International Journal of Safety and Security Engineering
Vol. 11, No. 1, February, 2021, pp. 59-68
Journal homepage: http://iieta.org/journals/ijsse

Secure and Guarantee QoS in a Video Sequence: A New Approach Based on TLS Protocol to Secure Data and RTP to Ensure Real-Time Exchanges

Hamza Touil[1*], Nabil El Akkad[2], Khalid Satori[1]

[1] LISAC Faculty of Sciences Dhar-Mahraz (FSDM), Sidi Mohamed Ben Abdellah University, Fez 30050, Morocco
[2] Laboratory of Engineering Systems and Applications (LISA), National School of Applied Sciences (ENSA) Sidi Mohamed Ben Abdellah University, Fez 30000, Morocco

Corresponding Author Email: hamza.touil@usmba.ac.ma

https://doi.org/10.18280/ijsse.110107

Received: 14 November 2020
Accepted: 2 February 2021

Keywords:
QoS, security, AES, cypher suite, RTP, compromise, sniffing, DDOS

ABSTRACT

Much of the Internet's communication is encrypted, and its content is only accessible at two endpoints, a client and a server. However, any encryption requires a key that must be negotiated without being revealed to potential attackers. The so-called TLS (Transport Layer Security) handshake is often used for this task without obviating that many fundamental parameters of TLS connections are transmitted explicitly. Thus, third parties have access to metadata, including information about the endpoints, how the connection is used. On the other hand, QoS is considered the central part of the communication used to judge the deliverable quality through several parameters (latency, jitter ...). This document describes a secure approach and meets mainly the requirements of quality of service on a communication channel (free, loaded, congested ...), using the robustness and flexibility of the TLS protocol represented on the characteristics of existing encryption keys on its list of "ciphers suites." We focused more particularly on the AES key (Advanced Encryption Standard), including the different sizes (128,192,256), given its resistance to various classical attacks (differential, linear, ...) and its lightness compared to other protocols such as DES, 3DES ... This method is useful in continuous communications in a time axis (video sequence, VOIP call...).

1. INTRODUCTION

Security is a significant challenge in network management and the ever-increasing number of individuals connecting to the Internet. The transmission of sensitive information and the desire to ensure this information's confidentiality has become an essential point in establishing computer networks [1-5]. Therefore, it is crucial to provide a stable technical and legal framework that guarantees adequate data protection. This new trend tends to become more than a rule of competitiveness; it is becoming a genuine legal obligation to protect personal data using adequate and sufficient security measures [6].

The recent strengthening of regulatory requirements has highlighted the security issues of systems (standard, sophisticated, intelligent...), applications, etc. The latter define and implement security policies, sometimes formalized, sometimes empirical, not only to cover the purpose of the system (authentication, prevent unauthorized disclosure of data, prevent unauthorized modification of data, prevent unauthorized use of network or computer resources in general ...). But also, at the level of choice of optimal and efficient algorithms, compatible with other solutions. Furthermore, the quality-of-service strategy specifies several network attributes such as clients or applications' priority and the actions for processing different traffic categories. However, in our case, we will deal more specifically with the QOS related to multimedia. The process consists of establishing a secured connection between two interlocutors (the server that broadcasts the video sequence and a client) using an AES encryption key of 256. A step of verification of the jitter (latency variation) periodic is essential on the part of the client to make a decision:

If the jitter is within the standards [7, 8], the system must keep the encryption with the AES256 key, if not, both ends must go through an automatic and uninterrupted fast renegotiation of the video to switch to a small size AES key (192,128) to reduce the bandwidth on the channel, this operation must be repeated hastily until the end of the communication. This provides a full grasp of the security parameters to be addressed to the QoS objectives. To assess the needs in terms of security and quality of service, the proposed solution allows a compromise was found between better security and a better quality of service. Depending on the different test scenarios, the dimensions of this solution can be evaluated. However, in any case, the requirements are more critical, as they directly impact users [9-14]. In the rest of this document, we will dissect the related works. Then we will simulate the problem that led us to realize this solution and the added value of our work [15].

2. RELATED WORKS

A set of studies carried out in this context. Wei et al. [16] proposes an implementation of the TLS protocol to secure the SIP school in VOIP communications. Applying the security implementation to the existing local server by adding credentials and filtering ports. IP tables are launched for each

port to list the defined rules. QoS performance is verified after the security approaches have been applied. Balhwan et al. [17] Offers a traffic analyzer capable of analyzing encrypted traffic flows using TLS. The feature extraction phase comprises a set of uncorrelated features and combines the statistical parameters of a traffic flow with information extracted from the encrypted traffic flows' metadata. This analysis is used to provide the Quality of Service (QoS) parameters mentioned in the Service Level Agreement. Chakaravarthi et al. [18] proposes a new protocol called HTTPI that implements the TLS protocol to ensure the network check meets QoS requirements such as authentication, authorization, integrity, and confidentiality at different OSI layer levels. It also guarantees the quality of service that covers non-functional characteristics such as performance (throughput), response time, security, reliability, and capacity. This proposed intelligent agent-based model results in excellent throughput, good response time, and increases the QoS requirements. Taleb [19] proposed a framework for the quality of protection that corresponds to security and QoS requirements using a multi-attribute decision-making model. In other words, the algorithm puts the encryption keys in order of performance; then if there is degradation at the QOS level, the algorithm replaces the key with another performing month. Deals with service attacks in telecom networks are widespread and particularly severe [20]. It treats security and QoS in an integrated way using the concept of Quality of Security Service where security is considered a parameter of quality of service. This solution works very well against service attacks.

Some protocols are part of the RTP family, which can ensure a certain level of security. SRTP [21] protocol provides encryption, authentication and integrity of messages and protects against the replay of RTP data. SRTP works in both unicast and multicast mode. In addition to preventing unauthorized eavesdropping on an RTP session, users can also limit the amount of personal information they provide. It recommended that applications do not issue RTCP source description packets without first informing the user. This protocol is robust in terms of security, and this is not the case in QOS, as it performs key changes at a given time interval and does not check the QOS parameters. ZRTP [22] describes a mechanism that allows two communicating parties to exchange encryption keys securely. In order to be able to encrypt traffic using SRTP. Although it is based on using the public key encryption algorithm, it does not require PKI or any particular infrastructure. The dialogue between the two parties carried out using the RTP protocol using specific extensions. Being independent of the signalling protocol is potentially compatible with all VOIP protocols (SIP, H323, Megaco...). A client that does not support ZRTP will ignore these extensions, without impacting communications. The key exchange is done peer to peer and does not require any central server. Infrastructure independence has been a priority in the design of this protocol.

