 Page(s):742 – 752, 2003.

[10] G. A. Thom, " H.323: the multimedia communications standard for local area networks" , Communications Magazine, IEEE, Volume 34, Issue 12, page(s): 52-56, 1996.

[11] L. Hong, & P. Mouchtaris, " Voice over IP signaling: H.323 and beyond. Communications Magazine, IEEE, Volume 38, Issue 10, Page(s):142 – 148, 2000.

[12] L. Milandinovic, & J. Stadler, " Multiparty Conference Signaling using SIP" , International Network Conference, 2002.

[13] T. Nguyen, F. Yegenoglu, A. Sciuto, & R. Subbarayan, " Voice over IP Service and Performance in Satellite Networks" , IEEE Communications Magazine, Volume: 39, Issue 3, page(s): 164-171, 2001.

[14] W.C. Hardy, " QoS Measurement and Evaluation of Teleocmmunication Quality of Service" , John Wiley & Sons, 2001.

[15] W.C. Hardy, " VOIP Service Quality: Measuring and Evaluating Packet-Switched Voice" , McGraw-Hill, 2003.

[16] Han-Chieh Chao, Y. M. Chu, & G. Tsuei, " Codec Schemes Selection Rim" , Conference on Multimedia: Advances in Multimedia Information Processing. Pages: 622 – 629, 2001.

[17] K.Salah and A.Alkhoraidly, " An OPNET-based simulation approach for deploying VoIP" , INTERNATIONAL JOURNAL OF NETWORK MANAGEMENT Int. J. Network Mgmt 2006; 16: 159– 183.

[18] P. Curry, J. Hagedorn, J. Hermanowicz, and M. Sparks, " Synchronized Voice Broadcast Over Congested IP Networks" , Dec. 1, 2007.

[19] Jitter. Available: http://www.en.VoIPforo.com/QoS/QoS_Jitter.php

[20] S. Kemp, E. Eng and A. Hassanali, BlueS.E.A. Semester Research Project. Available:

[21] http://itom.fau.edu/jgoo/fa05/ISM4220/Blusea.pdf.

[22] Noise and Voice Quality in VoIP Environments. Available: http://cp.literature.agilent.com/litweb/pdf/5988-9345EN.pdf.

[23] X. Chen, C. Wang, D. Xuan, Z. Li, Y. Min and W. Zhao, " Survey on QoS Management of VoIP" , Feb.. 03 2003.

[24] S. Kent and R. Atkinson. Security Architecture for the Internet Protocol., IETF RFC 2401, November 1998.

[25] D. Nguyen and J. Lequang, " cRTP Performance Enhancement" , Cisco System [ENG102721], 2002.

[26] "RFC 4306 IKE Version 2". Internet Engineering Task Force (IETF).

[27] S. Kent (BBN Corp) and R. Atkinson (@Home Network), "RFC 2402 IP Authentication Header". Internet Engineering Task Force (IETF). http://www.ietf.org/rfc/rfc2402.txt.

[28] S. Kent (BBN Corp) and R. Atkinson (@Home Network). ""RFC 2406 IP Encapsulating Security Payload (ESP)"". Internet Engineering Task Force (IETF). http://www.ietf.org/rfc/rfc2406.txt.

[29] US National Bureau of Standards, " Data Encryption Standard" , Federal Information Processing Standard (FIPS) publication 46-2, Dec. 1993, http://www.itl.nist.gov/fipspubs/ fip46-2.htm.

[30] R. Rivest, " The MD5 Message-Digest Algorithm" , RFC1321, Apr 1992.

[31] C. Madson, and R. Glenn, " The Use of HMAC-MD5-96 within ESP and AH," RFC 2403, Nov. 1998.

[32] R. Barbieri, D. Bruschi, E Rosti, " Voice over IPsec: Analysis and Solutions" . Proceedings of the 18th Annual Computer Security Applications Conference, Dec. 2002.

[33] Gouda I.Salama, M. Elemam Shehab, and A. A. Hafez, M. Zaki, " Performance Analysis of Transmitting Voice over Communication Links Implementing IPsec" , International Conference on AEROSPACE SCIENCES & AVIATION TECHNOLOGY, 2002. Proceedings. 13th Annual, 2009, Paper: ASAT-13-CE-13.

