



I EAICTI

I Encontro Anual de Iniciação Científica, Tecnológica e Inovação

DEFINIÇÃO E AVALIAÇÃO DE MÉTODOS DE SEGURANÇA PARA TRANSMISSÃO DE VÍDEOS RELATIVOS A PROCEDIMENTOS MÉDICOS

Leandro A. Ensina (PIBIC/CNPq/UNIOESTE)¹, Newton Spolaôr¹, Renato B. Machado¹, Wu Feng Chung^{1 2}, Hwei Diana Lee (Orientadora)^{1 2}, e-mail: hueidianalee@gmail.com.

¹Universidade Estadual do Oeste do Paraná (UNIOESTE)/Centro de Engenharias e Ciências Exatas/Foz do Iguaçu, PR.

²Universidade Estadual de Campinas (UNICAMP)/Faculdade de Ciências Médicas/Campinas, SP.

Área e subárea: Ciências Exatas e da Terra – Ciência da Computação

Palavras-chave: telemedicina, *streaming* de vídeo, videocoloscopia

Resumo

Cidades de menor densidade populacional e afastadas de grandes centros urbanos sofrem com a falta de especialistas em diversas áreas da saúde. O Laboratório de Bioinformática da Universidade Estadual do Oeste do Paraná, em parceria com o Serviço de Coloproctologia da Universidade Estadual de Campinas, desenvolveu o Sistema de Telemedicina em Tempo Real, a fim de auxiliar em procedimentos médicos à distância, via Internet. Nesse contexto, é importante garantir a segurança dos dados relativos a esses procedimentos, principalmente em se tratando de informações pessoais de pacientes, como laudos de exames, vídeos e imagens. Este projeto tem como objetivo o estudo e a incorporação de características complementares, a partir das funcionalidades previamente implementadas no Sistema de Telemedicina em Tempo Real, por meio de regras de segurança e de configuração do servidor de *streaming*. Essa configuração permite, por exemplo, criptografar a conexão entre cliente e servidor por meio de *Hyper Text Transfer Protocol Secure*. Os experimentos realizados mostram que o protótipo é funcional, não apresentando perda significativa na qualidade da transmissão de vídeo.

Introdução

O avanço tecnológico dos últimos anos, em especial da área computacional, tem favorecido a ampliação de possíveis aplicações de recursos computacionais em diversas áreas do conhecimento (Shortliffe & Cimino, 2006; Urtiga *et al.*, 2004).

Paralelamente a esta constatação, observa-se que a concentração de profissionais especialistas da área da saúde nos grandes centros urbanos repercute no fato de que muitas cidades, menores e afastadas de grandes centros urbanos, têm carência por médicos em diversas especialidades (Shortliffe & Cimino, 2006).



I EAICTI

I Encontro Anual de Iniciação Científica, Tecnológica e Inovação

Neste contexto, o Laboratório de Bioinformática da Universidade Estadual do Oeste do Paraná (LABI/UNIOESTE) em parceria com o Serviço de Coloproctologia da Faculdade de Ciências Médicas da Universidade Estadual de Campinas, desenvolveu o Sistema de Telemedicina em Tempo Real (S2TR). Este sistema é direcionado à área médica, e tem como principal objetivo a interação entre médicos e especialistas, de modo remoto e em tempo real, por meio de vídeo, áudio, texto e imagens, via Internet (Machado *et al.*, 2012; Wu *et al.*, 2014).

Partindo das funcionalidades previamente disponibilizadas no S2TR, neste trabalho foram estudadas e implementadas características complementares, agregando regras de segurança e de configuração. Também foi avaliado o desempenho da transmissão de vídeos considerando esses aspectos de segurança.

Materiais e Métodos

Para o desenvolvimento deste projeto, foram utilizados equipamentos, ferramentas e linguagens, sendo os principais:

- Computador com sistema operacional Windows 8.1, processador Intel Core I7, 8 GB de memória principal, HD 7200rpm 500 GB e placa de rede 1000 Mbps;
- Linguagens de programação: Java, Adobe Flex e ActionScript;
- Servidor de *streaming*: Red5 Media Server;
- Sistema Gerenciador de Banco de Dados (SGBD): MySQL.

O processo de desenvolvimento do protótipo foi dividido em cinco fases:

- Fase 1: Pesquisa Bibliográfica e Embasamento Teórico;
- Fase 2: Estudo e Compreensão das Soluções Previamente Desenvolvidas;
- Fase 3: Pesquisa de Métodos e Tecnologias Computacionais;
- Fase 4: Modelagem, Implementação e Avaliação do Protótipo;
- Fase 5: Publicação dos Resultados.

Na Fase 1, o projeto foi iniciado com o estudo de trabalhos científicos relacionados às áreas da saúde e da computação. O entendimento do estado da arte em telemedicina e em segurança da informação foi necessário para prover embasamento para o desenvolvimento deste projeto.

A Fase 2 compreendeu o estudo de soluções previamente desenvolvidas, como o Método Computacional para Acompanhamento de Procedimentos Médicos em Tempo Real, e o S2TR (Machado *et al.*, 2012; Wu *et al.*, 2014).

Na Fase 3 foi realizado o estudo das tecnologias computacionais a serem utilizadas durante o desenvolvimento do protótipo, bem como as linguagens de programação e o servidor de *streaming* descritos anteriormente.

Para a modelagem e a implementação na Fase 4, foram utilizadas técnicas de Engenharia de Software, como o diagrama de casos de uso e o diagrama de atividades, presentes na *Unified Modeling Language* (UML). Com base nestes



I EAICTI

I Encontro Anual de Iniciação Científica, Tecnológica e Inovação

diagramas, o protótipo foi desenvolvido para ambiente Web, por meio do paradigma cliente/servidor, sendo utilizado para o seu desenvolvimento as linguagens Flex e ActionScript para o cliente e Java para o servidor. Para *streaming* de vídeo, foi utilizado o Red5 Media Server, e o SGBD MySQL para o banco de dados. Ainda na Fase 4, foram realizados testes de funcionamento do protótipo proposto.

