6

Video Communication – Security and Quality Issues

Klaus Keus, Robert Thomys
Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn
Fax.: 0228/9582 455, e-mail: keus, thomys @bsi.de

Abstract

This paper deals with quality and security issues of multimedia applications with respect to video communication. Video communication is a communication service with the need for a specific attention for aspects as security and quality. Both aspects have to be considered very closely: on the one side the definition of *Quality of Service* (QoS) includes aspects of security, on the other side there are parts inside security which will have a direct or indirect influence to the quality parameters of QoS. The further scope and regard of security will be restricted to *Availability*, *Integrity* and *Confidentiality* and will be explained in more detail concerning video communication. Requirements for realtime aspects and requirements for large data amount have to be placed in the planning of security mechanisms and its realization and have to be considered in the description of the QoS parameters under the view of video communication.

Keywords

Video communication, QoS, Availability, Confidentiality, Integrity

1 INTRODUCTION

New classes of network applications combined with slogans as "super data highway" etc. have considerably enlarged in importance in the recent past, so called multimedia applications. On the one side the integration of different information typs as video, audio, wording, data, graphics etc. and on the other side the need for distributed processing of these information have influenced the speed for the development of so called integrated distributed multimedia systems (IDMS). IDMS helps to establish the opportunity for production, processing, presentation, storage and communication of discrete (time independent) and continous (time

R. Posch (ed.), *Communications and Multimedia Security*

dependent) media. Capable and secure communication systems are needed to satisfy all the quality and security requirements of IDMS. Different high speed networks (HSN) for local (LAN), regional (MAN) or wide area (WAN) are designed and in the standardisation phase (e.g. in the actual scene FDDI, FDDI II, DQDB, B-ISDN including ATM Technics) [Par 94, SKB 95].

This paper is restricted to media in the continous field and its focus is video communication, i.e. the transport of sequences of moving pictures in realtime; because this type of information has specific requirements concerning quality and security aspects.

Normally video sequences are compressed with constant (CBR) or variable bit rate (VBR) before transported [RaS 92, KOI 89, NFO 89, VeP 89], the constant bit rate is characterized by variable video quality (constant frame size and meantime arriving time). In opposite to CBR VBR is defined by constant video quality linked with variable frame size. The size of the frame depends on the intensity of the moving inside the scene and the algorithm of the compression. B-ISDN combined with ATM-technology should be preferred for the integration of services and the transportation of video sequences with a variable bit rate.

Actually there are no general accepted security measures or quality models for video communication. Practice including reality measurements in multimedial surrounding is needed to have a well balanced starting situation.

1.1 Video communication interfaces

The figure 1 illustrates possible video communication interfaces over an ATM network respecting the video information transformation [ThB 95], reduced to the behaviour of a transmitter; a receiver executes the same function in reverse order. In following, the interfaces I_1, I_2 and I_3 will be explained in more detail.

The interface I_1 describes the digital and uncompressed video sequences and has following characteristics:

- Pictures *meantime arriving time* (dependent on quality reguirements ca. 20-100 pictures/sec)[IBM 92 a, IBM 92b]
- Pictures format (e.g. 240x256, 1024x1280 pixels)
- Bits number per pixel (e.g. YUV-standard needs 24 bits, i.e.for each component Y, U and V 8 bits respective).

Picture meantime arrival time is important in respect to video transmission and its varation depends on the video application quality requirements between 20 and 100 pictures/sec. The intensity of the motion in scene has no direct influence on the data complexity of this interface.

Example: a workstation with:

Picture format 1024x1280	needs	1,310,720 pixel
and with 24 bits/pixel	needs	31,5 mbits/picture
and with video rate 25 pictures/sec	needs	**787 mbps**

This example demonstrates the dimension of data if no compression methods are insert.

