Estratégia de Segurança para Transmissão de Fluxos de Mídia em Alta Definição

Elenilson Vieira da Silva Filho
Lab. de Aplicações de Vídeo Digital
Universidade Federal da Paraíba
elenilson@lavid.ufpb.br

Anderson Vinícius A. Ferreira
Lab. de Aplicações de Vídeo Digital
Universidade Federal da Paraíba
anderson@lavid.ufpb.br

Julio César Ferreira da Silva
Lab. de Aplicações de Vídeo Digital
Universidade Federal da Paraíba
julio@lavid.ufpb.br

Marcello Galdino Passos
Lab. de Aplicações de Vídeo Digital
Universidade Federal da Paraíba
marcello@lavid.ufpb.br

Erick Augusto Gomes de Melo
Lab. de Aplicações de Vídeo Digital
Universidade Federal da Paraíba
erick@lavid.ufpb.br

Tatiana Aires Tavares
Lab. de Aplicações de Vídeo Digital
Universidade Federal da Paraíba
tatiana@lavid.ufpb.br

Gustavo H. M. B. Motta
Lab. de Arquitetura e Sistemas de Software
Universidade Federal da Paraíba
gustavo@di.ufpb.br

Guido Lemos de Souza Filho
Lab. de Aplicações de Vídeo Digital
Universidade Federal da Paraíba
guido@lavid.ufpb.br

ABSTRACT
The domain of Information and Communication Technology has been going through a notable transformation which is characterized by the global connectivity and the increasing use of multimedia devices. These factors have afforded the development of new transmission networks to handle large volumes of data and increasing power transmission. As the development of several multimedia technologies gets faster, even more data are generated and transmitted over the network. When applied to military, commercial and medical fields, for example, a major matter to be concerned about is security and privacy. Thus, this paper presents a secure scheme based on authentication and users authenticity verification as well as based on distribution of encrypted streams. This strategy was developed and integrated to Arthron, a tool for high definition multimedia stream transmission.

RESUMO
A área de Tecnologia da Informação e Comunicação (TIC) tem sofrido uma notável transformação caracterizada pela universalização das formas de conectividade e popularização de dispositivos midiáticos. Tais fatores propiciaram o surgimento de novas redes de transmissão para lidar com grandes volumes de dados e com grande poder de transmissão. Com o rápido desenvolvimento de várias tecnologias multimídia, cada vez mais dados são gerados e transmitidos pela rede. Quando aplicadas a domínios médicos, comerciais e militares, por exemplo, um dos principais pontos a serem considerados é a segurança e privacidade. Assim, este trabalho apresenta uma estratégia de segurança e privacidade, baseada na autenticação e verificação de autenticidade de usuários, além da distribuição de fluxos criptografados. Tal estratégia foi desenvolvida e integrada à Arthron, uma ferramenta para transmissão de múltiplos fluxos midiáticos de alta definição.

Categories and Subject Descriptors
C.2.0 [**COMPUTER-COMMUNICATION NETWORKS**]: Language Contructs and Features –*Security and protection*.

General Terms
Management, Security, Video Streaming.

Keywords
Media Streaming, Security, Videoconference, telemedicine, UDP, AES, RSA.

1. INTRODUÇÃO
A área de Tecnologia da Informação e Comunicação (TIC) passa por uma notável transformação caracterizada pela universalização das formas de conectividade e popularização de dispositivos midiáticos. Tais fatores propiciaram o surgimento de novas redes de comunicação para lidar com grandes volumes de dados e com grande poder de transmissão [1], como a Internet2 [11]. Redes com alto poder de transmissão permitem o desenvolvimento de aplicações com uma grande demanda de banda passante.

Dentre esses cenários encontra-se a transmissão de fluxos de mídia em que, para determinados contextos, faz-se necessário garantir a segurança na transmissão dos fluxos pela rede. Um exemplo de contexto é a Telemedicina. De acordo com Lima et al (2007), entre as diversas modalidades da telemedicina, incluem-se as videoconferências, que permitem a integração em tempo real,

WebMedia'11: Proceedings of the 17th Brazilian Symposium on Multimedia and the Web. Full Papers.
October 3 -6, 2011, Florianópolis, SC, Brazil.
ISSN 2175-9642.
SBC - Brazilian Computer Society

recebendo e enviando áudio e vídeo de alta qualidade entre pontos distantes geograficamente. Para tanto, é necessário utilizar mecanismos de segurança que garantam a transmissão segura de dados.

A ferramenta Arthron fornece um conjunto de componentes para o gerenciamento de transmissão de fluxos midiáticos de forma simples e intuitiva [2], porém o sistema não utiliza qualquer mecanismo de segurança. Para suprir esta carência da Arthron e poder aplicá-la de maneira efetiva no domínio de telemedicina, foi desenvolvida uma estratégia que utiliza métodos de criptografia de chave assimétrica e chave simétrica para garantir a confidencialidade das mídias transmitidas.