3. OVERVIEW OF PROTOCOL SSL/TLS

The purpose of the protocol is to provide secure data transmission. In this case, asymmetric encryption algorithms are used for authentication (a public-private key pair), and symmetric encryption algorithms (secret key) are used to maintain confidentiality. When a user visits a website, the browser requests certificate information from the server, and the server sends a copy of the SSL certificate together with the public key. Then, the browser checks the certificate, which must match the website's name, the validity date of the certificate, and the presence of a root certificate issued by a trusted certificate authority. If the browser trusts the certificate, it generates a session pre-master secret based on the public key using the highest level of encryption supported by both parties

The components of the protocol.

SSL is subdivided into four sub-protocols: the SSL record protocol, and the SSL handshake protocol. Plus, two other protocols, but which have a less essential role, are the SSL Change Cipher Spec, and the SSL Alert.

SSL record protocol defines the format that will be used for data exchange. While SSL handshake handles the various message exchanges between the customer and the server, at the moment they establish the connection such as authentication, protocol version, encryption algorithm, ...

Protocol SSL handshake: This protocol allows the client and the server to authenticate each other, negotiate the encryption algorithms, negotiate the MAC algorithms and finally negotiate the symmetric keys that will be used for encryption.

The communication SSL is done through four steps, as illustrated in Figure 1:

1. Establishment of security parameters.
2. Server authentication and key exchange.
3. Client authentication and key exchange.
4. End.

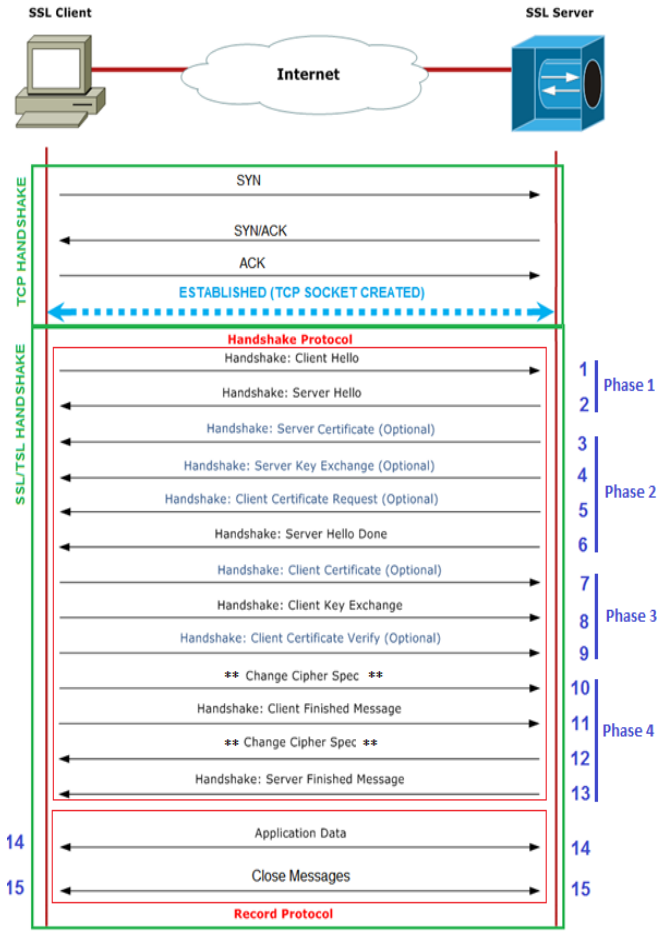

Figure 1. The steps of SSL communication

The server decrypts the pre-master secret using its private key, agrees to continue communication, and creates a master secret using encryption. Both parties now use a symmetric key that is only valid for that session. Once completed, the key is destroyed, and the next time you visit the site, the contact process begins again [23-26].

4. QUALITY OF SERVICE

Three main actors have essential stakes in designing and provisioning the Internet-based on the Internet Protocol (IP) [27]. These are the sender, the receiver and the Internet Service Provider (ISP). These actors compose the triangle of services (Figure 2). The sender wants to submit any form of traffic at any time (high load, saturation), while the receiver expects to receive all this sent traffic intact, with little delay (short delay, jitter, and packet loss). Also, the third player, the provider, wants to use the minimum possible network capacity per customer (whether sender or receiver) in order to be able to accommodate more customers on its network, resulting in higher profits.

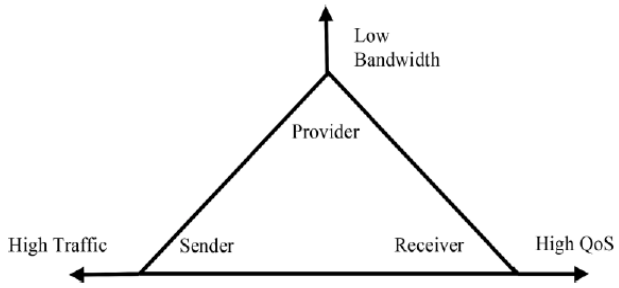

Figure 2. QoS triangle

The first objective of QoS is to give priority services, including bandwidth, jitter, and latency. It can also say that QoS represents the set of techniques needed to manage network bandwidth, delay, jitter, and packet loss. Another relevant term that will use shortly is a network flow or stream. A flow can be defined in several ways. One of them refers to a combination of source and destination addresses, source and destination socket numbers, and session identifiers. It can also be defined more broadly as any packet from a particular application or an inbound interface.

