World Journal of Engineering Research and Technology

WJERT

www.wjert.org

SJIF Impact Factor: 5.924

SECURE VIDEO TRANSMISSION OVER IP USING RSACRT CRYPTOGRAPHY

[*1]Hind Abdallah Osman, [2]Khalid Hamid Bilal Abdalla and [3]Afaf Mustafa Elhassan

[1]Faculty of Science and Technology, Omdurman Islamic University, Sudan.

[2,3]Department of Communication Engineering Systems, Faculty of Engineering, University of Science and Technology, Sudan.

Article Received on 08/03/2022 **Article Revised on 29/03/2022** **Article Accepted on 18/04/2022**

***Corresponding Author**
Hind Abdallah Osman
Faculty of Science and Technology, Omdurman Islamic University, Sudan.

ABSTRACT

Secure channels are required for the transmission of secret or proprietary information. Encryption is required for many secure transmission methods. This research objective study of a mechanism for building the RSACRT algorithm from the sender and receiver of these blocks of data, so that we can ensure the verification of these blocks of data. While maintaining a high degree of flow, the data transmitter and receiver. In this paper we use the RSACRT technique to encrypt video and use opnet program that simulation network to and describe the results using packet loss ratio, delay, and throughput. This paper objective in will describe how to make cryptographic calculations more secure using the RSA approach. And other advantages of using symmetric key calculations, despite legitimately corresponding with the expansion of document size.

KEYWORDS: Cryptography, Secure transmission, CRT, RSA, Multiple Channels, Block cipher.

INTRODUCTION

When sensitive information is kept and moved over the internet, where it is no longer protected by physical boundaries, security becomes a serious problem. Cryptography is a critical component for ensuring communication effectiveness and efficiency.

Secure channels are required for the transmission of secret or proprietary information. Encryption is required for many secure transmission methods. Other transmission mechanisms are used to exchange keys in order to open an encrypted file. Encryption is a cryptographic primitive that is commonly used to secure data confidentiality. If q0, q1...qk -1 are k pairwise relatively prime positive integers and a0, a1...ak -1 are positive integers, then there exists exactly one integer a where 0 a q for q=k-1 i=0 qi and a = ai mod qi for 0 I k, according to the Chinese remainder theorem CRT . The moduli are the integers q0, q1...qk -1, while the residues are the integers a0, a1...ak -1. The CRT has a long history of use in both secret sharing and error correction codes .In this paper, RSA encryption will be paired with the Chinese remainder theorem to create a technique for sending sensitive data over numerous channels. Parallel transmission is the simultaneous transmission of similar signal elements over two or more distinct pathways in digital communications. Multiple cables are employed, each of which can send multiple bits at the same time, allowing for faster data transfer speeds than serial transmission.[1,2] RSA (which stands for Rivest, Shamir, and Adleman, who were the first to describe it publicly) is an asymmetric public key cryptography algorithm. Video-over-IP (VoIP) is a method of sending video from one device to another over a computer network that is connected to the internet.IP stands for Internet Protocol, and it refers to the methods or protocols that are used to transfer data between two or more devices. The Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) are the two fundamental transmission protocols in the TCP/IP protocol stack (UDP). Real-time Transport Protocol is used by applications that stream real-time audio and video over IP (RTP).Video over Internet Protocol is a method of transmitting video signals to end users using audio and image data.[3] It is one of the most essential communication technologies in the world. After almost 20 years of investigation, some of the issues are still present. Multi-media over IP has numerous issues due to the loose nature of wireless networks. Issues such as allocating bandwidth for calls, having secure communications, and providing acceptable Quality of Service (QoS) are more complex than with a wired LAN.[4] As a result, secure video over IP networks continues to be a difficult research topic .In the realm of telecommunication, video over IP applications have seen the most rapid growth. It is used for both short-term and long-term speech and audio traffic transmission. The RSA algorithm is a type of asymmetric cryptography. It's asymmetric because it uses two separate keys: a Public Key and a Private Key.[2],[5] The Public Key is given to everyone, whereas the Private Key is kept private, as the name implies.