Neste artigo, apresentamos, portanto, uma estratégia de segurança e privacidade, baseada na autenticação de usuários e na transmissão de fluxos multimídia criptografados. Esta estratégia foi desenvolvida e integrada à Arthron. São apresentados, ainda, resultados de testes de desempenho realizados para avaliar o impacto da introdução da estratégia de segurança na Arthron. Testes de verificação para o cenário de telemedicina foram realizados no Hospital Universitário Lauro Wanderley para transmissão em tempo real de múltiplos fluxos de vídeo de procedimentos cirúrgicos.

2. SERVIÇOS DE TELEMEDICINA

A telemedicina teve início durante a corrida espacial, na década de 60, quando as funções vitais de astronautas no espaço eram monitoradas na terra por médicos da *National Aeronautics and Space Administration* (Nasa) [5]. No Brasil, uma das ações de telemedicina é a Rede Universitária de Telemedicina (RUTE) [12], uma iniciativa que tem o objetivo de aprimorar a infraestrutura de telemedicina nos hospitais universitários e proporcionar a integração dos projetos entre as instituições participantes.

No entanto, a infraestrutura hoje disponível na RUTE está voltada para o atendimento de serviços de videoconferência através de soluções dedicadas que dispensam o uso de computadores, pois possuem sistema de gerenciamento próprio. Estas soluções são ligadas diretamente a um dispositivo de áudio e vídeo e à rede, porém são mais onerosas que as soluções para computador.

Outra limitação das soluções dedicadas é requerer uma Unidade de Controle Multiponto (*Multipoint Control Unit* – MCU) para prover transmissões com múltiplos pontos. Este cenário é um método viável para a transmissão de informação em tempo real permitindo que cirurgiões de diferentes lugares, distantes geograficamente, trabalhem juntos durante procedimentos cirúrgicos. A estação de broadcast tem que ser capaz de receber vídeo e áudio de computadores geograficamente distribuídos e assim permitir a completa interação entre ambas as partes durante a transmissão. Neste caso, dados relacionados ao paciente devem ser transmitidos, tais como saída de dados de equipamentos médicos [13]. No entanto, a transmissão de múltiplos fluxos também é uma característica intrínseca dos procedimentos cirúrgicos. Esses múltiplos fluxos transmitidos permitem uma melhor avaliação do ambiente (através de diferentes pontos de vista) por todas as partes envolvidas: médicos, alunos ou profissionais. Portanto, apesar das soluções dedicadas existentes suprirem as necessidades de transmissão de fluxos, o alto custo no investimento é um fator importante na decisão de aquisição. Logo, uma solução generalizada voltada para computador se torna uma alternativa de baixo investimento e que pode levar a uma ampla expansão da RUTE.

Uma transmissão de fluxo caracteriza-se pela captura da mídia gerada por alguma fonte (câmera ou arquivo, por exemplo), transformação da mídia para o formato de stream e a consequente transmissão deste stream pela rede. Quando se trata de transmissão em tempo real, a fonte em um ambiente de telemedicina pode ser uma câmera (webcam ou câmera convencional ligada a uma placa de captura), a saída de dispositivos de ultra-som ou raios X, por exemplo, o fluxo gerado por sensores que verificam os sinais biológicos do paciente, entre outras possibilidades que podem variar de acordo com a necessidade do procedimento a ser realizado.

Geralmente os formatos utilizados para transmissão em tempo real são desenvolvidos com base em aspectos inerentes às transmissões. Um desses aspectos é a característica que permite ao cliente acessar o fluxo em qualquer ponto do tempo da mídia, e não apenas a partir do início como acontece no acesso a um arquivo, por exemplo. Para prover a sincronização dos elementos de um fluxo (vídeo, áudio, etc), faz-se necessária a utilização de mecanismos de transporte sinalizado, seja na forma de protocolos de transmissão, seja na forma de sinalização na codificação do vídeo.

Outros fatores importantes estão relacionados à infraestrutura necessária para transmissão de vídeo ao vivo, o que pode causar atrasos ou perda de pacotes na transmissão, características que são particularmente desagradáveis e que devem, portanto, ser minimizadas.

3. MÉTODOS DE CRIPTOGRAFIA

Os métodos de criptografia utilizados neste trabalho são o de chave simétrica e assimétrica [6]. Esses métodos diferem basicamente na forma como utilizam as suas chaves. O método baseado em chave assimétrica necessita de um par de chaves, ditas chave pública e privada, enquanto o de chave simétrica utiliza apenas uma chave que é compartilhada entre os dois pontos participantes da comunicação.

Nos métodos de chave assimétrica, a origem utiliza, para fins de sigilo na comunicação, a chave pública do destino para fazer a criptografia, enquanto o destino utiliza sua chave privada para efetuar a decriptografia. Já o método de criptografia de chave simétrica utiliza uma única chave para criptografar e decriptografar. Tais métodos diferem também em seu desempenho, em que os de chave assimétrica são quase 1000 vezes mais lentos que os de chave simétrica [7]. Porém, na criptografia de chave simétrica é necessário o compartilhamento da chave entre os dois pontos. Portanto, sistemas que requerem comunicação segura e alto desempenho comumente utilizam um algoritmo de chave assimétrica para o compartilhamento da chave simétrica entre os dois pontos participantes da comunicação e, a partir de então, utilizam apenas a chave simétrica compartilhada para a troca de informações.

