



UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

ELENILSON VIERA DA SILVA FILHO

**UMA ESTRATÉGIA DE REFLETORES MULTIMÍDIA
PARA CRIPTOGRAFIA E CODIFICAÇÃO EM TEMPO REAL**

João Pessoa - PB
2013

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

ELENILSON VIERA DA SILVA FILHO

UMA ESTRATÉGIA DE REFLETORES MULTIMÍDIA
PARA CRIPTOGRAFIA E CODIFICAÇÃO EM TEMPO REAL

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Informática do Centro de Informática da Universidade Federal da Paraíba, como parte dos requisitos para a obtenção do título de Mestre em Informática.

ORIENTADORES: Profa. Dra. Tatiana Aires Tavares e Prof. Dr. Gustavo Henrique Matos Bezerra Motta.

João Pessoa - PB

2013

*UMA ESTRATÉGIA DE REFLETORES MULTIMÍDIA
PARA CRIPTOGRAFIA E CODIFICAÇÃO EM TEMPO REAL*

S586u Silva Filho, Elenilson Vieira da.

Uma estratégia de refletores multimídia para criptografia e codificação em tempo real / Elenilson Vieira da Silva Filho.- João Pessoa, 2013.

116f. : il.

Orientadores: Tatiana Aires Tavares, Gustavo Henrique Matos Bezerra Motta

Dissertação (Mestrado) – UFPB/CI

1. Informática. 2. Fluxo de Mídia Multiple Unicast. 3. AES. 4. Criptografia. 5. Autenticação Federada. 6. Refletor multimídia.

UFPB/BC

CDU: 004(043)

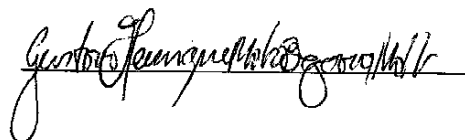
Ata da Sessão Pública de Defesa de Dissertação
de Mestrado de **ELENILSON VIEIRA DA
SILVA FILHO**, candidato ao Título de Mestre em
Informática na Área de Sistemas de Computação,
realizada em 22 de Março de 2013.

Ao vigésimo segundo dia do mês de março do ano dois mil e treze, às quinze horas, na Escola de Redes do Centro de Informática- da Universidade Federal da Paraíba, reuniram-se os membros da Banca Examinadora constituída para examinar o candidato ao grau de Mestre em Informática, na área de “*Sistemas de Computação*”, na linha de pesquisa “*Computação Distribuída*”, o Sr. **Elenilson Vieira da Silva Filho**. A comissão examinadora foi composta pelos professores doutores: GUSTAVO HENRIQUE MATOS BEZERRA MOTTA (PPGI-UFPB), Orientador e Presidente da Banca, TATIANA AIRES TAVARES (PPGI-UFPB), Orientadora, ALISSON VASCONCELOS DE BRITO (PPGI-UFPB), examinador interno e RODRIGO ELIA ASSAD (UFRPE) como examinador externo. Dando início aos trabalhos, o professor GUSTAVO HENRIQUE MATOS BEZERRA MOTTA cumprimentou os presentes, comunicou aos mesmos a finalidade da reunião e passou a palavra ao candidato para que o mesmo fizesse, oralmente, a exposição do trabalho de dissertação intitulado “*Uma Estratégia de Refletores Multimídia para Criptografia e Codificação em Tempo Real*”. Concluída a exposição, o candidato foi arguido pela Banca Examinadora que emitiu o seguinte parecer: “*Aprovado*”. Assim sendo, deve a Universidade Federal da Paraíba expedir o respectivo diploma de Mestre em Informática na forma da lei e, para constar, eu, Micherlon Xavier Bezerra, Assistente em Administração, servindo de secretário, lavrei a presente ata que vai assinada por mim mesmo e pelos membros da Banca Examinadora. João Pessoa, 22 de Março de 2013.