In the next step digital video sequences are coded and compressed. Multiple compression algorithm references for the execution of transformation in different ways are collected in

literature. The most importent and ISO standardized compression algorithm is MPEG *(Moving Pictures Expert Group),* generating a variable bit rate; its compression is based on the two following aspects:

- Spatial redundancy reduction
- Temporal redundancy reduction

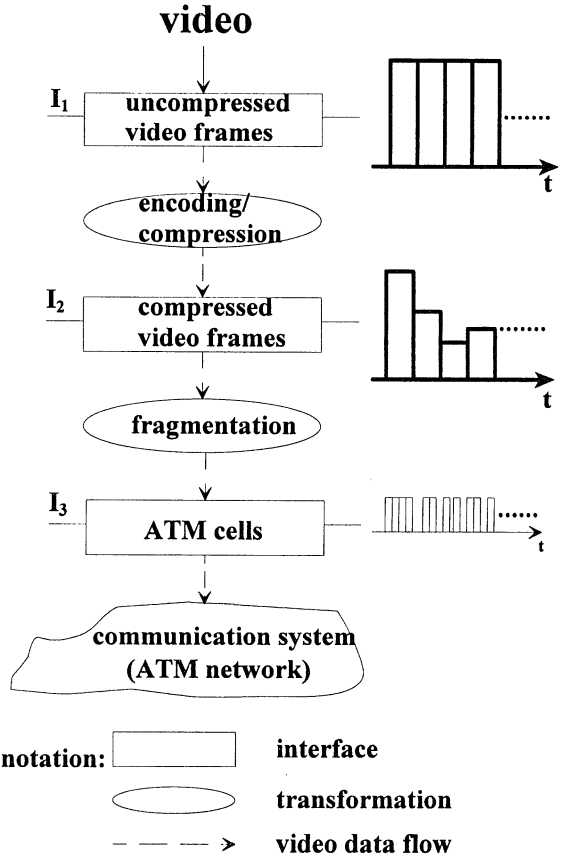

Figure 1 Typical video communication interfaces over ATM network

MPEG is not a loss-free compression algorithm, i.e. the sended and received pictures don't match completely. For some applications with the requirement for very high video quality the compression algorithm with corresponding parameter or other algorithms should be choiced. More details about MPEG and its parameter could be find in [Gal 91, PaZ 92, Ste 93]. On the other hand for video applications without high quality requirements this aspect is not as critical as it seems to be because in most cases the human physionomy isn't able to recognize it.

The interface I_2 provides the compression of the video sequence. The compression algorithms as MPEG generate frames with variable bit rate depending on the algorithm on the one side and on the video application (motion in the scene) on the other one.

After the fragmentation of the compressed video sequence to constant length and to the ATM specific cells format is performed it is passed through the interface I_3. Each ATM cell consists of one block with the fix length of 53 bytes (48 bytes for information area and 5 bytes for the cell header). As ATM network supports variable bit rate, the meantime arriving time of the cells is important.

2 QUALITY ISSUES IN VIDEO COMMUNICATION

In general the video communication quality features may be separated into:

- Functional features
- Performance features

According to functional quality features the following distingstions are useful:

- QoS concept choice, e.g.: Guaranteed/not guaranteed QoS, adaptive QoS
- free choice of kind of connection, e.g.: connectionoriented, connectionless with / without acknowledgement
- Reservation / allocation of resources , e.g.: Storage capacity, CPU time
- Group communication, e.g.: Multicast, Broadcast
- Synchronization level, e.g.: Synchronization between sender and receiver, Synchronization between different video streams [ZSF95], Synchronization inside the video streams
- Security Mechanisms choice, e.g.: Encoding and identification procedures

In according to performance quality features the following separations are useful:

- Minimal acceptable throughput between transport-service-user
- Maximal acceptable transmission delay
- Maximal acceptable variation of delay
- Error rate
- Maximal acceptable number of succesive packages

In combination these features represent an application oriented requirement to the QoS. User defined and required quality features have to be fulfilled and habe to be supported by service providers. Currently the description and mapping of detailled QoS parameter is still in the research status.