Real-Time Protocol (RTP): The first formal effort to support end-to-end, real-time transfer of stream data over network IP. RTP is a session layer protocol, which runs above the Datagram Protocol (UDP) user layer and is therefore transparent to network routers. This is an essential distinction from later technologies and architectures where routers have a key role in providing QoS differentiation. To get a better idea of how a video sequence [28] operating in standards affects traffic flow's bandwidth requirements, we classify them into one primary and two secondary constraints. The primary constraint is that the packet loss rate must be less than 1%. The secondary is that the 95th percentile of the end-to-end delay should be less than 50 ms, and the second constraint that jitter should be less than 30 ms.

5. POSSIBILITIES OF ATTACKS

This part aims to see the attacks that can cause a blockage on a communication channel such as the sniffing techniques [29] used by malware or hackers to exploit data that passes through a public network. Furthermore, it aims at identifying packets that circulate between communicators. This technique will make it possible to distinguish packets on routers or a communication channel thanks to dedicated tools (Wireshark in our case) connected to a database containing the attack model. If the sniffing system is detected as attacks, the firewall separates the Internet Protocol (IP) address. Then the communication between the attacker's host and the target will be interrupted. Our method allows us to encrypt the connection between two media (client-server) dynamically and regularly. Encryption ensures that no third party can read or falsify the data. Communications encrypted with a single key can expose sensitive data such as user names, passwords…, etc.

To capture confidential information from the flow of data packets over the network, an attacker must install an appropriate "sniffer" (network protocol analyzer) on the victim's system, e.g., Wireshark, Ettercap, Bettercap, Tcpdump, WinDump. It may not be just software. Sometimes the monitoring is done from a hardware device connected to the system.

DOS/DDOS: Attacks target corporate servers in companies and websites, much less often - individuals' personal computers. The aim of these actions, as a rule, is one: to cause economic damage to those attacked and to remain in the shadows. In some cases, DoS and DDoS attacks are steps in server hacking and are aimed at stealing or destroying information. In fact, a company or website belonging to anyone can become a victim of cybercriminals. Generally, we can distinguish several types: In the case of a massive (volume-based) DDoS attack, many requests are often used, often sent from legitimate IP addresses, so that the site "drowns" in traffic. These attacks aim to "block" all available bandwidth and block legitimate traffic [30]. In a protocol-level attack (such as UDP or ICMP), the goal is to deplete system resources. To do this, open requests are sent, e.g., TCP/IP requests with a fake IP, and due to the exhaustion of network resources, it becomes impossible to process legitimate requests. Typical representatives are DDoS attacks, known in narrow circles as Smurf DDos, Ping of Death, and SYN flood. Another type of DDoS attack at the protocol level involves sending many fragmented packets that the system cannot handle. Layer 7 DDoS attacks are the sending of seemingly harmless requests that appear to result from normal user activity. Botnets and automated tools are generally used to implement them. Notable examples are Slowloris, Apache Killer, Cross-site scripting, SQL-injection, Remote file injection [31]. The change to a small encryption key capable of ensuring a favorable quality of service while maintaining the data's security and integrity on the channel.

6. THE PROPOSED APPROACH

The field of intervention of our method is wide; however, we focus on studying the transmission of a video sequence from a server (broadcaster) to a simple client (consumer). The client sends information to the server, such as the SSL protocol version, session ID, and encryption suites, and then the information such as the cryptographic algorithms and keys supported. The server chooses the best encryption suite supported by it and the client, and sends it to the client (Certificate (Public Key, Data)), and then requests the client to

send its certificate if necessary. After the client verifies the certificate, it sends the encryption key used to encrypt messages; this is done once and for all in regular communication. However, in our case, we will modify it to be dynamic and automatic and linked to the channel and QoS status. To start with better security, we need to use a more secure key for this, and we need to start the encryption with the AES_256 key. The system will then automatically control the channel status through the existing parameters (latency, jitter...). If abnormal behavior is observed (network saturation, congestion ...), the system must intervene and change the key quickly to a smaller size than the one used initially and then continue the procedure. If stabilization is observed after, the system will change to a large key (Figure 4).

6.1 Concept of our method.

The diagram below (Figure 3) describes the steps followed in our method.

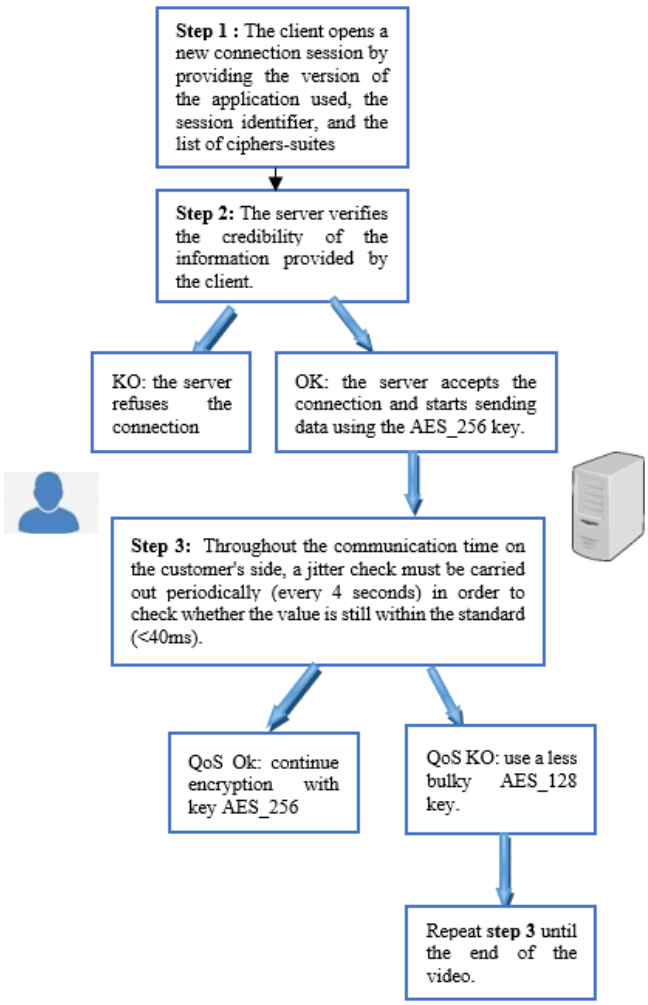

Figure 3. Operating principle of our method

This Algorithm will allow us to find compromises between various objectives:

➢ Automate renegotiations: this procedure did not exist before, because the negotiation is done once and for all, at the start of communication, but with this the algorithm we can have renegotiations if necessary, it all depends on the state of the channel, jitter, latency ...