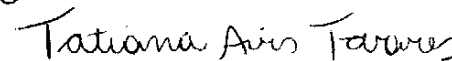


Micherlon Xavier Bezerra

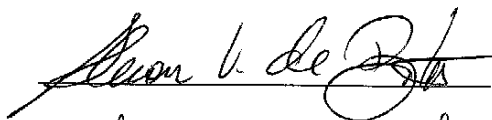
Prof. Dr. Gustavo Henrique Matos Bezerra
Motta
Orientador (PPGI-UFPB)



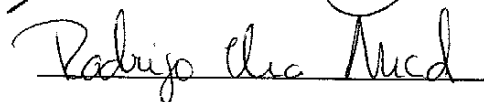
Profa. Dra. Tatiana Aires Tavares
Orientadora (PPGI-UFPB)



Prof. Dr. Alisson Vasconcelos de Brito
Examinador Interno (PPGI-UFPB)



Prof. Dr. Rodrigo Elia Assad
Examinador Externo (UFRPE)



ELENILSON VIERA DA SILVA FILHO

UMA ESTRATÉGIA DE REFLETORES MULTIMÍDIA
PARA CRIPTOGRAFIA E CODIFICAÇÃO EM TEMPO REAL

Dissertação de Mestrado apresentada ao
Programa de Pós-Graduação em
Informática do Centro de Informática da
Universidade Federal da Paraíba, como
parte dos requisitos para a obtenção do
título de Mestre em Informática.

Aprovado no dia 22 de março de 2013.

*UMA ESTRATÉGIA DE REFLETORES MULTIMÍDIA
PARA CRIPTOGRAFIA E CODIFICAÇÃO EM TEMPO REAL*

Dedico esse trabalho à minha querida avó que infelizmente não viveu tempo suficiente para acompanhar a minha longa caminhada e a minha mãe por ser A minha mãe.

UMA ESTRATÉGIA DE REFLETORES MULTIMÍDIA
PARA CRIPTOGRAFIA E CODIFICAÇÃO EM TEMPO REAL

AGRADECIMENTOS

A Deus, por eu estar vivo e com saúde.

Aos meus pais por me darem educação e as bases para que meus esforços fossem transformados em sucesso.

A minha tia Genilza por ser a minha segunda mãe durante todos esses anos de ajuda a mim e aos meus pais.

A professora Dra. Tatiana Aires Tavares e ao professor Dr. Gustavo Henrique Matos Bezerra Motta por terem aceitado orientar o meu trabalho e por toda a ajuda.

A Emanuella Soares de Moraes Freitas, Glauco de Souza e Silva e Yuri Gil Dantas por toda a contribuição na realização desse trabalho.

A equipe do Grupo de Trabalho Ambiente de Vídeo Colaboração em Saúde do LAViD/UFPB pela dedicação que fizeram o projeto e meu trabalho serem realizados.

Ao meu ex-tutor do PET Computação, o professor Dr. Leonardo Vidal Batista, por seus ensinamentos durante os três anos como petiano.

Ao PET.Com pelas oportunidades e conhecimentos adquiridos.

Aos meus amigos, por estarem sempre presentes nos momentos bons e ruins da minha vida.

A todos que um dia me apoiaram, eu não esqueci e um dia os recompensarei.

Graças a Deus a esse estado de fraqueza
Eu já tô imunizado, minha nação é nordestina
E traz no sangue o suor dessa caatinga
E tem no peito o alimento da fé
Embora a seca tenha secado o seu pranto
O mundo agora vai ter que ouvir meu canto
Sou renitente, continuo dizendo oxente.
(Geraldinho Lins)

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. Tais fatores propiciaram o surgimento de novas redes de transmissão para lidar com grandes volumes de dados e com grande poder de transmissão, o que leva o rápido desenvolvimento de várias tecnologias multimídia onde 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 integridade e confidencialidades desses dados. Assim, este trabalho apresenta uma estratégia de segurança com ênfase em confidencialidade, baseada na autenticação e verificação de autenticidade de usuários, além da distribuição de fluxos criptografados. Para atingir tais objetivos, foi dividido em duas partes: uma que descreve uma estratégia de refletores para transmissão de fluxos com criptografia AES e múltiplas codificações e outra que demonstra um servidor de segurança para fazer autenticação, criação de grupos e distribuição de chaves de grupos para usuários autenticados e com permissão para acessar tais informações, além da utilização de autenticação federada através da Comunidade Acadêmica Federada (CAFe). Um Mapeamento Sistemático foi feito o que permitiu a descoberta de diversas técnicas que puderam ser aplicadas ou comparadas tanto nos refletores quanto no servidor de segurança, além do destacamento de possíveis lacunas na literatura que permitem sua exploração. Como parte dos resultados, a estratégia foi aplicada à Arthron 3.0 e possibilitou realização de transmissões com diversos fluxos de vídeo em alta definição.

