Design and Implementation of a Collaborative Communication Network for Video Conference Services

Mihăiță RĂDOI and Petrică CIOTÎRNAE

***Abstract*—Under the current global conditions, strong emphasis is put on saving resources and reducing costs, migrating to collaborative unified communications solutions and developing open-source Web applications. The secure video-conferencing system will mainly use VoIP and WebRTC technologies to make multimedia calls, allowing end-users mobile and remote access (MRA) and therefore to facilitate communication between different networks, as well as the accessibility and the interoperability with any type of technology and device. This article will analyze the scalable implementation of the real-time communications network, providing redundancy and load balancing, therefore ensuring the high availability of the entire collaborative communications system. The call control and the dial plan are done through the Unified Call Manager software and WebRTC video-conferencing external access functionality is provided by configuring Traversal Using Relays around NAT (TURN) service across the Expressway Series server pair (Core & Edge). The ability to manage and monitor virtual meetings remains the responsibility of the open-source management tools.**

***Index Terms*—WebRTC, VoIP, UC&C, MRA, XMPP, TURN, CMS, Virtual Meeting, API REST, DMZ, LDAP.**

I. Introduction

At the moment, the society we live in as well as all work environments are directly dependent on voice, video and data communications, which are being absolutely necessary elements in carrying out the daily tasks.

The evolution and emergence of various technologies on the Internet has improved and facilitated the existence of new applications and services, such as collaboration systems, video-conferencing, cloud computing etc. Significant advances in the collaboration space simplify implementation, improve interoperability and enhance the overall end-user experience.

Voice over Internet Protocol, technology that incorporates a variety of methods for establishing bidirectional multimedia communications over the Internet or other networks based on IP packets switching. VoIP systems are capable of certain unique functions, such as video-conferencing, instant messaging and multicasting [1].

The Unified Communications and Collaboration (UC&C) are capable of providing unlimited communications in many ways and of giving the flexibility to implement WebRTC-based applications, in order to save resources and reduce the costs.

The WebRTC framework enables unified real-time communications through a Web browser, providing a range of cost-free audio and video codecs that offer high quality virtual meetings. When deploying in a web browser, audio, video, and network components can be accessed through API queries, providing flexibility in developing applications based on WebRTC technology [1].

REST API (Application Programming Interface Representational State Transfer) is used for the most advanced configuration activities, such as configuring the database cluster.

GET:
https://{{nodCMS}}:{{port}}/api/v1/system/database
POST:
https://{{nodCMS}}:{{port}}/api/v1/coSpaces/{{SpaceId}}
DELETE:
https://{{nodCMS}}:{{port}}/api/v1/coSpaces/{{SpaceId}}

Through the REST API platform, it can build individual applications that are functional on any type of specialized server, having a lot of possibilities in terms of programming languages. By developing applications using the REST API platform, it can avoid the expense of purchasing proprietary applications. These applications can also be customized according to the specific needs of a communications network.

The collaborative video-conferencing network allows end users to join in an encrypted audio and video conference, which is the virtual space where there are some facilities for collaborative unified communications such as: instant messaging, presence, contact management, video-conference participant management, share screen and privileged virtual spaces.

II. Collaborative Communications System Platform

The basic architecture of the WebRTC collaborative network contains the following components:

A. Internal Private Network (LAN):

- The MeetingCluster manages video-conferencing resources by hosting them in dedicated virtual spaces;
- Unified Call Manager (CUCM) software has an important role in call processing and controlling, creating software end users, integrating voice, video, media, and managing the resources in performing video-conferencing functions [2];
- Instant Messaging and Presence Service (IM&P) is an

M. RĂDOI is with the Communications Department, Military Technical Academy "Ferdinand I", Bucharest, Romania (e-mail: radoimihai111@gmail.com).

P. CIOTÎRNAE is with the Communications Department, Military Technical Academy "Ferdinand I", Bucharest, Romania (e-mail: petrica.ciotirnae@mta.ro).

Digital Object Identifier 10.32754/JMT.2020.1.02

open and extensible standards-based platform that facilitates the secure exchange of presence and instant messaging information, based on the XMPP protocol, between the CUCM server and other applications;

- Microsoft Active Directory is an implementation of Lightweight Directory Access Protocol (LDAP) directory services, providing the administrator a flexible environment with global effect for assigning permissions, installing programs, renewing security [2];
- Meeting Management (CMM) is a virtualized tool for managing the collaborative unified communications platform for conferencing and video calling.