[34] T. Adomkus, E. Kalvaitis. " Investigation VoIP quality of service using SRTP protocol" , Electronics and Electrical Engineering. – Kaunas: Technologija, 2008. No. 4(84). – P. 85-88.

[35] Mohan Krishna Ranganathan & Liam Kilmartin, " Performance analysis of secure session initiation protocol based VoIP networks" , Communication and Signal Processing Research Unit, Department of Electronic Engineering, National University of Ireland, University Road, Galway, Ireland- P552– 565, 2002.

[36] A Simulation with OPNET. Retrieved July 12, 2017.

[37] Optimum Network Engineering Tool (OPNET). "http://www.opnet.com", 2017.

[38] Marcos Portnoi, Joberto S.B.Martins TARVOS – an Event-Based Simulator for Performance Analysis, Supporting MPLS, RSVP-TE, and Fast Recovery" , CoRR abs/1401.7034, 2014.

[39] Bernard Fortz, Jennifer Rexford, Mikkel Thorup, " Traffic Engineering With Traditional IP Routing Protocols" , Journal IEEE

[40] Communications Magazine, Volume 40 Issue 10, October 2002 Pages 118-124

[41] G.114: One-way Transmission Time, ITU-T Recommendation, G Series, 2000.

[42] Lazzez, Amor. (2014). Securing VoIP Systems: A QoS-Oriented Approach. International Journal of Computer Science Issues. 11. 99-108.

[43] Sevcik, Lukas & Uhrin, D & Frnda, Jaroslav & Vozňák, Miroslav & Toral-Cruz, Homero & Mikulec, M & Jakovlev, Sergej. (2015). Encryption for confidentiality of the network and influence of this to the quality of streaming video through network. Proceedings of SPIE - The International Society for Optical Engineering. 9497. 10.1117/12.2177555.

[44] A. Mazalek, Z. Vranova and E. Stankova, "Analysis of the impact of IPSec on performance characteristics of VoIP networks and voice quality," International Conference on Military Technologies (ICMT) 2015, Brno, 2015, pp. 1-5.

[45] Sahel Alouneh1, Sa'ed Abed, and George Ghinea, "Security of VoIP traffic over low or limited bandwidth networks", SECURITY AND COMMUNICATION NETWORKS, Security Comm. Networks 2016; 9:5591–5599, Published online 8 January 2017 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1719.

[46] H. Schulzrinne, S. Casner, R. Fredrick, and V. Jacobson. " RTP: A Transport Protocl for Real-Time Applications" . RFC 1889, July. 2003.

[47] Kolahi, Samad & Mudaliar, Keysha & Zhang, Cheng & Gu, Zhizhong. (2017). Impact of IPSec security on VoIP in different environments. 979-982. 10.1109/ICUFN.2017.7993945.

[48] Amirisetti, Sushma & Sanguankotchakorn, T.. (2018). Implementation of IPsec VPN with SIP Softphones using GNS3. 152-156. 10.1145/3301326.3301333.

[49] Piotr Lubkowski, Rafal Polak, Robert Sierzputowski, Dariusz Laskowski (2019), " Assessment of voice call quality in SCIP encrypted traffic" , Conference: XII Conference on Reconnaissance and Electronic Warfare Systems, March 2019.

journal homepage:ojs.www.sabauni.net

Article

Comparative Study of TCP Performance Scenarios over mmWave in 5G Cellular Networks

Fuaad Abdulrazzak*, Eftekar Abdulaziz, Khalid Al-Hussaini
Department of Information Technology, Thamar University, Thamar, Yemen

Article info

Article history:

Accepted: Dec. 2018

Keywords:
mmWave 5G congestion control packet size

Abstract

The millimeter wave (mmWave) is one of the major innovations of the fifth generation (5G) of cellular networks, due to the potential multi-gigabit data rate given by large amounts of available bandwidth. This article provides a comprehensive scenarios of TCP performance in 5G considering various factors such as the TCP congestion control and TCP packet size.

* Corresponding author: Fuaad Abdulrazzak
E-mail: fuaad.abdulrazzak@gmail.com

All Rights Reserved © 2019 Saba Journal of Information Technology and Networking, Published by Saba University.