Os algoritmos utilizados neste trabalho são: o *Rivest-Shamir-Adleman* (RSA) de 1024 bits [4], como algoritmo de chave assimétrica e o *Advanced Encryption Standard* (AES) de 128 bits [3], como algoritmo de chave simétrica. Esses algoritmos foram escolhidos por serem considerados como algoritmos padrão de criptografia [8]. Como o AES é um método de criptografia em bloco, faz-se necessária uma adaptação para funcionamento como método de criptografa em fluxo. Neste modo de operação, cada bloco passa a ser criptografado em função de todos os blocos anteriores, e não apenas em função de si mesmo [9].

A transmissão de fluxos multimídia pela rede é uma tarefa que requer que os dados transmitidos sejam enviados com tempo de atraso delimitado e que os dados sejam exibidos em uma determinada taxa [10]. A criptografia de fluxos multimídia deve, portanto, ser feita em tempo reduzido e requerer baixo custo adicional a fim de que não influencie na exibição dos dados. A Figura 1 mostra um framework geral para a transmissão segura de fluxo multimídia. Entretanto, para aplicações em tempo real não existe buffer para o fluxo multimídia, visto que o fluxo deve ser exibido assim que requisitado.

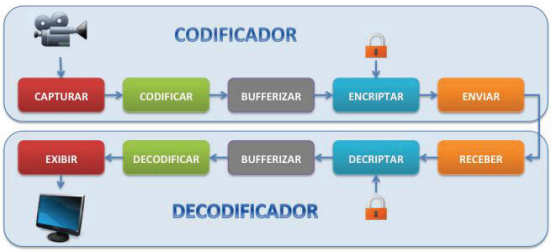

Figura 1: Framework geral para transmissão segura de fluxo. Fonte: Adaptado de [10].

4. TRABALHOS CORRELATOS

Asghar et al (2010) propõem um esquema de segurança com intenção de aplicar o máximo de segurança possível na transmissão de conteúdo multimídia pela rede. O esquema de segurança realiza, para isso, autorização de usuários, gerenciamento de chaves, criptografia, empacotamento e esquemas de autenticação. No esquema proposto, o processo de autorização é feito liberando o acesso à rede apenas para usuários cadastrados, as chaves são geradas por intermédio do mecanismo de troca de chaves *Diffie-Hellman*, o algoritmo AES é usado para criptografia dos dados e, então, os dados criptografados são embarcados em um cabeçalho SRTP (*Secure Real-Time Transport Protocol*). Os informes do *Sender* e *Receiver* do SRTCP (*Secure Real-Time Transport Control Protocol*) também são gerados para reconhecimento dos dados. Um algoritmo *keyed-hash* é usado para gerar um MAC (*Message Authentication Code*) para cada pacote SRTP. Após todos esses processos, os dados podem então trafegar pela rede. A Figura 2 ilustra este processo.

Figura 2: Esquema de segurança de transmissão segura de conteúdo multimídia. Fonte: Adaptado de [14].

Aly et al (2004) apresentam uma proposta de criptografia para transmissão de vídeo em tempo real utilizando o algoritmo de criptografia AES. Neste trabalho o autor tem como objetivos determinar como a criptografia pode ser implementada para aplicações de vídeo em tempo real, bem como computar o desempenho e o custo adicional da segurança multimídia. Em seus resultados, eles mostram que a utilização do AES é uma solução viável para transmissão de vídeo em tempo real, visto que o desempenho da encriptação é suficiente para mostrar os quadros recebidos em tempo real e com baixo custo adicional.

5. ESTRATÉGIA PROPOSTA

A estratégia desenvolvida fundamenta-se na autenticação de todas as fontes e destinos de vídeos, bem como, na transmissão criptografada dos fluxos de mídia.

Uma forma de abordar a transmissão segura de múltiplos fluxos é o compartilhamento de uma chave simétrica para cada par de usuários (fonte/destino). Todavia, esta estratégia é inviável devido ao alto custo de processamento na criptografia de um fluxo diferente para cada destino, pois para cada par de usuários um novo processo de criptografia dos dados deverá ser realizado, já que a chave de criptografia é diferente para cada par de usuários.

A ilustração desse cenário pode ser visualizada na Figura 3.

Figura 3: Cenário ideal para transmissão de múltiplos fluxos criptografados.

Para contornar essa limitação, o conceito de sessão surge como uma alternativa. A definição de sessão em dicionários de língua portuguesa é dada como um espaço criado para agrupar usuários e compartilhar dados em uma reunião deliberativa. Este conceito foi, portanto, utilizado para modelar o esquema de segurança utilizando sessões. Uma sessão criada pode ser moderada ou não, o que implica na permissão de acesso a suas informações para quaisquer usuários ou apenas para usuários convidados pelo seu criador. A Figura 4 ilustra este último cenário, atribuindo à sessão uma chave simétrica compartilhada entre todos os seus usuários. Desta forma, a criptografia é realizada uma única vez e o fluxo criptografado é distribuído a todos os destinos desejados.