Palavras-chave: Segurança, Fluxo de Mídia Multiple Unicast, Criptografia, AES, Autenticação Federada, Servidor Central de Autenticação, Refletor Multimídia.

ABSTRACT

The Information and Communications Technology (ICT) field has changed due to both universalization of connectivity and popularization of devices. Such events have provided for the appearance of new networks which are able to send large amounts of data and also on a faster way. The broadband networks support the development of new technologies and then more data can be generated and sent by these networks. When these technologies are applied to medical or military domains, for example, one of the main issues is the integrity and confidentiality of the data being transmitted over the network. This work presents a privacy and security strategy based on authentication, verification of users authenticity and distribution of encrypted streams. This paper is divided into two parts: the first one describes a strategy for multimedia reflectors which send AES-encrypted streams and are able to perform many types of media encoding. The second part describes a security server which authenticates, creates user groups and distributes group keys only to authenticated and permitted users. It uses Federated Authentications provided by the Federated Academic Community (CAFe). For the matter of comparison of the present strategy with previous studies, a systematic mapping was done to discuss the techniques for authentication and media transmission. In order to validate the work, the whole strategy was integrated to the Arthron - a tool for multimedia transmissions. The testing scheme used the 2^k factorial designs and it analyzed the influence of the processing, encrypting and coding in the time transmission.

Key-words: Security, Multiple Unicast Media Flow, Cryptography, AES, Federated Authentication, Authentication Central Server, Multimedia Reflector.

SUMÁRIO

CAPÍTULO 1: INTRODUÇÃO	19
1.1 Trabalhos Correlatos na Instituição	20
1.2 Identificação do Problema	22
1.3 Objetivos	24
1.4 Contribuição do Trabalho	25
1.5 Estrutura da Dissertação	25
CAPÍTULO 2: TRANSMISSÃO MULTIMÍDIA SEGURA	26
2.1 Fluxo Multimídia e Codificações	27
2.2 Transmissão <i>Multiple Unicast, Broadcast e Multicast</i>	29
2.3 Refletor Multimídia para Transmissão UDP	32
2.4 Criptografia de Chave Simétrica e Assimétrica	33
2.5 AES como Cifra de Fluxo no Modo Contador	35
2.6 Funções de HASH e o Algoritmo SHA	36
2.7 Autenticação Federada e a CAFé	37
CAPÍTULO 3: ARTHRON 3.0	40
3.1 Arthron 1.0 e 2.0	40
3.2 Arquitetura	42
3.3 Componentes	43
3.3.1 ArthronServer	43
3.3.2 <i>SenderComponent</i>	45
3.3.3 <i>ReceiverComponent</i>	46
3.3.4 VideoServer	47
3.3.5 Reflector	47
3.3.6 Recorder	48
3.3.7 VSecurityServer	49
CAPÍTULO 4: AUTENTICAÇÃO DE SUJEITOS E CRIPTOGRAFIA MULTIMÍDIA	
50	
4.1 Mapeamento Sistemático	50
4.1.1 Planejamento – Definição do Protocolo	50
4.1.2 Apresentação, Análise e Discussão dos Resultados	55
4.2 Trabalhos Relacionados	60

4.2.1 A Novel Scheme for HD Video Stream Encryption (FAN, 2011)	60
4.2.2 Secure Decentralized Group Key Management through Progressive Approach (SANDOSH, 2010)	62
4.2.3 A Secure Media Streaming Mechanism Combining Encryption, Authentication and Transcoding (MOU, 2009)	63
4.2.4 H2A: Hybrid Hash-chaining scheme for Adaptive multicast source authentication of media-streaming (CHALLAL, 2005)	65
4.2.5 Differentially secure multicasting and its implementation methods (HOLEMAN, 2002)	66
4.2.6 Efficient security mechanisms for overlay multicast based content delivery (ZHU, 2007)	66
4.2.7 Quasi-commutative watermarking and encryption for secure media content distribution (LIAN, 2009)	67
4.2.8 A Secure Scheme for Video Streaming Using SRTP AES and DH (ASGHAR, 2010)	69
4.2.9 Secure Advanced Video Coding Based on Selective Encryption Algorithms (LIAN, 2006)	69
4.3 Análise Comparativa	71
CAPÍTULO 5: REFLETORES PARA CRIPTOGRAFIA MULTIMÍDIA E SERVIDOR VSECURITYSERVER	74
5.1 Refletores para Codificação e Criptografia em Tempo Real	74
5.1.1 Modelo Conceitual	74
5.1.2 Modelo Arquitetural e Tecnológico	76
5.2 VSecurityServer	83
5.2.1 Modelo Conceitual	84
5.2.2 Modelo Arquitetural e Tecnológico	86
CAPÍTULO 6: VERIFICAÇÃO	93
6.1 Materiais	93
6.2 Refletores para Codificação e Criptografia em Tempo Real	93
6.3 VSecurityServer	99
CAPÍTULO 7: RESULTADOS E DISCUSSÃO	102
7.1 Análise Comparativa	102
7.2 Resultados Práticos	103