1. Introduction

End-to-end connectivity over the Internet largely relies on transport protocols that operate above the network layer. The most widely used Control Protocol (TCP), to offer reliable packet delivery and sending rate control to prevent congestion in the network [10].

Majority of applications and services in the Internet using TCP what results that more than 90 percent of traffic on the Internet is handled by TCP [19]. Thus, TCP controls of bytes and packets transmitted over the Internet, so to satisfy user needs and to provide quality of service (QoS) in modern networks predict TCP behavior and optimize its performance in different environments is very important. To predict the behavior of TCP in mmWave systems, we need to evaluate its performance. TCP performance assessment can be divided into empirical studies and analytical modeling. Although analytical modeling is exceptionally accurate and useful to try different scenarios by changing parameters.

However, the next generation of cellular networks will present new challenges for TCP, specifically related to millimeter wave (mmWave) links, this technology is seen as a promising enabler for the fifth generation (5G) targets of multi- gigabit-per-second data rates and ultra-low latency [11].

In this paper, we compare the performance of TCP between different scenarios describe the end-to-end evaluation of TCP performance in 5G mmWave cellular networks through Some recent studies have highlighted that the extreme variability of the signal quality over mmWave links yields either degraded TCP goodput and very low utilization of the resources at mmWave frequencies, or, in the presence of link-layer retransmissions, high goodput at the price of high latency.

The rest of this paper is organized as follows, we first describe the scenarios of end-to-end evaluation of TCP performance. Then we compare between these scenarios through algorithm, parameters and simulator. We conclude this article in last section.

2. Overview of TCP Performance Scenarios

Because TCP is the most widely used transport proto- col, it is important to understand the interactions that exist between mobile networks (for example, wireless channels) and the TCP performance. In wireless networks, the loss of a packet is not caused necessarily by congestion, instead might be due to a sudden (and possibly only temporary) drop in the signal quality.

Current and future mobile networks deploy different retransmission mechanisms to mitigate the effects of packet loss and increase the mobile devices, throughput. When using mmWave links, these retransmission protocols become a key element in hiding the highly dynamic and consequently unstable behavior of the channel to higher layer transport protocols such as TCP.

2.1 End-to-End Evaluation Scenario

In this section describe four scenarios about end-to-end evaluation of TCP performance in 5G mmWave cellular networks. The poor radio propagation and sensitivity to blockages at higher frequencies presents major challenges, which is why much of the current research is focused at the physical layer. However, innovations will be required at all layers of the protocol stack to effectively utilize the large air link capacity and provide the end-to-end performance required by future networks. The authors in [1] and [2] and [3] and [4] present the current state of the mmWave module for ns-3 with the LTE LENAmodule, radio stack and core network to evaluate cross-layer and end-to-end performance of 5G mmWave networks. They provide an overview of the module and discuss a number of enhancements and added features, such as improved statistical channel model derived from 28 GHz channel measurements as well as a new ray tracing-based model. In addition to, provide some example simulations showing (i) the capacity of a TDMA mmWave cell with multiple users and (ii) the performance of TCP for a single user under varying channel conditions.

2.1.1 NewReno

The scenario in [1] where 3 buildings are distributed between BS and UE. The number of antennas at the BS and the UE is 64 and 16, respectively. The user starts moving at a speed of 1.5 m/s 2 seconds after the start of the simulation and stops after 20 seconds. As expected, the Signal to Interference and Noise Ratio (SINR) is constant over time while the user is static (0-2 s and 22-25 s). However, the SINR varies over time when the user is in motion. The sudden SINR jumps result from the switching of the channel state, the channel matrices are updated after a fixed 100 ms intervals for the non-Los (NLoS) channel and remain unchanged for line-of-sight (LoS) transmissions.

The scenario in [2] and [3] where 6 buildings are distributed between BS and UE. UEs are uniformly distributed at distances between 10 to 150 meters from the serving BS and can have either LOS or NLOS links. The authors consider a simple traffic model with Poisson arrivals where each UE sends small 100-byte packets at an average rate of 10 Mb/s, as well as a separate, higher throughput case where 1000-byte packets are sent at a rate of 100 Mb/s. They simulate the performance for between 10 to 100 UEs for the 10 Mb/s (per UE) arrival rate and between 1 and 10 UEs for the 100 Mb/s case, equivalent to a total IP-layer arrival rate of between 100 to 1000 Mb/s in both cases.