B. Demilitarized Zone (DMZ):

- Expressway Edge & Core provides the ability to traverse firewalls that delimit the demilitarized zone, allowing access to and from the private internal network;
- The Domain Name System (DNS) server is used to convert the domain name to a numeric format, IP address.

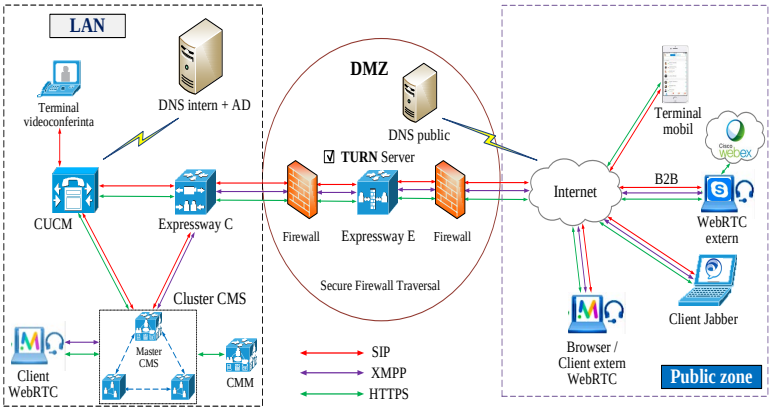

Figure 1. The topology of the Collaborative Video-conferencing Network

The components of the video-conferencing system, such as database, call bridge, XMPP server, Web bridge, are grouped into clusters, so that they will benefit from scalability, high availability, redundancy and load balancing.

The XMPP server allows WebRTC clients registration and authentication, as well as signaling between CMS cluster components [3].

The database for internal network servers can be either a local or an external database. For the platform described above, the database used is both a local and also an external database, Microsoft Active Directory, for managing xmpp clients.

The management and administration of the collaborative network of unified communications is performed by the following methods:

→ The command-line interface (CLI) is used for the trust digital certificates configuration.

→ The graphical user interface Web is the easiest and simplest method to configure the internal network servers, especially for setting up the dial plan and calling bridge.

→ The application programming interface REST API is known for most advanced configurations.

→ The SSH File Transfer Protocol (SFTP) is used to transfer backup file, licenses, upgrade-images, logs and trust digital certificates.

The clients mapping details of The Collaborative Video-conferencing System WebRTC are configurable through API commands for LDAP mapping maps, based on Active Directory entries.

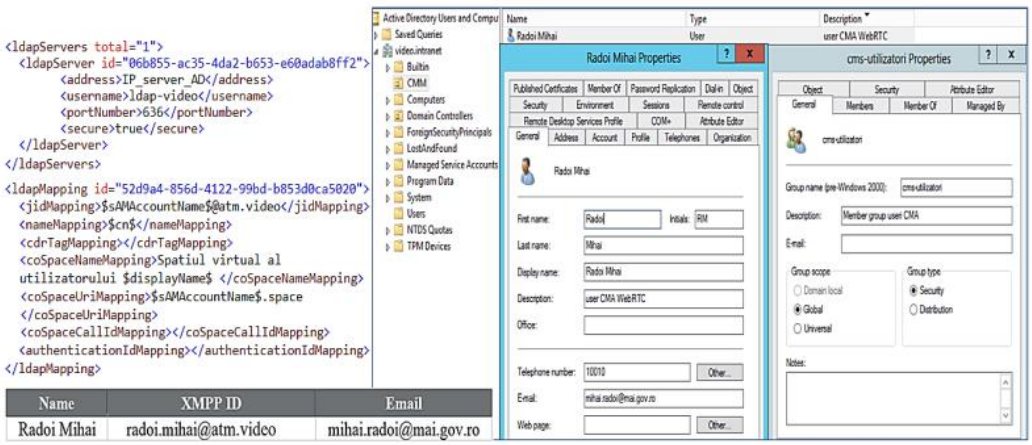

Figure 2. Mapping WebRTC clients in Active Directory

The SRV DNS records help to discover unified collaborative communications services.