3 SECURITY ASPECTS IN VIDEO COMMUNICATION

In the field of IT-Security it has to be distinguished between technical and non technical security measures. Of course non technical measures as e.g. personal, organizational or material issues etc. improve the level of security without controversing the technical aspects

but they will not be considered in this paper furthermore. The further respected technical security countermeasures will be realized depending on the security objectives and assumed threats.

Based on the definitions released in the ITSEC the main focus of this paper is built by the technical understanding of the following IT-Security aspects: [ITS 91]:

- Availability
- Integrity
- Confidentiality

Availability is defined as the prevention of the unauthorized withholding of information or resources. *Integrity* has to be understand as the property of an object to prevent the unauthorized change of information. *Confidentiality* is defined as the property of an object of to prevent the disclosure of information. In the following these security aspects will be tailored with regard to video communication.

3.1 Availability

Availability in the sense of "availability of video communication service performance" has to be regarded in a very close link to QoS which has to be guaranted during the complete transmission time. Otherwise the probability to meet these QoS-requirements has to be clearly defined. As the issue of availability in the ITSEC is not yet finally defined here the availability aspect is not restricted to the behaviour of unauthorized user or malicious attackers, e.g. the unauthorized claim or occupation of resources or information and is based on the more open definition in [KsUlLo94]. If the network doesn't offer any point-to-point connection (as it is in the case of B-ISDN technology, based on ATM-technology) the network resources overload or subsequently data loss may happen. Video communication represents a continous information and hence the reservation of resources (e.g. buffer reservation methods) will become more important. Based on this approach the efficiency of the used reservation method will get more importance with the specific respect to deadlock situation (e.g. during the allocation of resources) which means if the capacity of the network is completely in use any next user will have no chance to get any service. Otherwise the solution of preallocation of resources will not optimize the use of restricted resources, e.g during the process of VBR the frames will have different capacity depending on the motion in scene and the used compression algorithm.

As example the figures 2 and 3 illustrate two results of load measurements of difference video applications [ThB 94]. The video sequence measurements are compressed and agreed with interface I_2 in figure 1. Five motion video application classes *no-, small-, medium-, high-motion and scene changes* are defined. Figure 2 represents video phone as a video application class "small-motion" and figure 3 represents video clips as a video application class "scene changes". These examples explain that the behaviour of the video sequence stronly depends on the intensity of the motion in the scene and on the compression algorithm. Additional to that the behaviour of video users and in detail their load generated has to be taken into account considering the aspect of availability.

a) b)

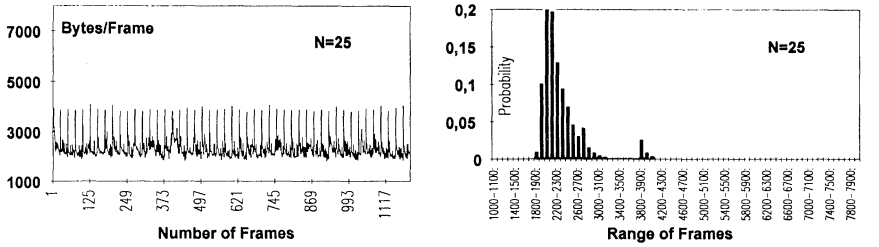

Figure 2 Video phone a) Generated frames, b) Distribution of the frequency of frames

a) b)

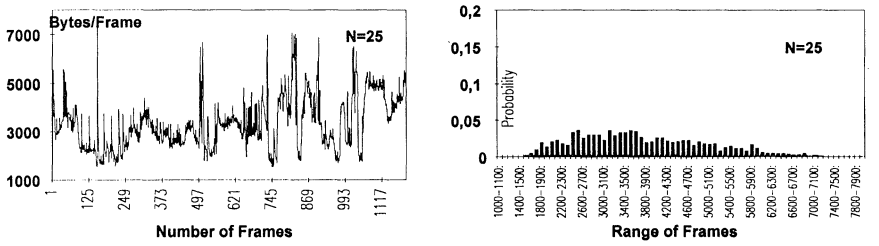

Figure 3 Video clips a) Generated frames, b) Distribution of the frequency of frames

3.2 Integrity

Integrity according to the definition in the ITSEC means preventing unauthorized changes of information by any unauthorized person. Expanding this definition by errors as such one based on the account of network overloading or by transmission errors, communication protocols errors, software or hardware errors etc. means the inclusion as well technical failures as errors based on the attack or the manipulation by unauthorized person (users or external attackers).