2.1.2 Cubic

The scenario in [4] no TCP retransmissions is triggered thanks to lower layer retransmission schemes. Nonetheless, the authors would like to observe how different TCP variants, namely NewReno and Cubic, react to link failures that can cause a retransmission timeout (RTO) expiration. To do so, they forced two outage events, of length 0:4 and 1 s, respectively.

In [5] the authors consider two different simulation scenarios, with different end-to-end transport protocols.

In the first, they deploy five base stations, in the center and at the four vertices of a square of side 200 m. NUE $\epsilon\{2,5,10\}$, users are randomly placed in a disc around each base station, for total of 10, 25 or 50 users. The base stations use a round robin scheduler. User Datagram Protocol(UDP) is used as transport protocol to access data in a remote server, at a maximum rate of 400 Mbit/s per user. For the 3GPP channel model the selected scenario is Urban Macro. The results are averaged over 20 independent runs, each with a simulated time of 10 s.

The second scenario, instead, involves a single user, three mmWave and one LTE base stations. The user moves in the scenario along a straight line for 100 m, and hands over between the different base stations. TCP NewReno is used as transport protocol, and the results for the throughput and latency with different RLC buffer sizes Brlc $\epsilon\{1,10,20\}$ MB and channel models. The 3GPP channel model has higher throughput and latency with respect to the simple model, even though for a small buffer size Brlc =1MB the performance is similar. For both channel models latency and throughput increase with the buffer size, but the latency increase is higher with the 3GPP model.

2.2 End-to-End Enhancing (TCP Proxy) scenarios

In this section will discuss the scenarios related about TCP proxy for 5G mmWave cellular networks and how to enhance TCP proxy for exploits the high variability in bandwidth of mmWave channels in LOS-NLOS transitions.

2.2.1 NewReno

In [6] the authors propose a novel TCP design for mmWave communications, ammWave performance enhancing proxy (mmPEP), enabling not only to overcome TCP performance collapse, but also exploit the properties of mmWave channels. The base station installs the TCP proxy to operate the two functionalities called Ack management and batch retransmission.

They consider a down link network consisting of a server, a mobile, and a base station. The server and the mobile are at the end of the links as TCP sender and TCP receiver respectively. The base station is located at the boundary between wired and wireless links. They assume that the wired link is error-free, to focus more on the impact of wireless channels. The server and the mobile use conventional TCP. When the mobile receives a data packet from the server, it forwards an Ack packet to the server as a response to the packet reception. The Ack packet includes a sequence number that is the last in-order delivered packet to the mobile.

In [7] the authors describe TCP proxy architecture for mmWaves, called milliProxy. They focus on testing the performance of milliProxy in a single user scenario, to evaluate the responsiveness of the proxy architecture to channel variations, from LOS to NLOS and vice versa. To model them, some obstacles are randomly deployed in the simulation scenario between the gNB (which is at coordinates (25,100) m) and the UE (moving from (0,0) m to (50,0) at speed υ). As the user moves, it will experience multiple transitions, with a random duration of each LOS

Table 1 Summary of End-to-End evaluation scenarios

Reference	Algorithm	parameters	Simulator	Con.
[1]	NewReno	Buildings=3 Rate=300Mbps Antenna=64-16 RLC buffer size=3MB RTT=40m LOS=4 , NLOS=3 Time=0-25	NS-3	Multi-Gigabit Ultra-low Latency Higher Frequencies
[2] and [3]	NewReno	Buildings=6 Rate=1Gbps Antenna=64-16 RLC buffer size=10MB RTT=40m LOS=6 , NLOS=5 Time=0-25	NS-3	Delivering end-to-end Ultra-low Latency Reliable
[4]	NewReno + Cubic	Buildings=1 RTT=40m LOS=2 , NLOS=1 Time=0-25	NS-3	High Throughput Massive Bandwidth High-dimensional Antennas
[5]	Cubic	Rate=400Mbps RLC buffer size=1MB LOS=3-20 , NLOS=2-10 Time=10s	NS-3	Dual-Connectivity Multi-Gigabit