- _collab-edge._tls. – represents the symbolic name of the service, indicating the location of the Expressway-Edge

server, together with the TLS transport protocol;

- _xmpp-client._tcp. – resolves the port 5222 on Meeting Servers and is used by WebRTC clients to locate an XMPP server, as well as the port 5269 (S2S - server to server);
- _turn._tcp./udp. – the TURN service uses port 3478 using TCP / UDP transport protocols, providing the location of the TURN server [4].

```
>nslookup -q=srv _xmpp-server._tcp.atm.video
Server:  AD-DNS
Address:  x.x.x.x
_xmpp-client._tcp.atm.video     SRV service location:
        priority       = 10
        weight         = 5
        port           = 5269
        svr hostname   = cms-web.atm.video
cms-web.atm.video       internet address = x.x.x.x
>nslookup -q=srv _xmpp-client._tcp.atm.video
_xmpp-client._tcp.atm.video     SRV service location:
        priority       = 5
        weight         = 5
        port           = 5222
        svr hostname   = cms-web.atm.video
cms-web.atm.video       internet address = x.x.x.x
>nslookup -q=srv _turn._udp.public.domain
_turn._udp.public.domain     SRV service location:
        priority       = 10
        weight         = 10
        port           = 3478
        svr hostname   = expres.edge.public.domain
expres.edge.public.domain       internet address = x.x.x.x
```

The general profile of privileged users, owners or members of virtual spaces dedicated to the WebRTC Collaborative Videoconferencing System is configured as follows [5]:

```
<callLegProfile id="d5f3b225-91b1-471e-b3ff-62107eaef77c">
  <needsActivation>false</needsActivation>
  <name>Host_Profile</name>
  <defaultLayout>allEqual</defaultLayout>
  <participantLabels>true</participantLabels>
  <presentationContributionAllowed>true</>
  <muteOthersAllowed>true</muteOthersAllowed>
  <videoMuteOthersAllowed>true</videoMuteOthersAllowe
  <endCallAllowed>true</endCallAllowed>
  <disconnectOthersAllowed>true</disconnectOthersAllowe
  <sipPresentationChannelEnabled>true</>
  <changeLayoutAllowed>true</changeLayoutAllowed>
  <bfcpMode>serverAndClient</bfcpMode>
  <callLockAllowed>true</callLockAllowed>
  <allowAllMuteSelfAllowed>true</allowAllMuteSelfAllowed>
  <changeJoinAudioMuteOverrideAllowed>true</>
  <recordingControlAllowed>true</recordingControlAllowed>
  <streamingControlAllowed>true</streamingControlAllowe
  <addParticipantAllowed>true</addParticipantAllowed>
  <participantCounter>always</participantCounter>
</callLegProfile>
```

Two types of callLeg profiles are created, one for the host user call configuration and another for guest clients that require activation, being placed in a virtual waiting room, known as lobby.

III. External Access Functionality of WebRTC Clients

Located in the demilitarized zone, the Expressway-Edge platform acts as a TURN server and establish the received media traffic on its interfaces so that collaborative end users can set up a bidirectional communication in real time. Expressway-Core connects to the Edge server along the firewall on certain dedicated ports with security credentials [6].

Expressway-Core sends keep-alive packages to Expressway Edge. When the Edge server receives an incoming call or other request for the collaboration service, it sends this request to Expressway-Core. Then, the Core server routes the request to the Meeting Server or Unified Call Manager, initiating the connection. The call is established and the media data crosses the firewall in a secure way.

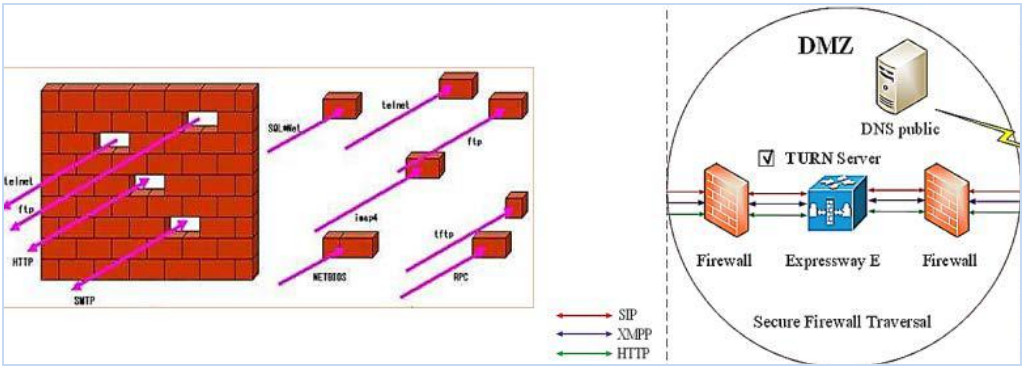

Figure 3.Secure external access of WebRTC clients

The UDP port 3478 and the TCP port 443are allocated for TURN requests and are opened on the front-end and back-end firewalls, from the private internal network servers to the dual network interfaces of the Expressway-Edge platform.