I. RSACRT cryptography algorithm

Between the transmitter and the receiver, R number of multiple transmission channels are used, from which S channels are chosen using some selection criteria. The plain text or original message is divided into N bits of cipher blocks. An RSA-CRT module is used to encrypt these blocks. The encrypted information is sent through a set of S-chosen channels. In order to prevent attackers from hacking, the remaining R-S channels are employed to broadcast irrelevant data.[7] The inverse of the RSA-CRT is applied to the original N-bit cipher block received through S-channels at the receiver end, and then the decode module is employed to recover the original message or plain text.The receiver is informed of the selected S-channels prior to encrypted data transmission. The data received through R-S channels is discarded at the receiving end.[8] The plain text is spewed out in blocks of equal size. After implementing RSA-CRT modifications, these blocks of data are delivered to the target destination across several channels.

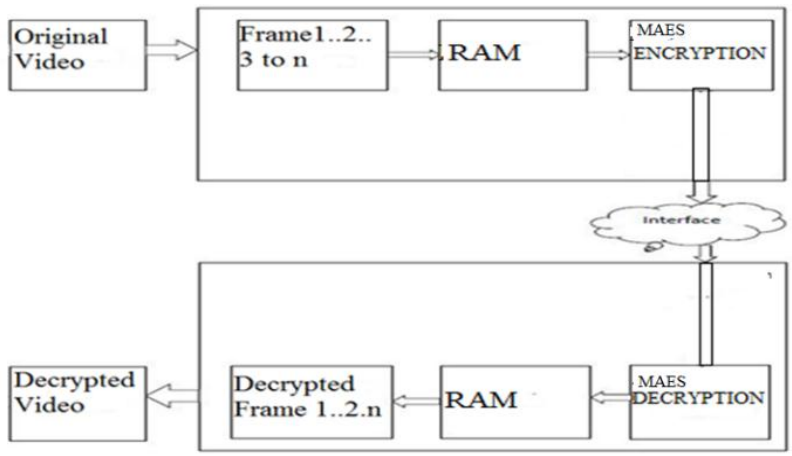

Figure 1: Block Diagram.

1. Phase of the Session

During transmission, two different sessions are carried out. The first session begins before the transmission, whereas the second begins after the transmission has completed. The first session is referred to as the sender session, while the second is referred to as the receiver session.

2. Session with the Sender

The steps followed by the sender process are as follows: 1. Data or message M is partitioned into blocks upon arrival for transmission. 2.After executing the RSACRT transformation, the partitioned block is sent. 3. Send the modified data across the S channels you've chosen. 4.

Until data is ready to send, the sender function waits for more input. A blocked phase exists on the sender side.

3. Sessions with the receiver

Following are the steps that the receiver process performs: The first step is to choose the channels. 2. The receiver process awaits information from several channels during this step. This is a block operation. 3. Each channel's received data is kept in its own block. The inverse module of the RSACRT transformation is used to decrypt these blocks.

4. Selecting a Channel

The transmission channels S, which are a subset of R, are chosen based on a number of factors, including network traffic, congestion occurrence, and previous network failures. Irrelevant data is sent across the R-S transmission channels. A stream of pre-determined bits is added to blocks of data before transmission on R-S channels to identify unnecessary material.

5. The total number of channels

With a max constraint on the max, the maximum number of channels max(S) used for transmission is based on the number of blocks to be communicated (S).

6. RSA's Chinese Reminder Theorem

Decryption is substantially faster when the Chinese Reminder Theorem (CRT) is used. In terms of key generation and decryption, the RSA-CRT differs from the regular RSA.

7. Generate RSA-CRT keys

We can claim that the security is maintained in this technique of transferring data using many channels and RSA-CRT since intruders may be able to crack the encrypted method utilizing the long permutation method. As a result, we can confidently assert that data transmitted across numerous channels will be more secure than data transmitted over a single channel. Even though the security of the data can be preserved via serial transmission, the chances of preserving reliability are slim. That example, some users are just interested in harming the transmission's reliability, not in compromising data confidentiality. Because we're working with numerous channels in this study, the pace of change is higher. Because we are dealing with numerous channels in our paper, the rate of reliability will be higher than if we were dealing with a single channel.[9],[10],[11]

II. Mathematical perspective

A generic exponentiation of a message m to the exponent d modulo N is considered. We conduct exponentiation modulo NR, where R is a 64-bit random integer, for example. We assume N and R are coprime, which means gcd(N,R)= 1.