➢ Change the key in an alternative way: this option has two major advantages:

✓ The key used in the session is temporary, and therefore it will be more difficult for a hacker to attack the canal.

✓ There is no need to allocate significant resources to use more keys secure. Alternatively, to implement more or less weak keys to save costs resources. Because thanks to this solution we can make changes between keys in a flexible way.

➢ Optimization of resources: instead of allocating significant resources to implement solutions in the worst cases, thanks to this algorithm, we can reserve resources compatible with the current situation.

➢ An equilibrium between security and service quality: i.e., if the channel is loaded, then the latency is important. The algorithm chooses by default the cyphers suites with encryption keys and lightweight hashing to ensure a better quality of service possible.

Our method is set up to satisfy users' needs by minimizing the workload due to the different treatments, i.e., to invent a dynamic algorithm that adapts to the different situations of the channel without any external intervention.

As already evoked the first phase consists of passing by a standard negotiation, the customer sends a hello + the list of cyphers suites that he supports as shown below (Figure 5).

A modification will be made to the previous phase by applying a filter at the cipher's suits list to support only the AES encryption key and eliminate the DES,3DES keys since they are too much and are not compatible with this kind of exchange. The new list is as illustrated Figure 6.

If you want to focus on a cipher's components, they usually consist of four parts, as shown in Figure 7.

After the server receives the client request the second filter is going to be applied this time on the server-side to tolerate that the AES key size 256 in the suggestions the goal is to start with a higher security level, using a more secure key of ample size for that we must start the encryption with the key AES_256(we do not take into account the robustness of the hash key in our study) (Figure 8).

The next step is to ensure confidentiality, so the server must send a certificate validated by a CA (Certification Authority) (Figure 9).

After the certificate verification phase on the part of the client, it sends the encryption key used to encrypt the messages; this phase is carried out once and for all in regular communication. However, in our case, we will modify it so that it is dynamic and automatic is linked to the channel and the QoS state. The certificate's sending on the client-side remains optional so that the two interlocutors can securely exchange data.

At this point, we have managed to provide favorable security but assuming we are facing a DDOS attack?

Our method can detect this attack on our flag for the security measures, which can make our task more manageable. The "timestamp" field is available on the RTP frames for our service at the calculation level to the latency variation (JITTER). We remind you that the tolerable value for videos estimated at 40ms.

After every 4 seconds, a check of the different QOS parameters (packet loss, latency, jitter) is done automatically if the system detects one or more abnormal things (e.g., jitter exceeds the tolerable threshold of 40 ms as a result of a DOS attack), i.e., the channel is well loaded and can cause service degradation. So a switch to another small key is essential to reduce the size of the frames sent.