With regard to integrity we can distinguish between integrity errors in data transmission and in integrity errors in communication connection. This paper is restricted to the integrity problems in data transmission. In respect to video communication, it can be distinguished between compressed and uncompressed video transmission. Refer to uncompressed video transmission - where a complete picture without any references will be sent - a restricted integrity violation may be accepted depending on the application requirements. Because of the nonrecognition by human eyes the simple change or loss of several bits in a single picture will not have any important impact. On the contrary the loss of several frames in the succession of video sequences will have a relevant influence and will lead to problems at the receiver side, i.e. a new definition for integrity in the field of video communication is required.

In specific the violation of integrity is extremly critical with regard to compressed video communication because the compression algorithm including all the possible parameters has to be tested according to consequences for video quality. On account of strong correlation in in the sequence of compressed video frames a small and relative unimportant violation concerning integrity will have a large effect on the video quality while complete pictures (i.e. including refresh pictures) will be sent only periodically. Hence the real time requirements for compressed video have to be defined more restrictive than uncompressed video communication.

Compressed video may have additional integrity violation. A lot of compression algorithms as MPEG run at a loss of information, i.e. the sent picture differs from the received one. So the definition of an acceptable range including a clear upper limit of integrity violation ΔI_{MAX} for algorithm has to be given.

Both compressed and uncompressed video communication must define a maximal violation integrity parameter $I_{MAX,}$. In the case of compressed video, the behaviour of the compression algorithm and the failure according to this algorithm defined as ΔI_{MAX} must be considered. The fixing of these parameters has to be based on practical measurement refering to the specific video application.

Integrity guaranting procedures shall not violate the video communication real time requirements. So these procedures have to meet at least the following aspects:

- Integrity violation recognition phase
- Correction phase.

For the recognition of integrity violation the value $I_{MIN\ has}$ to be defined in respect to the specifics of the application and under consideration of the compression algorithm. If I_{AV} represents the current integrity violation, then $I_{MIN} \leq I_{AV}$ defines the lower limit of violation.

In the phase of Video correction traditional mechanism based solutions repeating faulty information can't be applied in respect to the strong realtime requirements. Other procedures, e.g. *"forward correction"* based ones should be prefered. The background is based on the fact that additional picture information to be used for correction will be received by the receiver concluding that the video transmission data complexity will increase and as a consequence the realtime restriction will become stronger. The decision for the correction will be based on the relationship of I_{MIN} , I_{MAX} and I_{AV}. Hence in the case $I_{MAX} < I_{AV}$ the video frames will be refused. In the case, that the integrity is not violated, i.e. $I_{MIN} > I_{AV}$ any correction phase would be applied. Any other case with the requirement $I_{MIN} \leq I_{AV} \leq I_{MAX}$ would apply the correction method.

3.3 Confidentiality

The aspect of confidentiality is very important for multiple multi-media applications using video services as video conferencing, video phone, video mail etc., structured on generic headings as:

- Identification
- Authentication
- Access Control
- Audit
- Object Reuse

- Encoding procedure
- Data Exchange.

The requirements for security functions and their technical implementation (security mechanisms) may be oriented at the requirements for traditional IT security applications. The video encoding may be realized in analogous or digital way. Because the analogous methods are easy to break digital encoding methods have to be inserted into video encoding.