Table[1] network description.

Node	Class	Scheduling Type	Requested BW
UGS_ss:	Gold	UGS	16.8 Mbps
silver_A_ss:	Silver A	rtPS	2.0 Mbps
silver_B_ss:	Silver_B	rtPS	0.5 Mbps
default_ss:	System Default	BE	0.0 Mbps

Let α be such that $\begin{cases}\alpha = 0 \bmod R \\ \alpha = 1 \bmod N\end{cases}$ and β be such that $\begin{cases}\beta = 1 \bmod R \\ \beta = 0 \bmod N\end{cases}$

We can prove the existence and uniqueness of and in Z_{NR} using the Chinese Remainder Theorem. Garner's approach is used to generate these integers.

Consider R now as $R = r^2$, where r is a 32-bit random number, and we obtain the following result:

$\alpha=R.(R^{-1} \bmod N) =[N.(N^{-1} \bmod R)] \bmod NR$.

$\beta= N.(N^{-1} \bmod R) =1- [R.(R^{-1} \bmod N)] \bmod NR$.

A proof and accompanying mathematical details can be found in Appendix A. In any ring $(Z_N, +,)$, N ,Theorem 1 shows how to do a secure exponentiation[12-14],(exponentiation identity in Z_{Nr}^2) .let N and r be integers such that gcd(N,r)=1 ,let $\beta=N.(N^{-1} \bmod r^2)$ and $\alpha=1 - \beta \bmod N_r^2$ for any m € Z_{Nr}^2 and for d € N^* , $(\alpha m+\beta.(1+dr) \bmod N_r^2$.

III. Flow char RSACRT encryption algorithm[2],[9],[15]

1. Choose p and q as two huge prime numbers.
2. Multiply these integers to get n = p x q, where n is the encryption and decryption modulus.
3. Select an integer e smaller than n such that n is prime to (p - 1) x. (q -1)
4. The public key is e, n> if n = p x q.

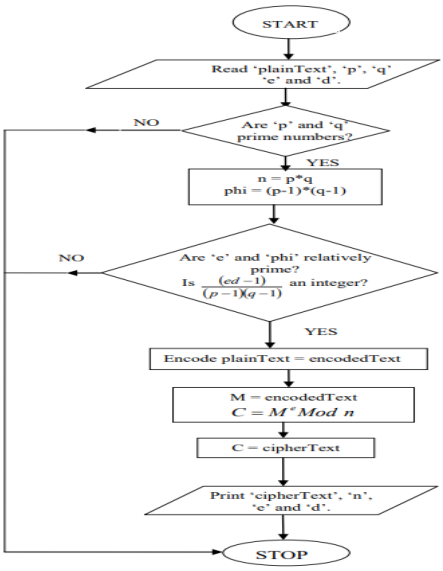

Figure 2: RSA flow chart.

IV. Simulation

This section explains how to use the RSA method in video and IP transmission, as well as how to extract and analyze video and WiMAX results using opnet simulation**.**

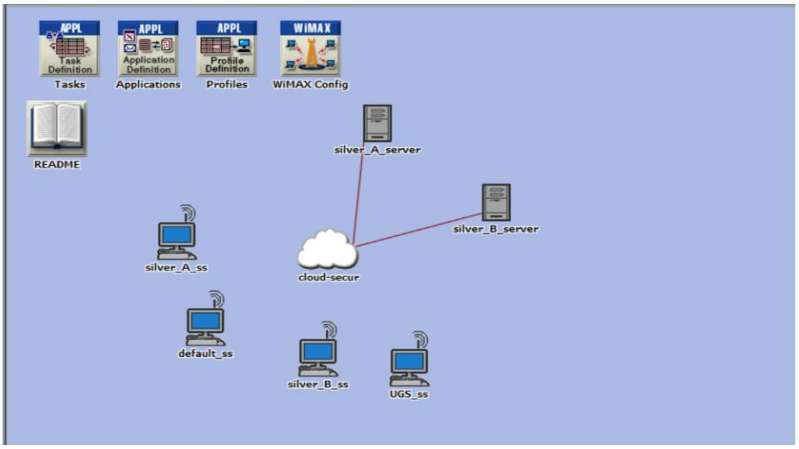

Figure 3: WiMAX architecture using RSA algorithm.