7.3	Publicações.....	106
7.4	Licenciamento	108
CAPÍTULO 8: CONSIDERAÇÕES FINAIS		109
8.1	Trabalhos Futuros	110

ÍNDICE DE FIGURAS

Figura 1. Componentes da Arthron em seus respectivos locais em um ambiente cirúrgico.....	23
Figura 2. Esquema geral de uma transmissão multimídia.....	29
Figura 3. Transmissão Multiple Unicast	30
Figura 4. Esquema de Transmissão Broadcast.....	31
Figura 5. Esquema de Transmissão Multicast.....	31
Figura 6. Esquema de um Refletor Multimídia para Transmissão UDP.	32
Figura 7. Refletores geograficamente distribuídos otimizando uma distribuição <i>multiple unicast</i> de forma similar à <i>multicast</i>	33
Figura 8. Esquema do Modelo de Cifra Simétrica	34
Figura 9. Esquema do Modelo de Cifra Assimétrica	34
Figura 10. Esquema de encriptação do AES no Modo Contador (VIEIRA, 2011)	36
Figura 11. Funcionamento da CAFé (CAFé, 2012).....	38
Figura 12. Evento transmitido utilizando a Arthron (MELO, 2010a)	40
Figura 13. Arquitetura da Arthron 1.0. Adaptada de Melo (2010a).....	41
Figura 14. Arquitetura da Arthron 2.0 (VIEIRA, 2012)	42
Figura 15. Arquitetura da Arthron 3.0	43
Figura 16. Gerenciamento de Sessões no ArthronServer	44
Figura 17. Gerenciamento de Fluxos de uma Sessão no ArthronServer	44
Figura 18. Interface Gráfica do Encoder	45
Figura 19. Interface Gráfica do VideoRoom	46
Figura 20. Interface Gráfica do Decoder	47
Figura 21. Interface Gráfica do VideoServer	47
Figura 22. Interface Gráfica do Reflector	48
Figura 23. Recuperação da Experiência no Decoder	49
Figura 24. Recuperação da Experiência no ArthronServer	49
Figura 25. Contribuição de Publicações dos Engenheiros de Busca.	53
Figura 26. Distribuição anual das publicações do mapeamento sistemático	55
Figura 27. Tipos de criptografia utilizados pelos estudos do mapeamento	56
Figura 28. Gráfico de bolhas do mapeamento sistemático	58
Figura 29. Estratégias de distribuição de chave utilizadas pelos trabalhos do mapeamento	58
Figura 30. Algoritmos de criptografia utilizados pelos estudos do mapeamento sistemático	59
Figura 31. Sequência do algoritmo de encriptação do fluxo. Adaptado de Fan (2011)	61
Figura 32. Resultado da estratégia de Fan (2011). Adaptado de Fan (2011)	62
Figura 33. Processo de verificação de membros autorizados de Sandosh (2010)....	63
Figura 34. Estrutura dos pacotes RTP modificados. Adaptado de Mou (2009).....	64
Figura 35. Esquema geral do Modelo descrito por Mou (2009).....	64