Realtime video stream requires specific conditions for the encoding procedures. The popular and for data encoding inserted encoding algorithm DES can be used to encode video stream in realtime. Currently hardware based realisation of DES with an encoding rate larger than 100 mbps in realtime are available. In video encoding both the synchronization information and the pictures itself will be encoded and a compressed MPEG I video stream corresponds between 1-2 bps.

These methods have to meet at least the following two requirements:

1 Encoding in realtime

2 The reconstruction of pictures by unauthorized person has to be avoided.

The encoding should be performed after compression because of two reasons: first the encoding would reduce any structure in the data, hence there wouldn't be any opportunity for further compression. Secondly from the crypto point of view it would be more efficient to encode the redundancy reduced or redundancy free and compressed data instead of the high redundancy one unless realtime hardware based solutions (algorithms) with the property of an encoding capacity larger than 140MBits/s are possible.

4 CLASSIFICATION OF VIDEO APPLICATION

Video applications can be distinguished and rated respecting different criteria. In general if V_A describes the quantity of all possible video applications, C_{AP} describes a class of video applications characterized by the common property P. In [ThB 94] realtime video applications are distinguished into five classes with regard to the motion intensity in the scene. Each class has its specific characteristics and representations concerning the video stream. The video measurements are needed for modeling the video load and analyse the performance in reference to high availability of provided services.

Another video classification refering to security aspects takes into account the three mentioned security aspects S_i, i.e. *Availability,* S_A, *Confidentiality,* S_C and *Integrity,* S_I. Each of these aspects may be rated into different quality levels Q_j depending on user security requirements:

- Q_0: No security required with regard to S_i
- Q_1: Low security required with regard to S_i
- Q_2: Middle security required with regard to S_i
- Q_3: High security required with regard to S_i
- Q_4: Very high security required with regard to S_i.

These video applications with the common security requirements built a security class.

The user security requirements have to be integrated into the QoS specification. As an example of a user security requirement the following video application would give an impression:

Tele-Diagnostic=[S_A with Q_4, S_C with Q_1, S_I with Q_4]

There are two important problems respecting QoS. The first one is to fix the requirements of each quality level Q_j to the security aspects S_I. The second one is the mapping from abstract security description to network and/or other available resources.

5 SUMMERY AND FORWARD

We have had an overview of quality and security aspects in a specific multimedia application, here the video communication. We have identified a fundamental link between security and quality. The definition of QoS (Quality of Service) includes aspects of security, otherwise there is a partly but significant influence of security to the quality parameters inside QoS. Security was explained based on the restricted scope of availability, integrity and confidentiality.

One aspect in the scope of QoS is the availability of service in the sense of dependability and reliability. The efficient and reliable administration of the available band width has to be respected. Hence a well operating matching of the required quality of service to the reliable one is necessary. This tracing has to satify at least the following aspects:

- The behaviour of the user and the resulting effects (e.g. the amount of data and the related burden for transport)
- The applied QoS model including the embedded description of the QoS parameter
- The kind of tracability of the abstract requirements to the quality of service.

In respect to the video communication the restrictive and on traditional dataprocessing based knowledge about the requirements concerning integrity hasn`t to be fulfilled in general. A frame for further decisions for integrity violation was built by the definition of I_{MIN} und I_{MAX}. These values have to be defined based on practical measurement of video sequences in respect to the typ of application and the used algorithm for compression.

The implementation of secure algorithm for crypto and their application in realtime will be required to satify the needs for confidentiality.

A sample of possible solutions for classifications of video communication applications and the related description of the QoS parameters with respect to the specific security and quality aspects by users was explained.

Nevertheless the integration of all these security and quality aspects into the development of IDMS would make a lot of sense and would improve the complete life cycle of the product and its application. This approach would imply partly a shift of the product requirements concerning security and related quality aspects to the process one, i.e. into the process of the development (e.g. in the conceptional and in the constructional sense) and into the process of the production itself, based on detailled technical conditions.