V. RESULT

By exploiting configurations presented above the following will be discussed and analyses of the obtained results through the OPNET Modeler 14.5 software. These results are gained for the case of topology shown in Fig. 3. Simulation time is limited to 60 minutes. in this paper we will discuss and analyses only the simulation results for Video applications. Restrictions on only these applications are made because of the limited number of pages for publication. On the other hand, video applications are more sensitive to delays that are caused by the network, compared with other applications.

Table 2: Parameters of network	
Parameters	**Values**
Legacy Network	IEEE 802.16a to IEEE 802.16d (For Mobile WiMAX with cloud)
Transmission Bandwidth (MHz	25
Subcarrier Spacing	15 kHz
Sampling/Base Frequency	10 GHz
Maximum transmission power (W)	0.5
Maximum traffic data Rate	5Mbps
Minimum traffic data Rate	1Mbps
No cell	1
No .BS	3
Cell Radius(Km)	2-7 km
Cell Capacity	10-100 users
Speed link	2.378 Gbps
Video frame rate	30 Fps
Video frame size	320x240 Pixels
Inter-repletion Time	Exponent ial (300) Seconds
Simulation time	1 hour

1. Video conference result

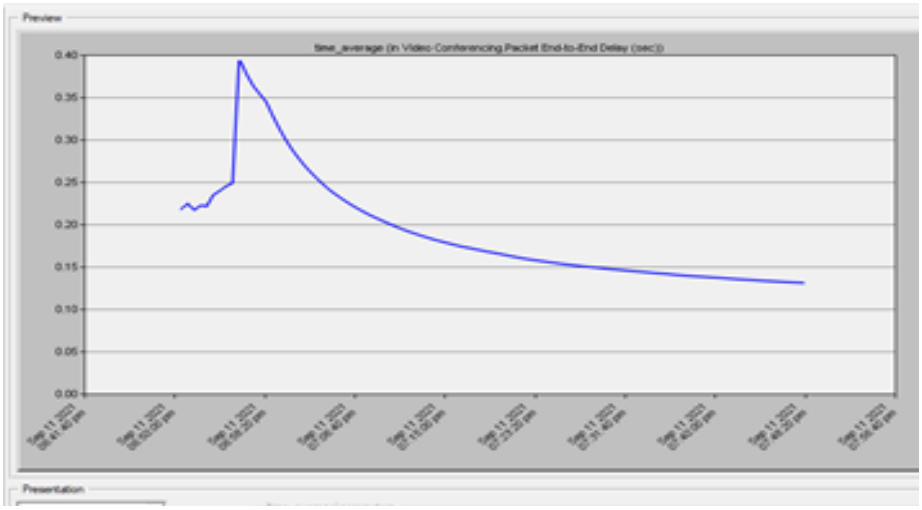

Figure 4: Video conference package delay.

Table3: explain Video Conferencing. Variation.	
Statistic	Scenario1-DES-1: Video Conferencing. Packet Delay Variation
Mean	0.000945457

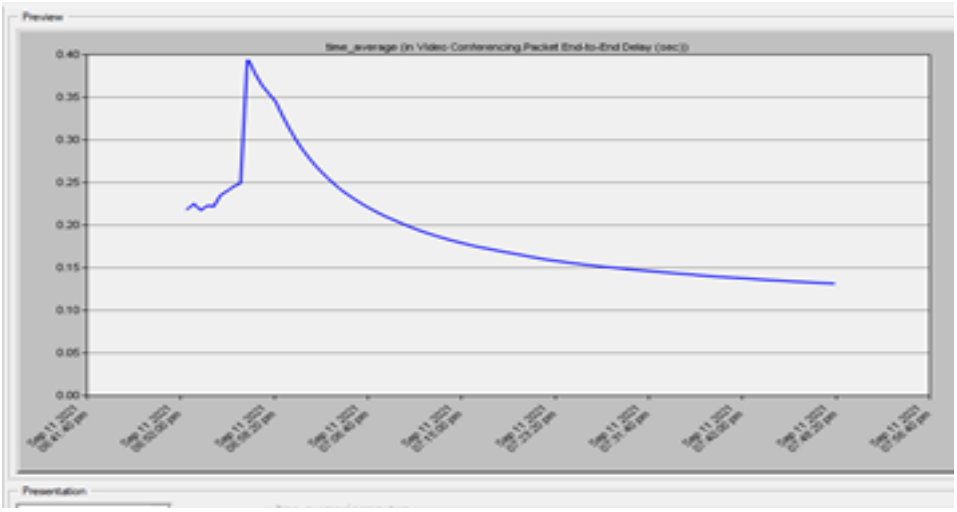

Figure 5: Video conference package end to end delay.