Figura 36. Esquema do envio de pacotes e QoRs. Adaptado de Challal (2005).....	65
Figura 37. Interação de Usuários e Servidores. Adaptado de Zhu (2007)	67
Figura 38. Criptografia e assinatura de vídeos utilizando método tradicional. Adaptado de Lian (2009).....	68
Figura 39. Criptografia e assinatura de vídeos utilizando método proposto por Lian (2009). Adaptado de Lian (2009).....	68
Figura 40. Esquema de segurança de transmissão segura de conteúdo multimídia. Adaptado de Asghar (2010)	69
Figura 41. Resultados. (LIAN, 2006)	70
Figura 42. Framework geral para transmissão segura de fluxo (VIEIRA, 2011).....	75
Figura 43. Visão Geral do Refletor Híbrido de Criptografia e Codificação. A largura da seta indica a qualidade da definição do fluxo	75
Figura 44. Sequência de passos necessária para a múltipla codificação e criptografia	76
Figura 45. Esquema do ReflectorJ	77
Figura 46. Esquema de Criptografia do AESReflectorC.....	78
Figura 47. Esquema de decriptografia do AESReflectorC	78
Figura 48. AESReflectorJ recebendo fluxo não criptografado e criptografando-o.....	79
Figura 49. AESReflectorJ recebendo fluxo criptografado e decriptografando-o.....	79
Figura 50. Esquema do AESHybridReflectorJ recebendo fluxo não criptografado ...	80
Figura 51. Esquema do AESHybridReflectorJ recebendo fluxo criptografado	81
Figura 52. Esquema modular do FullAESHybridReflectorJ	82
Figura 53. Cenário ideal para transmissão de múltiplos fluxos criptografados.....	84
Figura 54. Cenário de criptografia de múltiplos fluxos utilizando Sessão.....	85
Figura 55. Autenticação, criação de Sessão e distribuição de chave em um Servidor Central.....	86
Figura 56. Criação do Token de uma autenticação de um sujeito no VSecurityServer	88
Figura 57. Requisição de IdPs de um sujeito ao VSecurityServer	89
Figura 58. Autenticação de um sujeito na CAFé utilizando VSecurityServer como intermediador	89
Figura 59. Processo de iniciação de comunicação segura entre dois sujeitos utilizando o VSecurityServer	91
Figura 60. Tentativa de um sujeito se passar por outro em uma comunicação	92
Figura 61. Esquema de realização dos testes.....	94
Figura 62. Cadastro de usuário no ArthronServer	99
Figura 63. Tela de agendamento de Sessão no ArthronServer	100
Figura 64. Tela de autenticação no ArthronServer.....	100
Figura 65. Tela de autenticação do Encoder.....	101
Figura 66. Escolha de Sessão no Encoder	101
Figura 67. Lista de Sessões de um usuário no ArthronServer	101
Figura 68. Demonstração 1 no WRNP 2012	104
Figura 69. Demonstração 2 no WRNP 2012	104

Figura 70. Demonstração 3 no WRNP 2012	105
Figura 71. Video Wall do GT Cinema exibindo fluxos do GTAVCS no WRNP 2012	106
Figura 72. Bibliotecas e licenças utilizadas pela Estratégia	108

ÍNDICE DE TABELAS

Tabela 1: Comparação dos Parâmetros do SHA. Adaptado de STALLINGS (2008)	37
Tabela 2. Critérios de Inclusão de estudos no Mapeamento Sistemático.	54
Tabela 3. Critérios de Exclusão de estudos no Mapeamento Sistemático.	54
Tabela 4. Comparação dos trabalhos do mapeamento sistemático.....	71
Tabela 5. Notação utilizada pelo trabalho. Adaptado de Stallings (2008)	83
Tabela 6. Descrição dos dados da Sessão Colaborativa armazenados no Servidor	87
Tabela 7. Descrição dos dados do usuário armazenados no Servidor	87
Tabela 8. Descrição dos computadores utilizados para desenvolvimento e testes...93	
Tabela 9. Fatores e seus níveis aplicados no modelo 2^k	94
Tabela 10. Informações sobre os vídeos de teste.....	95
Tabela 11. Codificação de áudio e vídeo dos fluxos transmitidos pelo Refletor.....	95
Tabela 12. Tabela do Modelo 2^k , com $k = 4$	96
Tabela 13. Soma, q e SST de cada fator	97
Tabela 15. Comparação dos trabalhos correlatos	102

ÍNDICE DE ABREVIações

ACK	Acknowledgement
AES	Advanced Encryption Standard
AVC	Advanced Video Coding
CAFe	Comunidade Acadêmica Federada
CRBR	Certificate Revocation Based Group Rekeying Scheme
CRL	Certificate Revocation List
DEK	Data Encryption Key
DES	Data Encrytion Standard
GK	Group Key
GS	Group Server
GT	Grupo de Trabalho
GTAVCS	Grupo de Trabalho Ambiente de Vídeo Colaboração em Saúde
GTMDA	Grupo de Trabalho de Mídias Digitais e Artes
HTTP	Hypertext Tranfer Protocol
HULW	Hospital Universitário Lauro Wanderley
IDE	Ambiente de Desenvolvimento Integrado
IdP	Identity Provider
IHC	Interação Humano Computador
J2EE	Java Enterprise Edition
JVM	Máquina Virtual Java
KEK	Key Encryption Key
LARQSS	Laboratório de Arquitetura e Sistemas de Software
LASID	Laboratório de Sistemas Digitais
LAViD	Laboratório de Aplicações de Vídeo Digital
MAC	Message Authentication Code
MARS	Multimedia Application Routing Server
MCU	Multipoint Control Unit
MD5	Message-Digest Algorithm 5
NASA	National Aeronautics and Space Administration
POP	Ponto de Presença
RNP	Rede Nacional de Ensino e Pesquisa