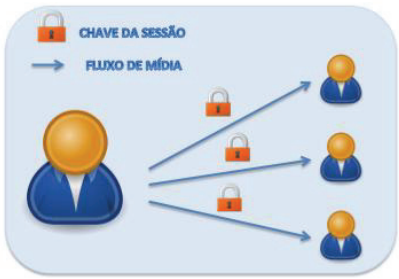

Figura 4: Cenário de criptografia de múltiplos fluxos utilizando sessão.

A autenticação é realizada por intermédio de consultas a um cadastro de usuários localizado em um servidor centralizado. Os dados cadastrados são: nome de usuário, nome, endereço *e-mail*, tipo de perfil, chave pública e o *hash* da chave privada. Esses dados são descritos na Tabela 1.

Tabela 1: Descrição dos dados do usuário armazenados no servidor

DADO	DESCRIÇÃO
NOME	Nome do usuário
NOME DE USUÁRIO	Identificador do usuário
EMAIL	*E-mail* do usuário
TIPO DE PERFIL	Define permissões
CHAVE PÚBLICA	Chave pública utilizada pelo AES para comunicação com o servidor
HASH DA CHAVE PRIVADA	O *hash* da chave privada utilizada pelo RSA

Os dados armazenados da sessão são: identificador, data de início e término, criador da sessão, usuários participantes, chave simétrica e a informação se é moderada. Esses dados são descritos na Tabela 2.

Tabela 2: Descrição dos dados da sessão armazenados no servidor

DADO	DESCRIÇÃO
IDENTIFICADOR	Identificação única da sessão
DATA DE INÍCIO	A data da criação da sessão
DATA DE TÉRMINO	A data de finalização da sessão
CRIADOR	O usuário criador da sessão
USUÁRIOS PARTICIPANTES	Os usuários participantes (convidados pelo criador ou que requisitaram acesso)
CHAVE SIMÉTRICA	Chave secreta utilizada para criptografia/decriptografia dos fluxos, utilizada pelo algoritmo AES
MODO	Designa se a sessão é moderada. Quando moderada, apenas usuários convidados pelo criador podem acessar

O processo de autenticação tem início com a requisição ao servidor de um valor aleatório, valor este que é enviado ao usuário de forma confidencial utilizando o algoritmo RSA. O cliente concatena a esse valor o *hash* da chave privada RSA e gera um *hash* dessa concatenação, valor este denominado "token". Esse valor é enviado ao servidor de forma confidencial utilizando o RSA e o servidor repete o processo de criação do *token* comparando sua igualdade. Caso os valores sejam iguais, está concluída a autenticação do usuário e o valor aleatório recebido se torna a chave simétrica AES a ser utilizada para futuras comunicações entre o usuário e o servidor. Essa estratégia garante que apenas o portador da chave privada, ou seja, o usuário crie um *token* corretamente e, para cada nova conexão, um novo *token* será gerado. O processo de autenticação é mostrado na Figura 5.

Figura 5: Processo de autenticação e posterior troca de dados entre cliente e servidor.

Na comunicação entre os usuários, o solicitante envia um segundo *token* ao destino, *token* este que consiste em um *hash* da concatenação do *token* criado para autenticação no servidor com o nome de usuário destino. O usuário destino envia o *token* recebido ao servidor juntamente com o nome do solicitante. O servidor faz o mesmo processo de criação desse novo *token* e verifica a igualdade com o *token* do usuário solicitante, informando ao usuário destino a autenticidade ou não do usuário solicitante. Dessa forma o usuário destino pode aceitar ou rejeitar a conexão do usuário solicitante. Essa estratégia permite a verificação de intrusão já que impossibilita que um usuário se passe por outro, visto que, na verificação de autenticidade, um usuário usa um *token* diferente para cada outro usuário.

A Figura 6 descreve o processo de verificação de autenticidade de usuários onde o cliente A está devidamente autenticado e tem sua conexão aceita pelo cliente B. Já o cliente C tenta se passar pelo cliente A, forjando um valor de *token*, porém o servidor informa a não autenticidade de C e B rejeita a conexão.

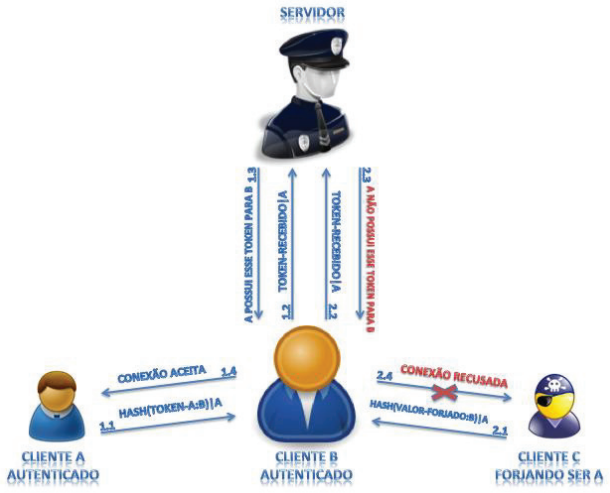

Figura 6: Verificação de autenticidade de clientes no servidor.