As it is located in the public area, in particular, Expressway-Edge certificates must be signed by a trusted public certification authority (CA). Expressway-Edge must also trust connections from its peers, the firewall traversal client, Expressway-Core and the videoconferencing web-server, as a TURN client [6].

The public key of the trusted certification authority is displayed in the SPKI field, while the electronic signature is generated by the RSA private key of the Let's Encrypt authority, which is a non-profit certification authority that offers X.509 certificates for TLS encryption.

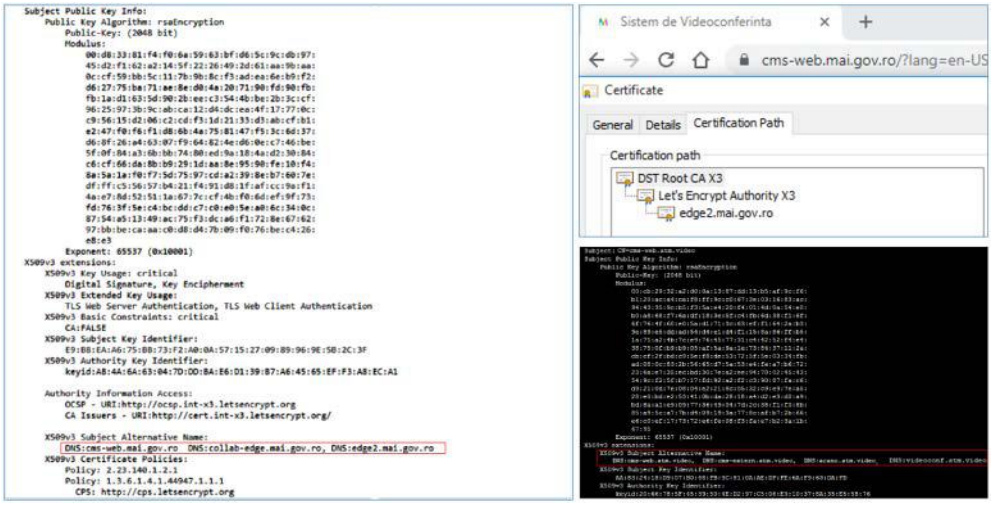

Figure 4. Trusted digital certificates

The SSH tunneling session is used to access collaborative services in the internal network across the firewall, through an encrypted SSH connection. Two secure connections are established, one with Expressway-Core, which is the firewall traversal client, and one with the Meeting server, as a TURN client.

A set of algorithms, crypto-suite, is known to secure the connection on TLS transport networks, including: a cryptographic key exchange algorithm, a block encryption algorithm, AES-Counter Mode and an authentication code algorithm, SHA1.