A Fase 5 compreende a publicação dos resultados deste projeto.

Resultados e Discussão

No protótipo proposto neste trabalho foram inseridas opções de configuração de *streaming*, como possibilidade de alteração de qualidade (de 1 a 100%), resolução e taxa de quadros por segundo (QPS). Foram incluídas regras de segurança, como autenticação do usuário, mantendo a senha armazenada de modo criptografado, utilizando o sumário de mensagem *Message Digest 5* (MD5), o qual gera uma *hash* da senha original e a armazena no banco de dados. Também foi inserida a adição e a exclusão de domínios autorizados para acessar o protótipo.

Outra característica importante incluída neste protótipo foi a troca do protocolo HTTP (*Hyper Text Transfer Protocol*) pelo HTTPS (*Hyper Text Transfer Protocol Secure*), permitindo a criptografia na comunicação entre o cliente e o servidor e, portanto, maior segurança na troca de informações. A utilização do HTTPS garante confidencialidade (criptografia dos dados), integridade (garantia de que os dados não sejam alterados no caminho) e autenticação. Esses pontos positivos, destacados no HTTPS, não ocorrem no HTTP, uma vez que com a adoção do último qualquer usuário da rede pode interceptar os dados e utilizá-los indevidamente.

Para a avaliação do protótipo, foram instanciados componentes do S2TR (emissor, servidor e cliente) para transmissão de um Vídeo real de Exame (VE) de coloscopia, com resolução de 720x480 *pixels*, sete (7) minutos de duração, taxa de transmissão (*bit rate*) de 12 megabits e 25 quadros por segundo (QPS). O emissor foi representado por uma máquina virtual (MV) Ubuntu, com um processador Intel Xeon 2,40GHz, 512MB de memória e FFmpeg, um programa que simula *stream* de áudio e vídeo. Para atuar como servidor, foi destinada uma máquina virtual Windows XP, com dois processadores Intel Xeon 2,40GHz e 4GB de memória. Ambos estão alocados no servidor de máquinas virtuais HP ProLiant ML350 G6, gerenciado pelo sistema XenServer 6.2. Já o cliente, um *laptop* Windows 8.0 64 bits, possui processador Intel I3 2ª geração 1,50 GHz e 4GB de memória.

Ao todo, foram realizadas cinco (5) transmissões de sete (7) minutos cada (duração do VE). Nesses experimentos foram coletados os valores de *bit rate* e QPS recebidos pelo cliente via redes locais *Fast Ethernet* (FE) 100 Mbps e 802.11g (*Wi-Fi*). As médias e os desvios padrão (DP) correspondentes a esses valores são exibidos na Tabela 1. Além disso, o desempenho obtido nas transmissões via FE e *Wi-Fi* é comparado via teste estatístico de Mann-Whitney ($\alpha=0,05$).



I EAICTI

I Encontro Anual de Iniciação Científica, Tecnológica e Inovação

Tabela 1 – Média e DP (entre parênteses) para valores de taxa de transmissão e quadros por segundo obtidos na avaliação experimental

	Taxa de Transmissão em megabits	Quadros por Segundo
Wi-Fi	12,13 (2,74)	15,78 (9,24)
Fast Ethernet	12,08 (2,43)	23,58 (1,98)

Como esperado, FE atingiu uma quantidade de QPS significativamente melhor do que a obtida por *Wi-Fi*, aproximando o valor emitido pelo servidor (25 QPS). Por outro lado, não foi identificada diferença significativa no *bit rate*.

Conclusões

Através dos resultados obtidos neste trabalho, conclui-se que o protótipo é funcional e apresenta as regras de segurança e configuração para a transmissão segura de vídeos. Trabalhos futuros incluem a substituição do protocolo de transmissão de vídeo RTMP (*Real Time Messaging Protocol*) pelo RTMPS (*Real Time Messaging Protocol Secure*) ou outro protocolo que utilize criptografia para o *streaming* de vídeo. Adicionalmente, novos experimentos com mais usuários conectados em uma transmissão auxiliarão a verificar possíveis perdas na qualidade do vídeo recebido.

Agradecimentos

A UNIOESTE/CNPq pela concessão de bolsa de iniciação científica. Ao Weber S. R. Takaki pelo auxílio no desenvolvimento deste trabalho.

Referências

Machado, R.B.; Wu, F.C.; Lee, H.D.; Coy, C.S.R.; Fagundes, J.J.; Maciel, J.N.; Voltolini, R.F.; Maletzke, A.G.; Leal, R.F. & Ayrizomo, M.L.S. (2012). Método em Telemedicina para o Acompanhamento Remoto e em Tempo Real de Procedimentos Médicos. Brasil Patente (BR 10 2012 033125 0) INPI.

Shortliffe, E. H. & Cimino, J. J. Biomedical Informatics: Computer Applications in Health Care and Biomedicine. (2006). 3 ed. New York, USA: *Springer Science+Business Media*.

Urtiga, K.S.; Louzada, L.A. & Costa, C.L.B. (2004). Telemedicina: uma visão geral do estado da arte. *IX Congresso Brasileiro de Informática Médica*.

Wu, F.C.; Coy, C.S.R.; Lee, H.D.; Machado, R.B.; Fagundes, J.J.; Ayrizono, M.L.S.; Voltolini, R.F. & Spolaôr, N. (2014). S2TR. Patente: Programa de Computador. Número de registro: BR512014000324-8. INPI.