Entre os recursos a serem protegidos estão os fluxos enviados entre os usuários da sessão e estes são previamente criptografados utilizando sua chave simétrica do AES e decriptografados nos destinos que possuírem essa chave.

O modo de operação do AES utilizado neste trabalho é o Modo Contador (*Counter Mode*), em que o próximo bloco é gerado por intermédio da encriptação de sucessivos valores de um "contador". O contador pode ser qualquer função que produza uma sequência que garantidamente não se repetirá por um longo tempo, embora um contador de fato seja a solução mais simples e popular. A Figura 7 ilustra o esquema de encriptação do AES no Modo Contador.

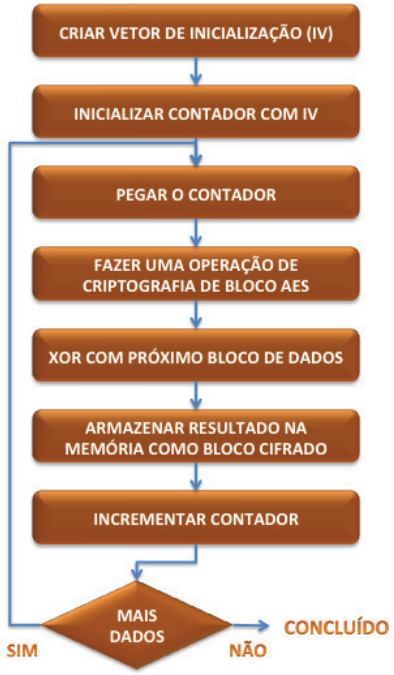

Figura 7: Esquema de encriptação do AES no Modo Contador.

6. ESTUDO DE CASO

A estratégia foi implementada e está sendo utilizada na segunda versão da ferramenta Arthron. A Arthron 2.0 tem como principal foco atender os requisitos de transmissão de múltiplos fluxos simultâneos em um ambiente cirúrgico. O domínio de telemedicina exige uma segurança diferenciada para garantir a confidencialidade dos dados a serem transmitidos.

6.1 Arthron 1.0

A Arthron [02] é uma ferramenta desenvolvida com o intuito de gerenciar e articular remotamente fontes distribuídas de mídia com diferentes formatos de codificação em eventos de cunho artístico-tecnológico. Ela é formada basicamente por oito componentes: Decodificador, Codificador, Refletor, Articulador, Gerenciador de Mapas, Servidor de Vídeo para Web, Monitor e Gerador de Cenário, em que cada módulo tem um papel específico na preparação de um evento e podem estar localmente ou geograficamente distribuídos na rede.

A Figura 8 ilustra a arquitetura dos componentes da Arthron 1.0 que estão diretamente envolvidos com fluxos de mídia.

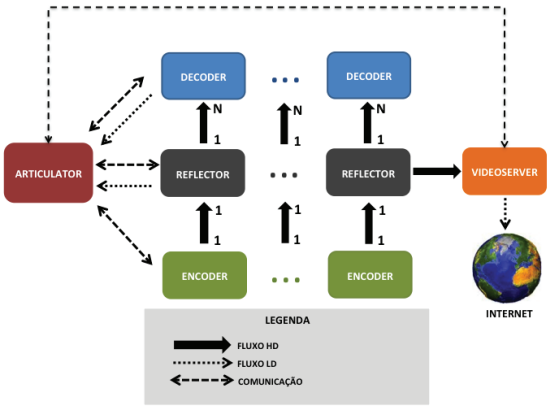

Figura 8: Arquitetura da Arthron 1.0. Fonte: Adaptado de [15].

6.2 Arthron 2.0

Para a construção da Arthron 2.0 os requisitos de segurança e videoconferência foram os que guiaram as mudanças. Novos módulos foram criados para atender esses requisitos: o *WebService* para gerenciar a criptografia e o *VideoRoom* para propiciar uma interface com o usuário mais intuitiva para videoconferências. A arquitetura da versão 2.0 está ilustrada na Figura 9.