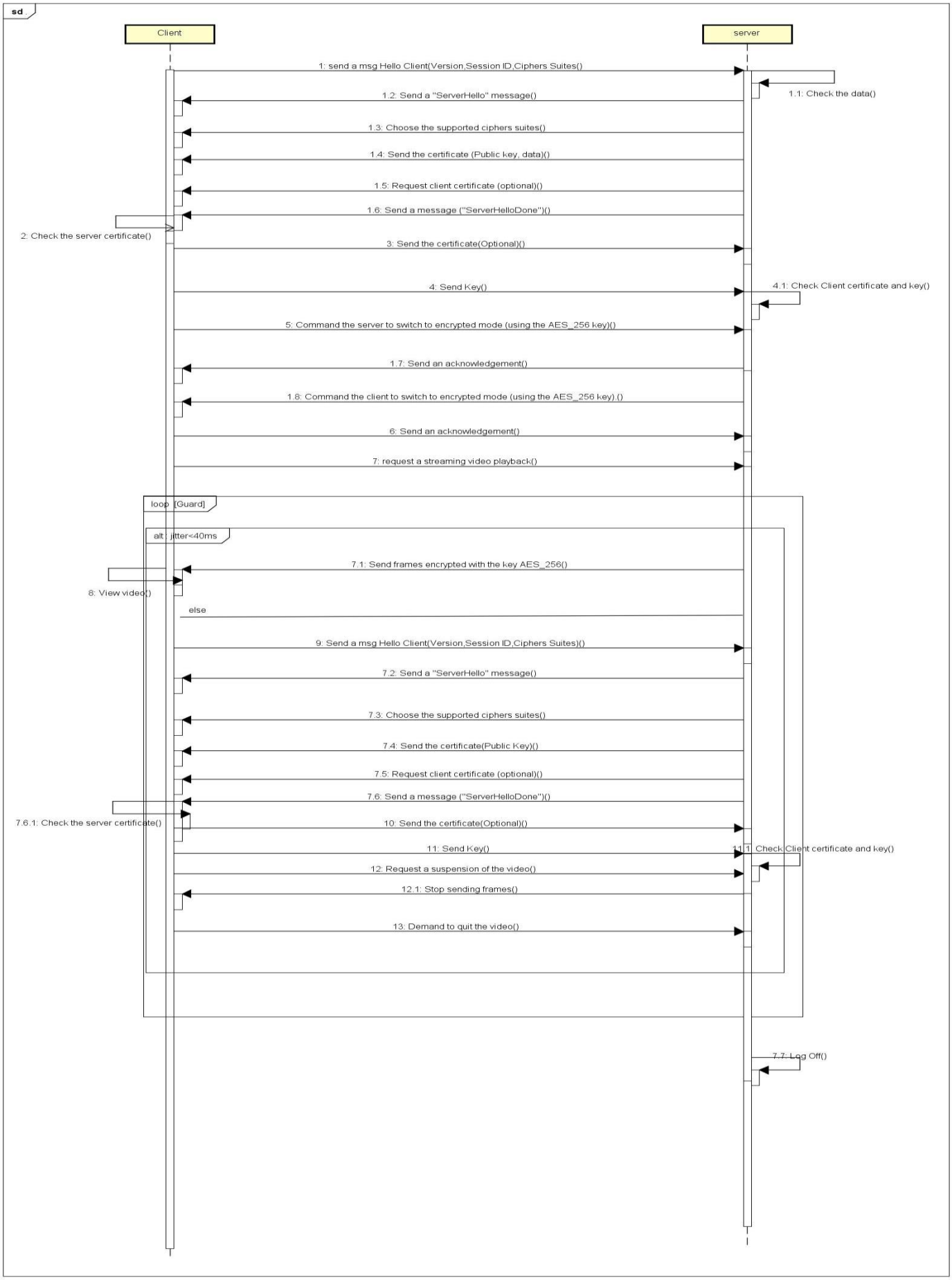

Figure 4. Sequence diagram of our method

Figure 5. Starting an SSL negotiation

Figure 6. Parametric SSL negotiation

Figure 7. Components of a cipher suits

Figure 8. Parametric SSL negotiation_ AES256

Figure 9. Final round of negotiations

In time, an axis that does not exceed one second, the client must request a small key through a quick renegotiation with the server. However, this time he must propose the AES128 keys in the list of cipher suites.

In the same way, after every 4 seconds, a jitter calculation is done automatically. If the jitter is above the tolerable threshold, we always keep the same key if we move to the next size to increase the security.

On the practical side and implementation of this solution we have used a class diagram indicated in the above (Figure 10) consists of three main classes (Server, Client, RTPPacket).

A server can establish one or more connections, and to do so it needs auxiliary threads, and because java has been used as a programming language, the threads need well-defined methods.

The VideoStream class is used to decompose the video into frames to send them to the Clients.

And to guarantee a real time communication between the client and the server the RTPPacket class is used.

6.2 Experiments

To simulate our method, we have used two virtual machines that use a Linux operating system, and the first machine will be the client and the second a secure broadcast server, which can stream videos on demand in a secure mode. The server uses RTP to transport the data in real-time, and SSL to secure the exchanges. One or more clients can retrieve and manipulate the video remotely using the RTSP protocol. To retrieve a video sequence, the client sends a request to create the channel and initialize the session. At this step, the client and the server make exchanges (Certificate, encryption key, cyphers suites, ...) We used the Wireshark tool to capture different interactions. The client sends to the server information such as SSL protocol version, session id, and cypher suites information such as cryptographer algorithms and supported keys. Then the server selects the cypher suite supported by it and the client. Client and server exchange certificates with each other; each certificate contains a public key plus data specific to the certificate. After the certificate verification phase, the client sends the encryption key used to encrypt messages; this phase is performed once and for all in regular communication. However, in our case, we will modify it to be dynamic and automatic is linked to the channel status and the QoS. A standard IP frame with the essential elements (source and destination address, version, flags, fragments, TTL, total length...) encapsulates the data sent (Figure 11).

As marked in red, in the preceding figure the number (1) the components of the hello-client frame, (2) the server response, (3) the session encryption, and then (4) the data exchanges.

2) The customer must send that the ciphers-suites whose encryption key is AES256 (as described in Figure 12).

3) The server chooses the first support cipher on its part, as shown below with the number (2) in red (Figure 13).

4) After starting the video playback, the resulting packets are encrypted using the denial function during the negotiation and write key. The algorithms used for encryption are AES_256 (Figure 14).

As already mentioned, the algorithm must work in different scenarios. It must also be able to automate the change of keys; for this, we will discuss both solutions:

Free channel: in ordinary cases using two virtual machines connected, a server and a client, then observe the results under Wireshark.

Saturated channel: in this case, we used the Hping3 tool to apply a DOS attack, to load the channel and see the behavior of the algorithm.

6.2.1 Free channel

After starting the video at the client, the calculation of the different QOS parameters (latency, jitter.) is done automatically every 4 seconds. If one or more parameters exceed the recommended thresholds, the key must be changed. The encryption is carried out with the AES_256 key (Figure 15).

6.2.2 Channel saturated

As explained, Denial of Service is a technique that consists of sending a data stream that is too large concerning what the target can receive and process. If someone has an IP address and wants to deny you access to the Internet or block access to

your site, they will be able to do so if they have a sufficiently large connection. It will then flood and saturate upload bandwidth, which will cause a massive disruption to Internet Traffic in both directions. After performing a DOS attack with the Hping3 tool to saturate the channel, it turns out that the algorithm only uses the AES_128 key to minimize the packet size and manage network congestion.

The client starts the encryption with the AES_256 key to having a reliable security level. However, as soon as the jitter exceeds the 30ms threshold, it is necessary to automatically change the key to AES_128 to reduce the frames' size and facilitate the communication as mentioned (Figure 16).