Table 4: explain Video Conferencing. Packet End-to-End Delay (sec)	
Statistic	Scenario1-DES-1: Video Conferencing .Packet End-to-End Delay (sec)
Video Conferencing .Packet End-to-End Delay (sec)	0.196509111

From the given figure 4and 5 it is analyzed that packet end to end mean delay in case of RSACRT cryptography algorithm's is Lowe.

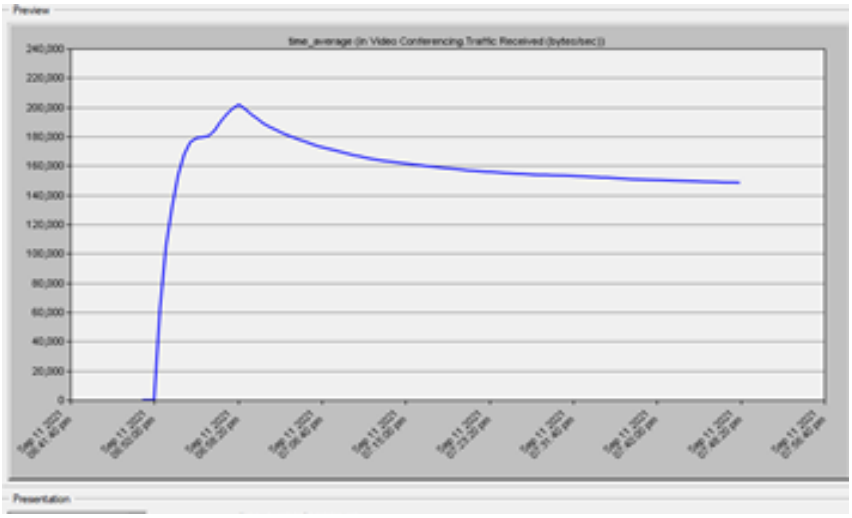

Figure 6: Video conference traffic received package (byte/sec).

Table 6: WiMAX. Load (packets/sec)	
Statistic	Scenario1-DES-1: WiMAX .Load (packets/sec)
WiMAX .Load (packets/sec)	1,545.53

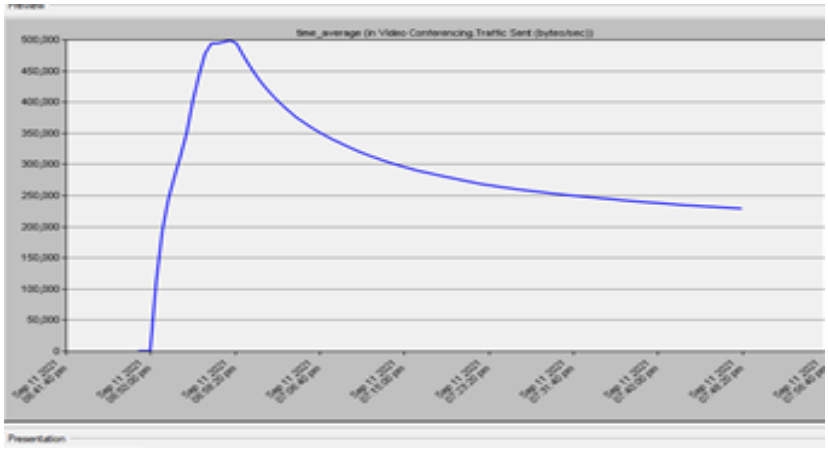

Figure 7: Video conference traffic send package (byte/sec).

Table 5: Video Conferencing. Traffic Received/send (packets/sec)				
Statistic	**Video Conferencing. Traffic Received (packets/sec)**	**Video Conferencing. Traffic Sent (packets/sec**	**Less Packets**	**Packet Loss Ratio**
Video Conferencing. Traffic (packets/sec)	15.94608671	17.1797392	1.233652	0.077363964%

Received traffic is the amount of data received by the mobile station. It can be measured in bits/sec and packets/sec. From Figure 6 it is clearly analyzed that the scheme receives less traffic than the transmission scheme. There is a packet loss rate, but it is low.