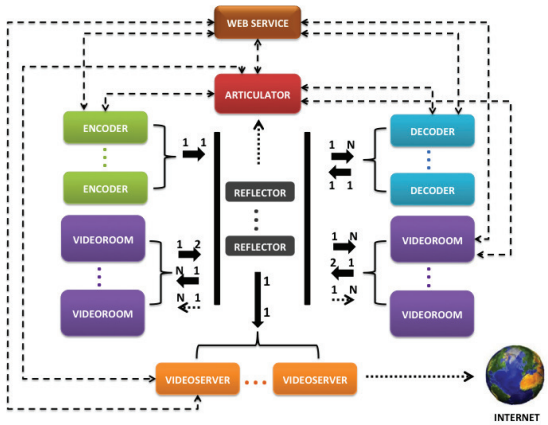

Figura 9: Arquitetura da Arthron 2.0

Na aplicação da estratégia de segurança, o componente *WebService* representa o servidor. Ele é responsável por manter o cadastro de usuário, possibilitar a criação e gerenciamento de sessões e gerenciar a autenticação e verificação de autenticidade desses usuários.

Os componentes Articulador, Codificador, Decodificador e Refletor são componentes que gerenciam, enviam, recebem ou replicam fluxos de mídia. Para cada um destes componentes há um usuário associado. A comunicação entre os componentes e a consequente troca de conteúdo é permitida apenas após autenticação no WebService e verificação de autenticidade de seus usuários.

A Figura 10 ilustra a aplicação da estratégia de segurança na Arthron 2.0.

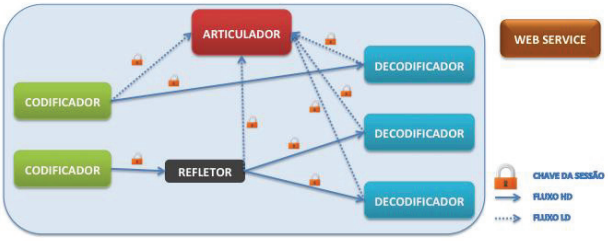

Figura 10: Estratégia de segurança aplicada à Arthron 2.0

6.3 Experiências de Uso

A utilização da Arthron na telemedicina envolve uma proposta para transmissão de cirurgias em dois hospitais universitários da rede RUTE: o Hospital São Paulo da UNIFESP e o Hospital Universitário Lauro Wanderley (HULW) da UFPB. Em ambos os casos é exigida a gerência remota e a captura e distribuição segura de múltiplos fluxos simultâneos (vídeo, áudio e parâmetros clínicos).

No primeiro caso - Hospital São Paulo da UNIFESP – o objetivo é transmitir um procedimento cirúrgico baseado em quatro fluxos simultâneos de vídeo, cujo nome é cirurgia de implante transapical de valva aórtica. Neste procedimento uma prótese é utilizada para substituir a válvula problemática que pode ser implantada por um corte mínimo, sendo conduzida até o peito por meio de um cateter. Durante o procedimento, o coração continua batendo e não há necessidade do equipamento de circulação extra-corpórea. Este procedimento exige uma alta complexidade para sua execução e ainda é mais complexo o seu acompanhamento por alunos ou outros profissionais in loco. A Figura 11 mostra a dinâmica desse procedimento onde podemos observar o número elevado de envolvidos.

Para contornar o problema do pouco espaço na sala de cirurgia e permitir o acompanhamento de um número maior de expectadores, a Arthron será utilizada para prover a interação entre o professor na sala de cirurgia e outros participantes geograficamente distribuídos.

Figura 11: Procedimento cirúrgico que demonstra uma aula aos alunos do médico

No Hospital Universitário Lauro Wanderley (UFPB) a Arthron já foi utilizada para transmissão cirúrgica. Nas experiências realizadas foram feitas a transmissão de múltiplos fluxos entre a sala de cirurgia, onde o procedimento cirúrgico foi realizado, a sala de telemedicina, onde alunos e professores acompanhavam e interagiam com o procedimento em tempo real.

O procedimento transmitido foi uma cirurgia de hérnia inguinal utilizando videolaparoscopia conforme pode ser observado na Figura 12. Neste experimento, um cirurgião executou a cirurgia enquanto outro médico acompanhava o procedimento com seus alunos na sala de telemedicina do HULW conforme pode ser observado na Figura 13. Os médicos poderiam interagir através de áudio e imagem a qualquer momento da cirurgia, dessa forma a condução da aula tornou possível o acompanhamento remoto de todo procedimento. Duas câmeras foram utilizadas durante o experimento: a endocâmera (visão interna) e uma câmera externa na sala de cirurgia.

A Figura 14 exibe o Articulador, módulo que gerencia os fluxos capturados pelos Codificadores e exibidos pelos Decodificadores onde podemos observar os fluxos que são manipulados durante a cirurgia.

A sala de cirurgia e a sala de telemedicina enviavam e recebiam fluxos, o que permitia uma interação entre os participantes das duas salas. Um fluxo multimídia era capturado na sala de telemedicina e exibido na sala de cirurgia e dois fluxos multimídia eram capturados na sala de cirurgia e exibidos na sala de telemedicina, porém apenas um era exibido por vez. Esses fluxos eram chaveados de acordo com a necessidade dos participantes em ver o procedimento cirúrgico de diferentes ângulos. Os pesquisadores no LAViD acompanhavam os acontecimentos de ambas as salas, porém não enviavam fluxo para nenhuma das salas.