6 REFERENCES

[Gal 91] D. Le Gall: A video compression standard for multimedia applications. *C. ACM, Vol. 34, No. 4, 1991.*

[IBM 92 a] ActionMedia II Developer`s Toolkit: Application Programmer`s Guide, 1992, Part. No. 10G2990

[IBM 92b] ActionMedia II Developer`s Toolkit: Technical Reference, 1992, Part. No. 04G5144

[ITS 91] ITSEC: *Information Technology Security Evaluation Criteria, June 1991*

[KsUlLo94] K. Keus, M. Ullmann, D. Loevenich: Availability in International Harmonized Security Evaluation Criteria, *Post-Workshop Proceedings der Fachtagung IT-Sicherheit, Uni Wien, 22.-23. September 1994, Oldenbourg Verlag Wien ISBN 3-7029-0395-X*

[KOI 89] R. Kishimoto, Y. Ogata, F. Inumaru: Generation Interval Distribution Characteristics of Packetized Variable Rate Video Coding Data Streams in an ATM Network. *IEEE J. on Sel. Areas in Comm., Vol. 7, No. 5, 1989.*

[NFO 89] M. Nomura, T. Fujii, N. Ohta: Basic Characteristics of Variable Rate Video Coding in ATM Environment. *IEEE J. on Sel. Areas in Comm., Vol. 7, No. 5, 1989.*

[Par 94] C. Partridge: Gigabit Networking. *Addison-Wesley Professional Computing series, 1994*

[PaZ 92] P. Pancha, M. El Zarki: A look at the MPEG video coding standard for variable bit rate video transmission. *Infocom '92, Florence, Italy.*

[RaS 92] G. Ramamurthy, B. Sengupta: Modeling and Analysis of a Variable Bit Rate Video Multiplexer. *Infocom '92, Florence, Italy.*

[SKB 95] D. Saha, D. Kandlur, T. Barzilai: A Video Conferencing Testbed on ATM: Design, Implementation and Optimizations. *2nd IEEE International Conference on Multimedia Computing and Systems (ICMCS), May, 1995, Washington D.C.*

[Ste 93] R. Steinmetz: Multimedia-Technologie. Einführung und Grundlagen. *Berlin, Springer, 1993.*

[ThB 94] R. Thomys, L. Bräuer: Messungen für Videoverkehr als Basis für Lastmodelle. *24. GI-Jahrestagung im Rahmen des 13th World Computer Congress IFIP Congress, Hamburg 1994*

[VeP 89] W. Verbiest, L. Pinnoo: A Variable Bit Rate Video Codec for Asynchronous Transfer Mode Networks. *IEEE J. on Sel. Areas in Comm., Vol. 7, No. 5, 1989.*

[ZSF 95] T. Znati, R. Simon, B. Field: A Network-Based Schema For Synchronization Of Multimedia Streams. *2nd IEEE International Conference on Multimedia Computing and Systems (ICMCS), May, 1995, Washington D.C.*

7 BIOGRAPHY

Klaus Keus :

Studied Mathematics, Economics and Computer Sciences at the University of Aachen (RWTH), Germany and got a degree as Diplom Mathematican in 1982. After a long periode of experience in SW-development and named account project manager in several multinational computer companies he joined the BSI. Currently he is head of the division "Accreditation and Licencing" and is involved in multiple national and international IT-Security projects. He has published numerous papers in IT-Security and is involved or member of international program comitees.

Robert R. Thomys:

Studied Navigation from 1983 to 1986 and Computer Science from 1987 to 1993 at the University of Hamburg focused on distributed systems and communication systems; particularly formal specification, parallel and distributed processing, communication technology and protocols in LANs, MANs, WANs area. From 1993 to 1994 assistent for science at the University of Hamburg with the main area of interest in load modeling and performance analyses of innovative communication systems and high speed networks in multimedia area. Now he is at BSI, Department: Scientific Fundamentals and Certification, Division: Accreditation and Licencing