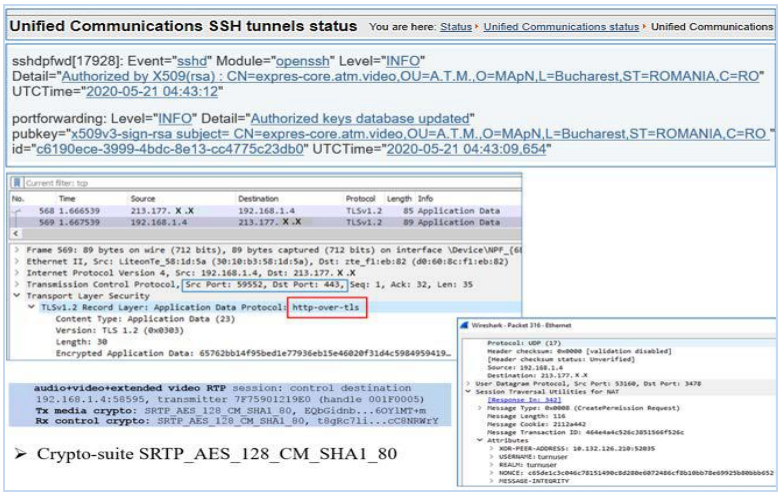

Figure 5. Establishing SSH tunnels and exchanging cryptographic keys

The SRTP_AES_128_CM_SHA1_80 crypto suite defines the encryption and authentication transformations that will be used for the secure real-time transport media stream. It provides a 128-bit long master key, along with an 80-bit authentication tag with a default lifetime of 2^48 SRTP packets. Therefore according to the likelihood function, the probability of any received packet to be totally wrong is one in 2^48packets. The pseudo-random function is the default PR-SRTP function that uses a standardized algorithm for symmetric block-based encryption, AES, with a key length of 128 bits [7].

The requests and answers of the SRV DNS services of the collaborative system are presented in the next figure.

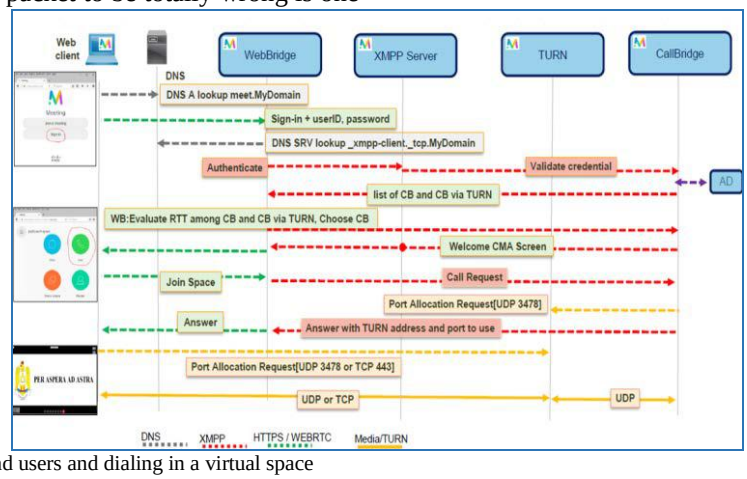

Figure 6. Connecting WebRTC end users and dialing in a virtual space

This image illustrates the process of connecting WebRTC end users (e.g. user.atm@atm.video) and their participation in a dedicated virtual space, as well as the participation of WebRTC guest clients (e.g. guest91310937@atm.video) in a virtual space; in this case, a temporary guest client is automatically created, which will only be active during the video-conference.

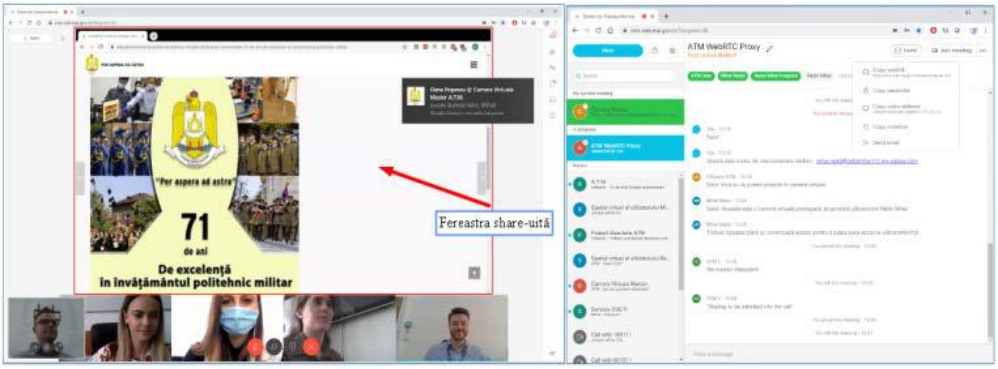

Figure 7. Collaborative unified communications

Video-conferencing codecs are designed to eliminate minor variations in incoming data by intentionally delaying the playback of received packets. The packets introduce a jitter buffer that adds an imperceptible delay to the listening experience, but allows the terminal to create a continuous audio stream for the receiver. However, when jitter becomes excessive, the buffer may become empty or overflow, causing disruptive audio experiences.