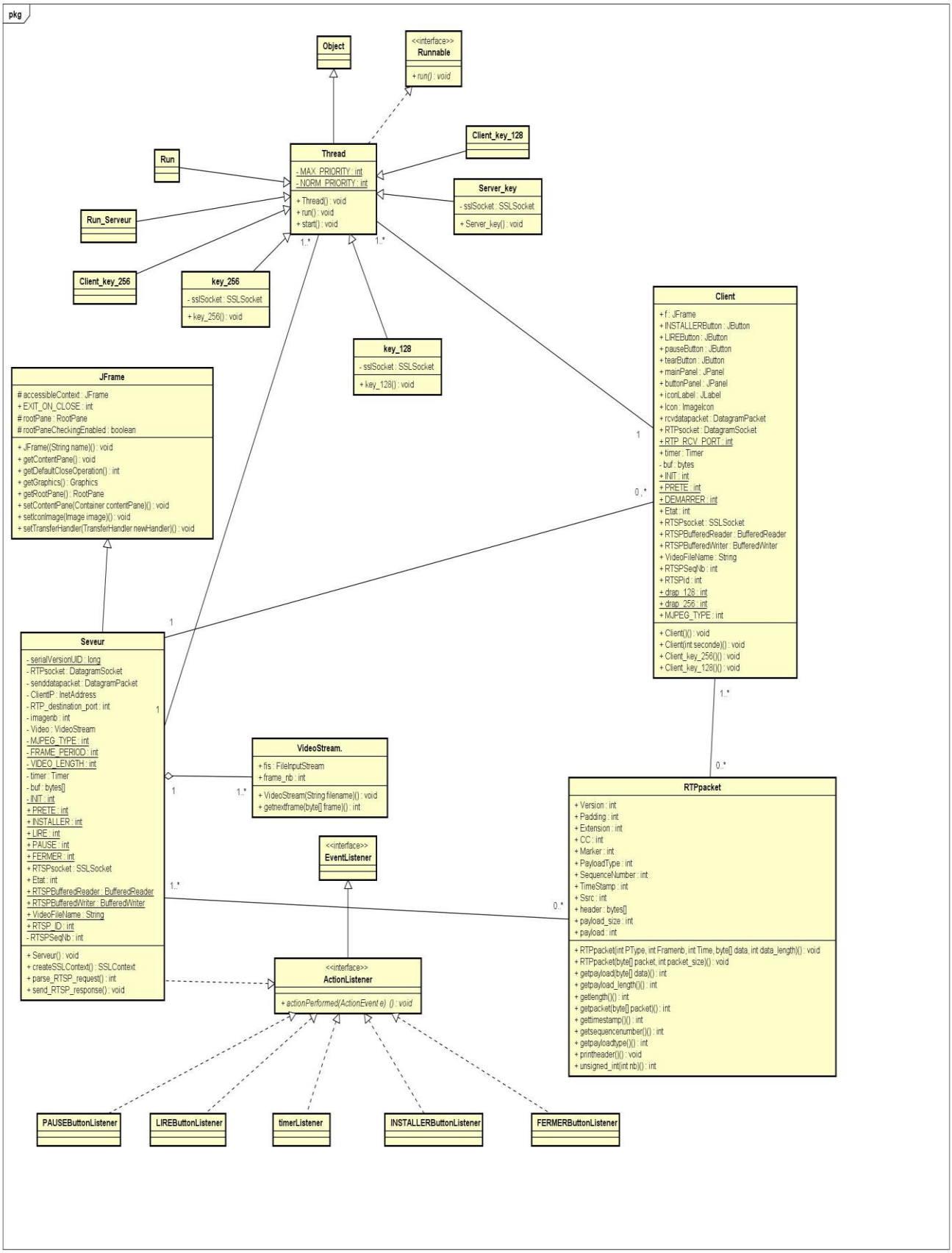

Figure 10. Class diagram of our method

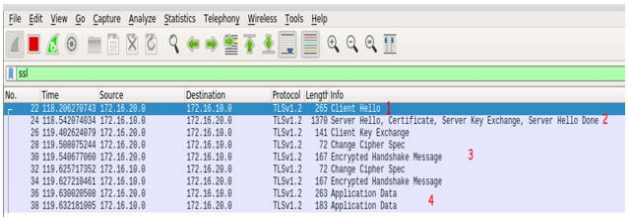

Figure 11. Initialization of the SSL session under Wireshark

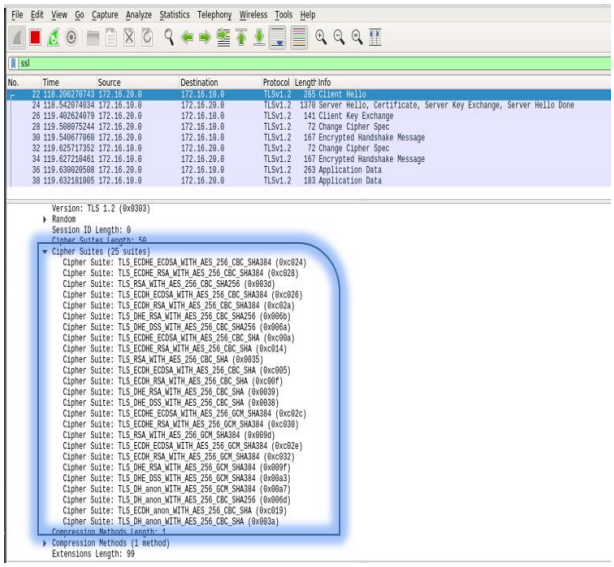

Figure 12. The list of AES_256 suite ciphers provided by TLS1.2

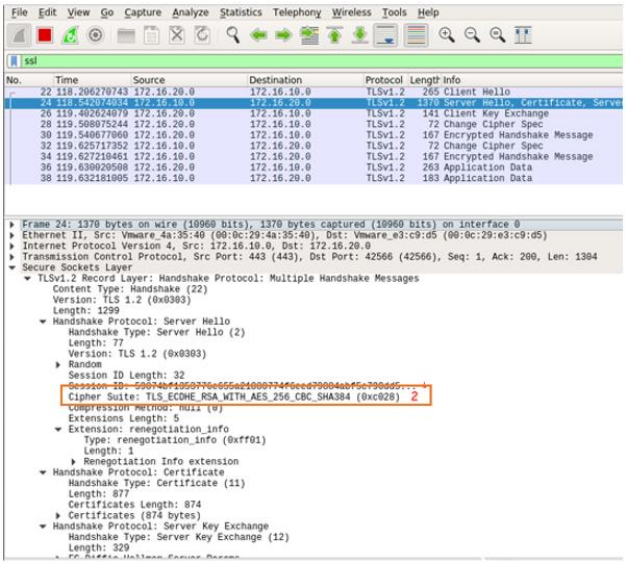

Figure 13. The choice of cipher suit

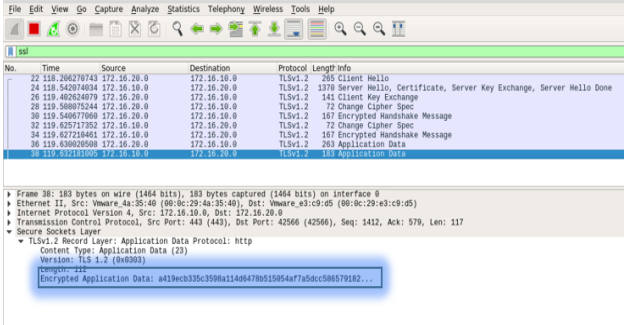

Figure 14. Data encryption

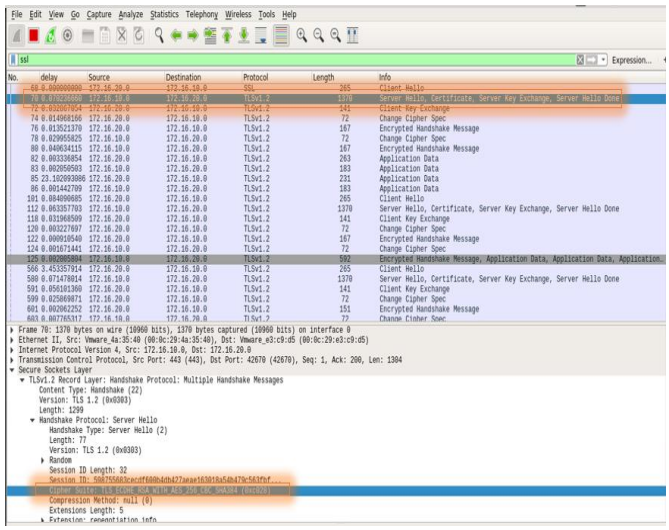

Figure 15. Encrypt with the AES256 key

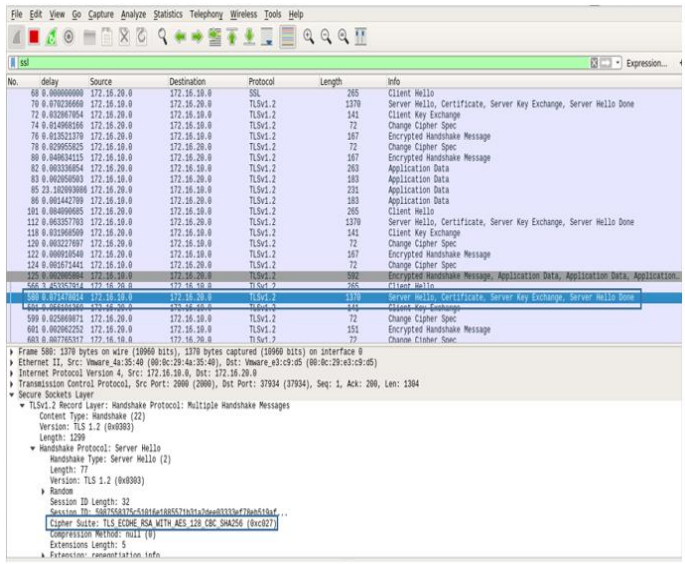

Figure 16. The exchange of the key to AES_128

6.3 Comparative studies

Benchmarking involves the continuous evaluation of best practices of certain solutions that stand out. Benchmarking is a process designed to allow both internal and external evaluation to develop and implement a plan to address the various issues. The proposed solutions follow the same context, it is to secure the exchanges between two communicators, the level of security changes from one solution to another, also the utility.

Beginning with the SRTP protocol used by the RTP protocol. SRTP has the added value of confidentiality and anti-replay protection, mainly intended for VoIP communications. This protocol is strong in terms of security, and this is not the case in QOS, as it performs key changes at a given time interval and does not check the QOS parameters.

The second solution dealt with is the use of the ZRTP protocol, which has good cryptographic functionality in many other VoIP encryption methods. Although it uses a public key algorithm, it avoids the complexity of a Public Key Infrastructure (PKI). It does not use persistent public keys. It uses Diffie-Hellman with hash algorithms and allows detection of man-in-the-middle (MiTM) attacks. This protocol

is also strong in terms of security and provides a channel management mechanism but has the same SRTP problem, it does not use a QOS management mechanism.

The last solution proposed is to realize a hybrid algorithm that supports the strong points of the protocols (SRTP, ZRTP), and that merges the two protocols RTP and TLS to automate the change of keys in relation to the different parameters of the QOS. The Table 1 below illustrates the comparison between the three solutions.