Table 2 Summary of End-to-End Enhancing (TCP Proxy) scenarios

Reference	Algorithm	parameters	Simulator	Con.
[6]	NewReno	Rate=100Mbps Frequency=28GHz Bandwidth=1GHz	NS-3	Enhances the end-to-end Rate Exploit the mmWave Channels
[7]	NewReno	Rate=3.2Gbps Frequency=28GHz Bandwidth=1GHz RLC-AM buffer size=[10,20]MB	NS-3	Maximize Throughput Minimize Latency

or NLOS phase in each different run of the simulation.
TCP proxy architecture that improves
the performance of TCP flows without any modification at the remote sender side. The proxy is installed in the Radio Access Network, and exploits information
available at the Next Generation Node Base (gNB) to maximize throughput and minimize latency.

2.3 End-to-End Effects (TCP Dynamics) scenarios

In this section will discuss the scenarios of end-to-end perspective on the effects of blockage in 5G mmWave cellular systems, and provides the most realistic modeling of blockage in an end-to-end evaluation mmWave cellular networks.

2.3.1 NewReno

In [8] the authors compare the performance of Drop-tail and CoDel queues in two scenarios, where a mobile UE is experiencing blockages from (i) other humans or (i-i) buildings. The main difference is that, with humans, the channel deteriorates slowly and the blockage lasts a short interval; on the other hand, with buildings, the link capacity drops rapidly and the blocking interval is much longer. The sender opens a FTP connection and
sends a large _le to the UE. The congestion control is TCP Cubic, with delayed ACK disabled. The maximum queue length is 50k packets. The core network latency
is 40 ms. Conversely, the dynamic receive window approach is more responsive and therefore supports higher channel utilization while mitigating the delay, thus representing a viable solution.

2.3.2 Cubic

In [9], to evaluate the end-to-end performance with blockage, the authors simulate sending TCP traffics to the UE whose mmWave channel. They use a 400 MHz bandwidth and full buffer traffic. The RLC buffer size is configured to be 5 MB and the core network round-trip delay is set to 10 ms. The measurement-based simulation illustrates how recovery from blockage depends on the path diversity and beam search.

2.4 End-to-End Performance (MP-TCP) scenarios

In this section will discuss the scenarios of multi-path transmissions improve the performance of the mmWave network, by using Multipath TCP (MP-TCP) with different congestion control algorithms.

2.4.1 Cubic

In [12] the authors performed some simulations, they considered uplink connection from a User Equipment (UE) placed at different distances from an evolved Node Base (eNB). They use Linux implementation of TCP CUBIC, with the statistical channel model, and perform Montecarlo simulations for each distance d $\epsilon\{50,75,100,150\}$m. RLC-AM introduces additional redundancy to perform the retransmissions, but, when the distance between the eNB and the UE is equal to
d = 50 m and the UE is in LOS with very high probability, these retransmissions are not actually needed, because of the low packet error rate of the channel.

2.4.2 BALIA

In [13] the authors consider whether using LTE or mmWave as a secondary subflow yields a higher throughput. When the UE has a high probability of being in LOS (that is, for d $\leq$ 50m), the solution with MP-TCP on mmWave only links outperforms SP- TCP, with a gain between 800 Mbit/s and 1 Gbit/s (about 3040 percent). The LTE link, instead, has a much smaller rate than ammWave link when d $\leq$ 50m, and therefore the throughput of MP-TCP on LTE and mmWave subflows is close to or
worse than that of the reference SP-TCP.

Table 3 Summary of End-to-End Effects (TCP Dynamics) scenarios

Reference	Algorithm	parameters	Simulator	Con.
[8]	NewReno	Rate=3Gbps RTT=40ms TCP size=15MB Time=0-10ms	NS-3	Greater Capacity Higher Channel Utilization Low delay
[9]	Cubic	Bandwidth=400MHz RTT=10ms RLC buffer size=5MB Time=0-5ms	NS-3	Reduce the effects of blockage power efficient methods

Table 4 Summary of End-to-End Performance (MP-TCP) scenarios

Reference	Algorithm	parameters	Simulator	Con.
[12]	Cubic	frequency=28GHz, 73GHz Bandwidth=1GHz	NS-3	High TCP Throughput on mmWave links Multipath TCP (MP-TCP) over multiple LTE
[13]	BALIA	frequency=28GHz Bandwidth=6GHz	NS-3	High Reliability and Availability of Communications Low-power massive MTC.