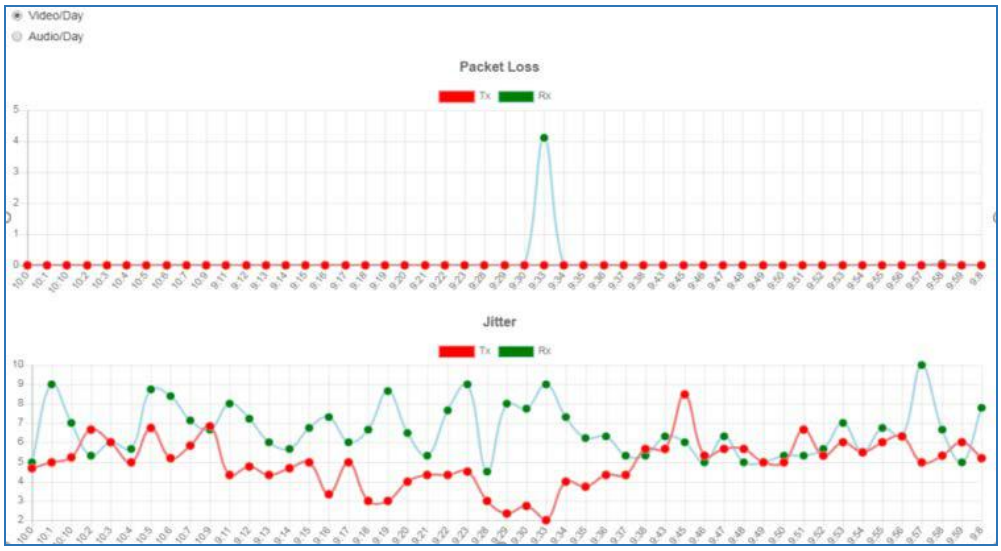

Figure 8. Codec specifications in a video-conference

The delay's variation, the jitter, is a very important indicator of the quality of video-conferences. Values between 0 and 20 ms are values that are considered to be acceptable and not to degrade the SIP call [8].

IV. Conclusion

What has been highlighted in this article represents only a fraction of the facilities offered by the virtualization of the secure network of real-time collaborative unified communications.

The video-conferencing network allows end users to join an encrypted audio and video conference, which represents the virtual space where there are some facilities for collaborative unified communications such as instant messaging, presence, contact management, video-conference participant management, share screen, privileged virtual spaces etc.

The conceptual network architecture of the demilitarized zone ensures that publicly accessible servers cannot come into contact with other segments of the private internal network if one of these servers is compromised. Therefore, by placing public services in the DMZ area, an additional layer of security is added to the internal network. External WebRTC users can connect to Collaborative Video-conferencing System services, but cannot access LAN.

It can be appreciated that the use of WebRTC technology and sockets for media signaling is a step forward for real-time collaborative communications applications, whether it is live streaming or instant messaging. The algorithms used for audio and video compression contribute to increase the quality of unified communications.

Following the tests, it was observed that the secure video-conferencing network is perfectly functional and can be used as a platform for collaborative interconnection of various beneficiaries within the National Defense System, as well as for educational purposes, as a laboratory platform for university education.

In conclusion, it can be said that the future of communications is increasingly based on software, which

will accelerate innovative processes. The virtualization of communication systems will transform today's static networks into flexible networks, equipped with programmable platforms that allow an intelligent and dynamic allocation of resources, load balancing media supporting the scalability and quality of services.

ACKNOWLEDGMENT

This work was supported by a grant of the Ministry of Innovation and Research, UEFISCDI, project number 9SOL/12.04.2020 within PNCDI III.

REFERENCES

[1] A.B. Roach, "WebRTC Video Processing and Codec Requirements", March 2016, <https://tools.ietf.org/html/rfc7742>.

[2] https://www.cisco.com/support/Configure-Multiple-CMS-WebBridges-via-Expressway.pdf.

[3] Extensible Messaging and Presence Protocol (XMPP): Core.

[4] [RFC4787] J. Rosenberg - Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT.

[5] CISCOLIVE - LTRCOL-2250 - Multiparty Conferencing for Audio, Video and Web Collaboration using Cisco Meeting Server.

[6] https://www.cisco.com/support/Configure-Proxy-WebRTC-With-CMS-over-Expressway-with-Dual-Domain.pdf.

[7] https://www.ietf.org/rfc/rfc4568/crypto-suites.txt.

[8] S. Wenger, M.M. Hannuksela, "RTP Payload Format for H.264 Video," https://tools.ietf.org/html/rfc3984.

 Digital Object Identifier 10.32754/JMT.2020.1.02