Table 1. Comparison between SRTP, ZRTP and our protocols

	SRTP	ZRTP	Our method
Security	Strong	Strong	Strong
QOS management	Low	Low	Strong

7. CONCLUSIONS

This study has allowed us to move on to a more important phase that citing the different needs, dysfunctions, and challenges we have encountered. Afterward, we carried out studies on the requirements and the different possible approaches to realize this hybrid algorithm based on RTP and SSL protocols.

The security provided by standard RTP is insufficient because it does not support authentication, and its default encryption algorithm (DES) is fragile at present and simpler to hack.

The biggest security challenge is the management of security keys, how to distribute them, how to store and update them, how to protect them from hackers. For this purpose, we thought about realizing a dynamic and automatic security solution.

REFERENCES

[1] Al-Maqri, M.A., Mansoor, A.M., Sabri, A.Q., Ravana, S.D. (2020). High performing multimedia transmission approach based on QoS support and admission control over IEEE 802.11e networks. International Journal of Communication Systems, 33(5): e4193. https://doi.org/10.1002/dac.4193

[2] Serhrouchni, A., Hajjeh, I. (2006). Integration of the digital signature in the protocol SSL/TLS. Annales Des Télécommunications, 61: 522-541. https://doi.org/10.1007/BF03219921

[3] Hu, Q.S., Fan, X.N., Zhang, Q.W. (2019). An effective differential power attack method for advanced encryption standard. International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC, Guilin, China. https://doi.org/10.1109/CyberC.2019.00019

[4] Nakasone, T., Li, Y., Yu, S., Mitsugu, I., Kazuo, O., Kazuo, S. (2012). Key-dependent weakness of AES-based ciphers under clockwise collision distinguisher. International Conference on Information Security & Cryptology, 7839: 95-409. https://doi.org/10.1007/978-3-642-37682-5_28

[5] Stinson, D.R., Paterson, M.B. (2019). Cryptography théorie and pratices. International Standard Book Number-13: 598-599.