3. Conclusion

In this paper, introduced a comprehensive scenarios of TCP performance in 5G cellular networks considering various factors such as TCP congestion control and TCP packet size. So, we comparing the performance of TCP between different scenarios describe the end- to-end evolution of TCP performance in 5G mmWave cellular networks through the algorithms, parameters and simulator of each scenario and we introduced conclude about these scenarios.

References

[1] Russell Ford, Menglei Zhang, Sourjya Dutta, Marco Mezzavilla, Sundeep Rangan and Michele Zorzi, "A framework for end-to-end evaluation of 5G mmwave cellular networks in ns-3", Proceedings of the Workshop on ns-3, ACM, pp. 85-92, 2016.

[2] Russell Ford, Menglei Zhang, Marco Mezzavilla, Sourjya Dutta, Sundeep Rangan and Michele Zorzi, "Achieving ultra-low latency in 5G millimeter wave cellular networks", IEEE Communications Magazine, volume 55, number 3, pp.196-203, 2017.

[3] Marco Mezzavilla, Menglei Zhang, Michele Polese, Russell Ford, Sourjya Dutta, Sundeep Rangan and Michele Zorzi, "End-to-End Simulation of 5G mmWave Networks", arXiv preprint arXiv:1705.02882, 2017.

[4] Menglei Zhang, Marco Mezzavilla, Russell Ford, Sundeep Rangan, Shivendra Panwar, Evangelos Mellios, Di Kong, Andrew Nix and Michele Zorzi, "Transport layer performance in 5G mmWave cellular", Computer

Communications Workshops (INFOCOM WKSHPS), 2016 IEEE Conference on, IEEE, pp. 730-735, 2016.

[5]Michele Polese and Michele Zorzi, "Impact of Channel Models on the End-to-End Performance of mmWave Cellular Networks", 2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), pp. 1-5, 2018.

[6] Minho Kim, Seung-Woo Ko and Seong-Lyun Kim, "Enhancing TCP End-to-End Performance in Millimeter-Wave Communications", 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1-5, 2017.

[7] Michele Polese, Marco Mezzavilla, Menglei Zhang, Jing Zhu, Sundeep Rangan, Shivendra Panwar and Michele Zorzi, "milliProxy: a TCP Proxy Architecture for 5G mmWave Cellular Systems", 2017 51st Asilomar Conference on Signals, Systems, and Computers, IEEE, pp. 951-957, 2017.

[8] Menglei Zhang, Marco Mezzavilla, Jing Zhu, Sundeep Rangan and Shivendra Panwar, "TCP Dynamics over mmWave Links", 2017 IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), pp. 1-6, 2017.

[9] Christopher Slezak, Menglei Zhang, Marco Mezzavilla and Sundeep Rangan, "Understanding End-to-End E_ects of Channel Dynamics in Millimeter Wave 5G New Radio", 2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), pp.1-5, 2018.

[10] Menglei Zhang, Michele Polese, Marco Mezzavilla, Jing Zhu, Sundeep Rangan, Shivendra Panwar and Michele Zorzi, "Will TCP Work in mmWave 5G Cellular Networks?", IEEE Communications Magazine, volume 57, number 1, pp. 65-71, 2019.

[11] Ming Xiao, Shahid Mumtaz, Yongming Huang, Linglong Dai, Yonghui Li, Michail Matthaiou, George K Karagiannidis, Emil Bjornson, Kai Yang and I Chih-Lin, "Millimeter wave communications for future mobile networks", IEEEJournal on Selected Areas in Communications, volume 35, number 9, pp. 1909-1935, 2017.

[12] Michele Polese, Rittwik Jana and Michele Zorzi, "TCP in 5G mmWave networks: Link level retransmissions and MP-TCP", 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 343-348, 2017.

[13] Michele Polese, Rittwik Jana and Michele Zorzi, "TCP and MP-TCP in mmWave 5G Networks", IEEE Internet Computing, 2018.