2. Result WiMAX

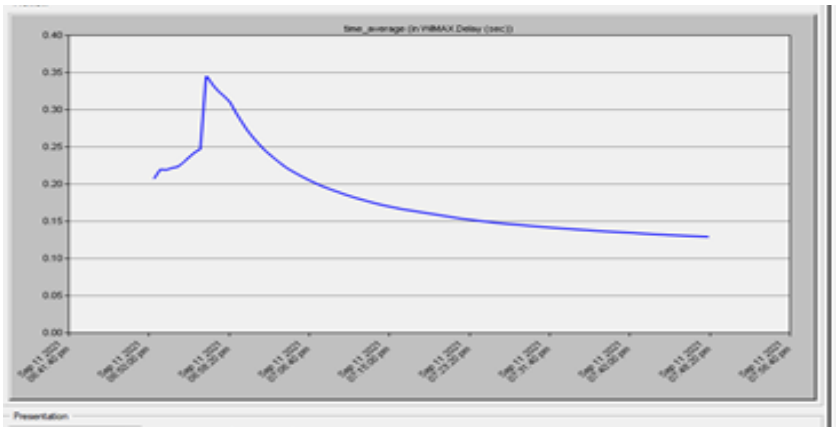

Figure 8: WiMAX delay.

Table 5: WiMAX .Delay (sec)	
statistic	scenario1-DES-1: WiMAX .Delay (sec)
WiMAX .Delay (sec)	0.194624704

From the given figure 8 it mean WiMAX delay is Lowe.

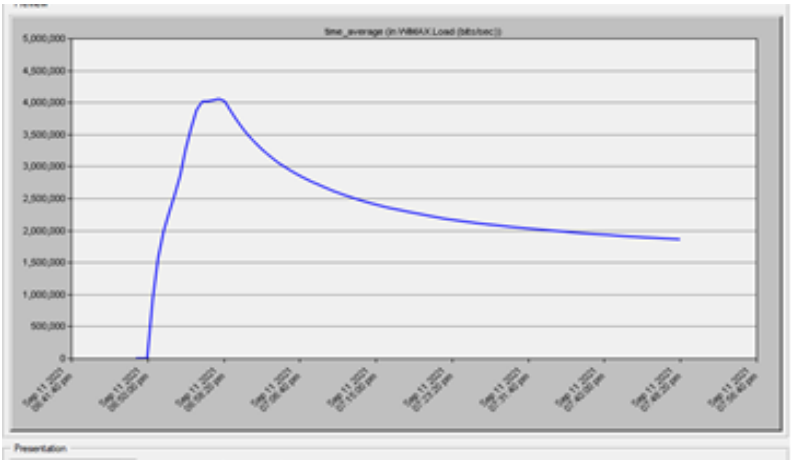

Figure 9: WiMAX load package.

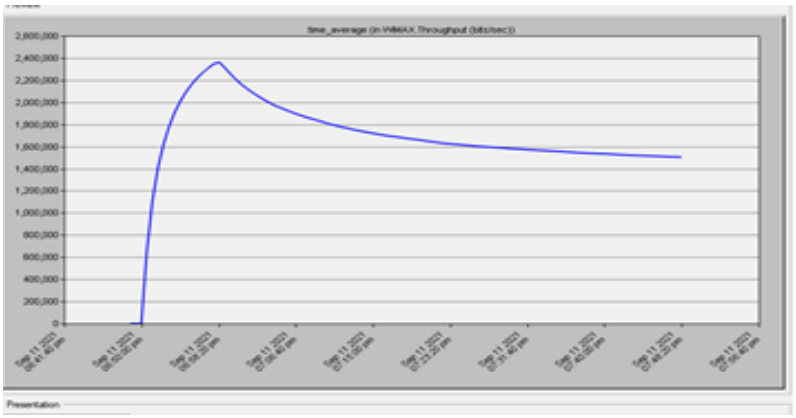

Figure 10: WiMAX throughput.