[6] Kambourakis, G., Rouskas, A., Gritzalis, S. (2002). Using SSL/TLS in authentication and key agreement procedures of future mobile networks. 4th International Workshop on Mobile and Wireless Communications Network. Stockholm, Sweden. https://doi.org/10.1109/MWCN.2002.1045713

[7] Pisheh, Z., Sheikhi, A. (2004). Detection and compensation of image sequence jitter due to an unstable CCD camera for video tracking of a moving target. Proceedings. 2nd International Symposium on 3D Data Processing, Visualization and Transmission, 2004. 3DPVT 2004. https://doi.org/10.1109/TDPVT.2004.1335203

[8] Yang, C.Y., Ling, Y., Li, X. (2019). Information encryption algorithm in power network communication security model. IOP Conference Series: Materials Science and Engineering, 750: 012161.

[9] Acharya, B., Panigrahy, S.K., Patra, S.K., Panda, G. (2009). Image encryption using advanced hill cipher algorithm. International Journal of Recent Trends in Engineering, 1(1): 663-667.

[10] Mansouri, A. (2021). Image encryption using shuffled Arnold map and multiple values manipulations. The Visual Computer, 37(6). https://doi.org/10.1007/s00371-020-01791-y

[11] Hofmann, G.R. (1993). The modelling of images for communication in multimedia environments and the evolution from the image signal to the image document. The Visual Computer, 9(6): 303-317. https://doi.org/10.1007/BF01901911

[12] Lin, C.H., Chao, M.W., Liang, C.Y., Lee, T.Y. (2010). A novel semi-blind-and-semi-reversible robust watermarking scheme for 3D polygonal models. The Visual Computer, 26(6): 1101-1111. https://doi.org/10.1007/s00371-010-0461-y

[13] Tu, S.C., Tai, W.K., Isenburg, M., Chang, C.C. (2010). An improved data hiding approach for polygon meshes. The Visual Computer, 26(9): 1177-1181. https://doi.org/10.1007/s00371-009-0398-1

[14] Li, G.D. (2019). Double chaotic image encryption algorithm based on optimal sequence solution and fractional transform. The Visual Computer, 35(9): 1267-1277. https://doi.org/10.1007/s00371-018-1574-y

[15] Touil, H., El Akkad, N., Satori, K. (2020). Text Encryption: Hybrid cryptographic method using Vigenere and Hill Ciphers. In 2020 International Conference on Intelligent Systems and Computer Vision (ISCV) IEEE, pp. 1-6. https://doi.org/10.1109/ISCV49265.2020.9204095

[16] Wei, X., Sellal, K., Bouslimani, Y. (2012). Security implementation for a VoIP server. In 2012 International Conference on Computer Science and Service System IEEE, pp. 983-985. https://doi.org/10.1109/CSSS.2012.249

[17] Balhwan, S., Kumari, N., Mohapatra, A.K. (2018). Encrypted web traffic classification. In 2018 3rd International Conference on Contemporary Computing and Informatics (IC3I) IEEE, pp. 1-6. https://doi.org/10.1109/IC3I44769.2018.9007264

[18] Chakaravarthi, S., Selvamani, K., Kanimozhi, S., Arya, P.K. (2014). An intelligent agent based privacy preserving model for Web Service security. In 2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE) IEEE, pp. 1-5.

https://doi.org/10.1109/CCECE.2014.6901164
[19] Taleb, T., Aoul, Y.H., Benslimane, A. (2010). Abderrahim Benslimane; Integrating Security with QoS in Next Generation Networks. 2010 IEEE Global Telecommunications Conference GLOBECOM, pp. 6-10. https://doi.org/10.1109/GLOCOM.2010.5683321
[20] Aiash, M., Mapp, G.E., Lasebae, A. (2011). Security and QoS integration for protecting service providers in heterogeneous environments. International Journal of Computer Science, 38(4): 384-393.
[21] (Bud) Bates, R.J. (2014). Securing VOIP: Keeping Your VoIP Network.
[22] Bresciani, R., Butterfield, A. (2010.) A formal security proof for the ZRTP Protocol. International Conference for Internet Technology and Secured Transactions, ICITST 2009 5402595.
[23] Lindell, Y., Katz, J. (2015). Introduction to Modern Cryptography Second Edition 500. International Standard Book Number,13: 978-1-4665-7027-6.
[24] Elazzaby, F., Akkad, N.E., Kabbaj, S. (2020). A new encryption approach based on four squares and Zigzag. The 1st international conference on Embedded Systems and Artificial Intelligence, ESAI, 1076: 589-5970. https://doi.org/10.1007/978-981-15-0947-6_56
[25] Es-sabry, M., El akkad, N., Merras, M., Saaidi, A., Satori, K. (2019). A new color image encryption using random numbers generation and linear functions. The 1st International Conference on Embedded Systems and Artificial Intelligence, ESAI, 1076: 581-588. https://doi.org/10.1007/978-981-15-0947-6_55
[26] Yan, Q., Yu, F.R. (2015). Distributed denial of service attacks in software-defined networking with cloud computing. IEEE Communications Magazine, 53(4): 52-59. https://doi.org/10.1109/MCOM.2015.7081075
[27] Anjum, B., Anjum, B., Perros, H. (2015). Bandwidth Allocation for Video under Quality of Service Constraints. Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc. https://doi.org/10.1002/9781119073178
[28] Seetha, S., Francis, S.A.J., Kanaga, E.G.M., Daniel, E., Durga, S. (2019). A framework for multi-constraint multicast routing in wireless mesh networks. 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, pp. 445-451. https://doi.org/10.1109/ICACCS.2019.8728498
[29] Atoum, Y., Liu, Y., Jourabloo, A., Liu, X. (2018). Face anti-spoofing using patch and depth-based CNNs. IEEE International Joint Conference on Biometrics, 2018-January, 319-328.
[30] Deshmukh, R.V., Devadkar, K.K. (2015). Understanding DDoS Attack & Its Effect in Cloud Environment. Procedia Comput. Sci, 49(1): 202-210.
[31] Malik, M., Singh, Y. (2015). A review: DoS and DDoS attacks. International Journal of Computer Science and Mobile Computing, 4(6): 260-265.