As impressões do experimento realizado foram de boa avaliação entre médicos, alunos e pesquisadores do LAViD. Foi gerada uma expectativa para atividades similares e a possibilidade da adoção do método como parte das aulas realizadas no hospital.

Figura 12: Visão Esquemática da Cirurgia

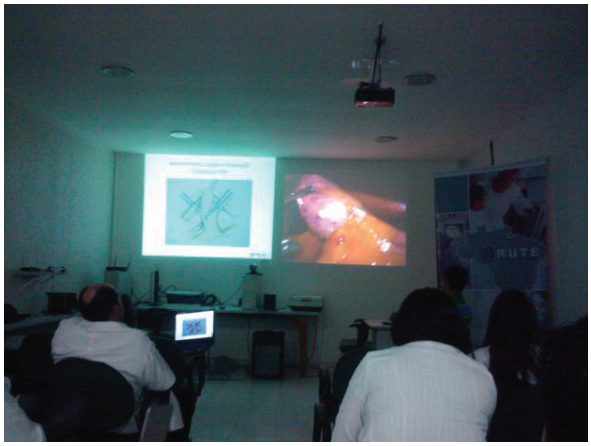

Figura 13: Visão da sala de telemedicina no HULW

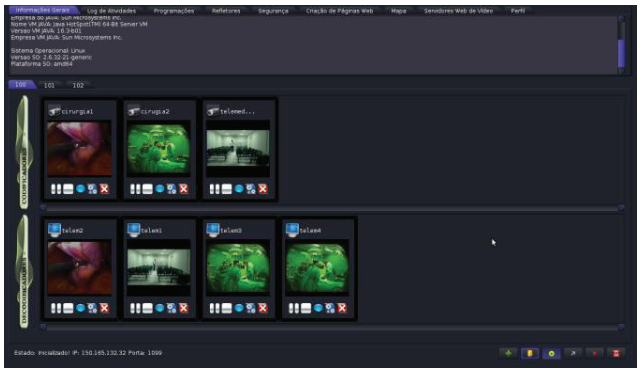

Figura 14: Articulador gerenciando a transmissão de uma cirurgia no Hospital Lauro Wanderley da UFPB

7. RESULTADOS E DISCUSSÃO

Os resultados apresentados a seguir foram obtidos em uma sequência de testes realizados com computadores com processador Intel Core 2 Duo T5850 de 1.6 Ghz com 4 Gb de memória DDR3 1333Mhz. Os computadores possuíam Sistema Operacional GNU/Linux Ubuntu 10.04 de 32 bits. Os testes foram realizados utilizando um Codificador, um Decodificador e um Articulador onde cada módulo foi executado em uma máquina separada sem a execução de qualquer outra aplicação, exceto o Monitor de Sistema do próprio Ubuntu.

Para os cenários que envolvem a codificação do fluxo multimídia, a Tabela 3 descreve a codificação de vídeo e a Tabela 4 descreve a codificação de áudio utilizadas no Encoder, no Decoder e no vídeo utilizado para os testes.

Tabela 3: Codificações de vídeo utilizadas nos testes

	Encoder	Decoder	Video Teste
Codec	**MP4V**	**MP4V**	**MPEG-2**
Taxa de bits	**8192kbps**	**4096kbps**	**841kbps**
FPS	**30**	**30**	**25**
Escala	**1**	**1**	**1**
Largura	**640**	**640**	**480**
Altura	**480**	**480**	**576**

Tabela 4: Codificações de áudio utilizadas nos testes

	Encoder	Decoder	Video Teste
Codec	**MPGA**	**MPGA**	**MPEG-1**
Taxa de bits	**64kbps**	**64kbps**	**224kbps**
Taxa de amostragem	**44100**	**44100**	**44100**
Canais	**1**	**1**	**2**

A implantação da estratégia de segurança na Arthron 2.0 causou impactos no processamento conforme exibido na Tabela 5. Neste trabalho, o impacto no processamento foi medido como a diferença entre a média do percentual de processamento da CPU executando os módulos com e sem segurança. Nessa tabela é possível perceber que os impactos não são muito significativos no Articulador já que seu processamento aumentou pouco mais que 3 pontos percentuais. Os principais impactos ocorreram no Codificador e no Decodificador sem utilização de codificação em que os impactos chegaram perto dos 9 pontos percentuais. Pode-se notar, também, que no cenário de fluxos criptografados sem codificação a utilização da CPU foi mais intensa que no cenário com codificação. Isto se deve ao fato de que a codificação utilizada diminui o tráfego de dados pela rede, ou seja, a quantidade de dados a serem criptografados e decriptografados é menor em relação ao cenário sem codificação. Foi possível observar que a implantação da estratégia de segurança não causou impactos significativos na utilização de memória.