Table 7: WiMAX. Throughput (packets/sec)	
statistic	scenario1-DES-1: WiMAX .Throughput (packets/sec)
WiMAX. Throughput (packets/sec)	389.8714309

Throughput is measured in bits/second (bps) or packet/second. From the figure we can analyze that data transferred over specific time period high throughput.

3. the analysis of the results.

In this section, we'll look at the performance metrics of video transmission over IP.

- lower delay.
- Lowe packet loss ratio

4. Analyses WiMAX:

- Low delay.
- Low load.

- high throughput.

VI. CONCLUSION

In this paper, the performance analysis for QoS of video conferencing over WiMAX network using OPNET modeler 14.5 is carried out with respect to different modulation schemes. To better analyze the performance service is used RSACRT cryptography algorithm method and its application to data transmission using the opnet network simulation tool. The system is proven to be more secure by sending video across several channels for the same receiver in separate blocks, and this paper explains how to encrypt video using the RSA algorithm and send it over IP, as well as analyze the results using the opnet network program performance is good in traffic sent, load and packet end to end delay. In future, QoS parameters should be improved to get minimum delay and maximum throughput.

VII. Recommendation

Many encryption applications have been created in the past that are solely for data encryption. We infer from our research that a video encryption system has been developed, however it is not dependable, implying that it has some flaws. Recommendation from us In this thesis, novel encryption techniques are used to improve RSA.

REFERENCES

1. Pavani, K. and P. Sriramya. *Enhancing Public Key Cryptography using RSA, RSA-CRT and N-Prime RSA with Multiple Keys*. in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, 2021. IEEE.
2. Smriti, M., et al., *Secure File Storage in Cloud Computing Using a Modified Cryptography Algorithm*, in *Advancing Smarter and More Secure Industrial Applications Using AI, IoT, and Blockchain Technology*, 2022; IGI Global. p. 200-224.
3. Sinha, K., et al., *Randomized Block Size (RBS) Model for Secure Data Storage in Distributed Server*, 2021; 15(12): 4508-4530.
4. Aumasson, J.-P., *Serious cryptography: a practical introduction to modern encryption*. 2017: No Starch Press.
5. Iqbal, S., et al., *DM-GKM: A key management scheme for dynamic group based applications*, 2020; 182: p. 107476.

6. Ulz, T., et al. *Sensing Danger: Exploiting Sensors to Build Covert Channels*. in *ICISSP*, 2019.
7. Hermawan, N.T.E., E. Winarko, and A. Ashari. *Multi prime numbers principle to expand implementation of CRT method on RSA algorithm*. in *AIP Conference Proceedings*, 2021. AIP Publishing LLC.
8. Kaedi, S., et al., *A New Side-Channel Attack on Reduction of RSA-CRT Montgomery Method Based*, 2021; 30(03): 2150038.
9. HIDAYAT, R., A. Abdiansah, and M.D. Marieska, *ANALISIS PERBANDINGAN EFISIENSI ALGORITMA KUNCI PUBLIK RABIN-P DAN ALGORITMA KUNCI PUBLIK RSA-CRT PADA PENGAMANAN PESAN*. 2022, Sriwijaya University.
10. Sirait, E.Y., *Kombinasi Algoritma Rc-5 Block Cipher Dan Algoritma Rsa-Crt dalam Pengamanan File Pdf dan Docx*, 2021.
11. Hamburg, M., M. Tunstall, and Q. Xiao. *Improvements to RSA Key Generation and CRT on Embedded Devices*. in *Cryptographers' Track at the RSA Conference*. 2021. Springer.
12. Sarna, S. and R. Czerwinski. *RSA and ECC universal, constant time modular inversion*. in *AIP Conference Proceedings*. 2021. AIP Publishing LLC.
13. Lasheras, A., et al., *Securing RSA hardware accelerators through residue checking*, 2021. 116: p. 114021.
14. Mohamed, T.M., I.Z. Ahmed, and R.A.J.P.C.S. Sadek, *Efficient VANET safety message delivery and authenticity with privacy preservation*, 2021; 7: p. e519.
15. Liu, J.-J., et al., *A variant RSA acceleration with parallelisation*, 2022; p. 1-15.
16. Nasution, A.M., *Hybrid Cryptosystem dengan Algoritma Hill Cipher dan Algoritma RSA-CRT dalam Pengamanan File Teks*, 2021.