[14] Drozdy rpd, Jouko Kapanen, and Jukka Manner, "User level performance analysis of multi-hop in-band backhaul for 5G", Wireless Networks 24, no. 8 pp. 2927-2941, 2018.

[15] Krmer Zsolt, Sndor Molnr, Szilrd Solymos and Attila Mihly, "On the Bene_ts of Multi-Domain Congestion Control in LTE Networks", In 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 1-6, 2019.

[16] Michele Polese and Michele Zorzi, "Impact of Channel Models on the End-to-End Performance of mmWave Cellular Networks", In 2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), pp. 1-5, 2018.

[17] Dong Pingping, Jingyun Xie, Wensheng Tang, Naixue Xiong, Hua Zhong, and Athanasios V. Vasilakos, "Performance Evaluation of Multipath TCP Scheduling Algorithms", IEEE Access 7 pp. 29818-29825, 2019.

[18] Dong Pingping, Kai Gao, Jingyun Xie, Wensheng Tang, Naixue Xiong, and Athanasios V. Vasilakos, "Receiver-Side TCP Countermeasure in Cellular Networks", Sensors 19, no. 12, 2019.

[19] Kumar Vinay, Sadanand Yadav, D. N. Sandeep, S. B. Dhok, Rabindra Kumar Barik, and Harishchandra Dubey, "5g cellular: Concept, research work and enabling technologies", In Advances in Data and Information Sciences, pp. 327-338. Springer, Singapore, 2019.

[20] Arunachalam Karthikeyan, YoungKi Hong, Wonbo Lee, and Jamsheed Manja Ppallan, "Low Power TCP for Enhanced battery life in mobile devices", In ICC 2019-2019 IEEE International Conference on Communications (ICC), pp. 1-7, 2019.

[21] Shurman Mohammad, Eyad Taqieddin, Omar Oudat, Ra_ Al-Qurran, and Abd Alrahman Al Nounou, "Performance Enhancement in 5G Cellular Networks Using Priorities in Network Slicing", In 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), pp. 822-826, 2019.

[22] Bisu Anas A., Andrew Gallant, Hongjian Sun, Katharine Brigham, and Alan Purvis, "Experimental Performance Evaluation of TCP Over an Integrated Satellite-Terrestrial Network Environment", In 2019 15th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 781-786, 2019.

[23] Tayyaba Sahrish Khan, and Munam Ali Shah, "Resource allocation in SDN based 5G cellular networks", Peer-to- Peer Networking and Applications 12, no. 2 pp. 514-538, 2019

[24] Okano Mayuko, Yohei Hasegawa, Kenji Kanai, Bo Wei, and Jiro Katto, "TCP throughput characteristics over 5G millimeterwave network in indoor train station", In 2019 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-6, 2019.

[25] Peng Yan, Yiqing Zhou, Ling Liu, Jinhong Yuan, Jinglin Shi, and Jintao Li, "Prediction-Based User Plane Handover for TCP Throughput Enhancement in Ultra-Dense Cellular Networks", In 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), pp. 1-5, 2019.

[26] Krmer Zsolt, Sndor Molnr, Attila Mihly, and Szilveszter Ndas, "Towards multi-domain congestion control in nextgeneration networks", In 2019 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-7, 2019.

[27] Quinlan Jason J., and Utz Roedig, "The bene_ts of Deceit: a Malicious client in a 5G Cellular Network", In 2019 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), pp. 1-2, 2019.

[28] Mateo Pablo Jimenez, Claudio Fiandrino, and Joerg Widmer, "Analysis of tcp performance in 5g mm-wave mobile networks", In ICC 2019-2019 IEEE International Conference on Communications (ICC), pp. 1-7, 2019.

[29] Zugno Tommaso, Michele Polese, Mattia Lecci, and Michele Zorzi, "Simulation of Next-generation Cellular Networks with ns-3: Open Challenges and New Directions", In Proceedings of the 2019 Workshop on Next Generation Wireless with ns-3, pp. 38-41, 2019.

[30] Michele Polese, Marco Mezzavilla, Sundeep Rangan, and Michele Zorzi, "Mobility Management for TCP in mmWave Networks", mmNets17, October 16, 2017, Snowbird, UT, USA, 2017.