A Tabela 6 ilustra os limites de execução dos módulos da Arthron sem e com a utilização de criptografia dos fluxos enviados/recebidos. Esses testes foram realizados executando vários módulos iguais em uma mesma máquina até seu processador atingir o limite de 100% de utilização. É possível observar que, apesar de quase idênticos, os impactos causados no Codificador são mais notáveis do que no Decodificador. Esse fato é facilmente percebido nas linhas que tratam do Decodificador com criptografia e sem codificação e na linha com criptografia e com codificação, em que ambas tiveram o mesmo limite: 4 Decodificadores.

Tabela 5: Impactos de processamento na Arthron com a adição de segurança

Cenário	Módulo	CPU	Memória
Fluxos Criptografados sem Codificação	Codificador	8,95%	0%
	Decodificador	7,1%	1,1%
	Articulador	1,35%	0%
Fluxos Criptografados com Codificação	Codificador	1,65%	0,6%
	Decodificador	3,95%	0%
	Articulador	3,1%	0%
Fluxos Criptografados no Articulador (miniatura)	Codificador/ Decodificador	3,2%	0%
	Articulador	2,56%	0%

Tabela 6: Limites de execução dos módulos da Arthron com e sem criptografia e codificação dos fluxos

Módulo	Criptografia	Codificação	Quantidade
Codificador			6
Codificador		X	4
Codificador	X		4
Codificador	X	X	2
Decodificador			6
Decodificador		X	4
Decodificador	X		4
Decodificador	X	X	4

8. CONSIDERAÇÕES FINAIS

A estratégia visa contemplar a aplicação da Arthron em cenários onde é necessária a transmissão de fluxos midiáticos com segurança. A evolução da Arthron para o âmbito de telemedicina integrado com o esquema proposto neste trabalho atendeu as expectativas iniciais em prover uma estrutura eficiente, intuitiva e com menor custo financeiro em relação às soluções dedicadas utilizadas na RUTE.

Como trabalhos futuros propõe-se a verificação de aplicabilidade da estratégia de segurança em outros domínios como teatros conectados e cinema digital.

9. AGRADECIMENTOS

Agradecemos à CAPES e a Rede Nacional de Ensino e Pesquisa (RNP) pelo apoio financeiro e ao Hospital Universitário Lauro Wanderley pela contribuição para realização deste trabalho.

10. REFERÊNCIAS

[1] MELO, E. A. G. et al. Arte e tecnologia: Lições aprendidas com a realização de performances artísticas baseadas na distribuição de conteúdo multimídia. In: Conferência Latino Americana de Informática. 2009. Pelotas, RS.

[2] MELO, E. A. G. et al. ARTHRON 1.0: Uma Ferramenta para transmissão e gerenciamento remoto de fluxos de mídia. In: Simpósio Brasileiro de Redes de Computadores. 2010. Gramado, RS.

[3] AES. Disponível em: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>. Acesso em: 3 fev. 2011.

[4] RSA. Disponível em: <http://people.csail.mit.edu/rivest/Rsapaper.pdf>. Acesso em: 20 jan. 2011.

[5] LIMA, Claudio Marcio Amaral de Oliveira et al . Videoconferências: sistematização e experiências em telemedicina. Radiol Bras, São Paulo, v. 40, n. 5, out. 2007 . Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-39842007000500012&lng=pt&nrm=iso>. Acesso em 14 mai. 2011.

[6] STALLINGS, William. Criptografia e segurança de redes – 4. ed. – São Paulo: Pearson Prentice Hall, 2008.

[7] MINAAM, D. S. A. et al. Evaluating the effects of symmetric cryptography algoritms on power consumption for different data types. In: International Journal of Internet Security, Vol. 11, No.2, PP.78-87, Sept. 2010.

[8] ABOMHARA, M. et al. An Overview of Video Encryption Techniques. In: International Journal of Computer Theory and Engineering, Vol. 2, No.1, Feb. 2010.

[9] DWORKIN, M. Recommendation for Block Cipher Modes of Operation. NIST Special Publication 800-38A. 2001. Disponível em; <http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf >. Acesso em: 15 maio 2001.

[10] ALY, S. A Light-Weight Encrypting For Real Time Video Transmission. College of computing and digital media, Depaul university. 2004.

[11] Internet2. Disponível em: <http://www.internet2.edu/about/>. Acesso em: 14 de mai. 2011.

[12] RUTE. Disponível em: <http://rute.rnp.br/>. Acesso em: 14 de mai. 2011.

[13] ZHANG, F. LI, B. Medical Video Stream Transmission in Telemedicine. In: IEEE International Conference on Automation and Logistics. 2007. Jinan, China.

[14] ASGHAR, M. et al. A Secure Scheme for Video Streaming Using SRTP AES and DH. In: European Journal of Scientific Research. 2010.

[15] MELO, Erick Augusto Gomes de. ARTHRON: UMA FERRAMENTA PARA GERENCIAMENTO E TRANSMISSÃO DE MÍDIAS EM PERFORMACES ARTÍSTICO-TECNOLÓGICAS. Dissertação de Mestrado defendida em 05/11/2010. Disponível em http://www.ppgi.di.ufpb.br/wp-content/uploads/dissertacao-itvnews-marcelo300810final.docx Acessado em maio de 2011.