RSA	Rivest, Shamir e Adleman
RTP	Real Time Protocol
RTSP	Real Time Streaming Protocol
RUTE	Rede Universitária de Telemedicina
SAML	Security Assertion Markup Language
SBRC	Simpósio Brasileiro de Redes de Computadores
SC	Sessão Colaborativa
SHA	Secure Hash Algorithm
SP	Service Provider
STCFED	Transposição de Credenciais de Autenticação Federadas
TIC	Tecnologia da Informação e Comunicação
TS	Transport Stream
UDP	User Datagram Protocol
UFPB	Universidade Federal da Paraíba
VLC	VideoLAN Client
VSS	VSecurityServer
WSDL	Web Service Definition Language

CAPÍTULO 1: INTRODUÇÃO

As transformações da área de Tecnologia da Informação e Comunicação (TIC) tem agregado universalização e popularização das formas de conectividade e isso contribuiu para o surgimento de novas redes de comunicação com a finalidade e capacidade de transmitir dados em larga escala (MELO, 2009). A Internet2 (INTERNET2, 2012) é um exemplo dessas redes e é uma iniciativa norte-americana voltada a comunidades acadêmicas para desenvolvimento de tecnologias e aplicações avançadas de redes *Internet* para as comunidades acadêmicas e de pesquisa. Essa iniciativa visa o desenvolvimento de novas aplicações que usem o grande poder de transmissão que a Internet2 propicia e que não são viáveis com a tecnologia das redes comuns. No Brasil a principal representante de rede com alto poder de transmissão é a Rede Ipê da Rede Nacional de Ensino e Pesquisa (RNP), que foi a primeira rede óptica nacional e acadêmica da América Latina. A rede foi projetada para garantir largura de banda para o uso de serviços e aplicações avançadas e a experimentação, englobando mais de 27 Pontos de Presença (PoPs) e várias ramificações visando atender mais de 500 instituições de ensino e pesquisa em todo o país (IPÊ, 2012).

Diante de uma rede que propicia transmissões em grande quantidade de dados em alta velocidade e voltada para a comunidade acadêmica, é natural o surgimento de pesquisas relacionadas. Um contexto que pode usufruir da Rede Ipê é a transmissão de fluxos multimídia em alta definição e um exemplo de aplicação é o de Cinema Digital, em que um filme pode ser distribuído e reproduzido em cinemas em tempo real, fator importante visto que menos de 90% das cidades brasileiras tem cinema (CULTURAL, 2012) e isso pode ser uma alternativa para exibição de filmes nesses municípios. Outra aplicação muito semelhante é a de teatros conectados, em que um espetáculo teatral pode ser reproduzido ao vivo e simultaneamente em diversos locais diferentes de onde está acontecendo e os telespectadores remotos poderiam visualizar, muitas vezes, melhor do que um expectador local.

No contexto da Rede Ipê surgiu a Arthron (MELO, 2010a), uma solução que, inicialmente, permitia a interação distribuída e em tempo real em espaços midiáticos compartilhados, através de redes de altíssima velocidade e com grande volume de informação. Com essa ferramenta é possível, por exemplo, efetuar a captura de

fluxos de vídeo de diversas câmeras situadas em locais distintos e fazer sua exibição em locais também distintos, fazendo o controle (captura, exibição, trocas, codificação) de maneira remota. A Arthron fornece um conjunto de componentes para o gerenciamento de transmissão simples e intuitiva de fluxos midiáticos (MELO, 2010a) e foi perceptível que a ferramenta poderia ter outras aplicações, como na telemedicina (LIMA, 2011). Porém o sistema não possuía mecanismos de segurança que, nesse novo contexto, são fundamentais. Imagens médicas passaram a ser transmitidas por redes inseguras, sendo necessária uma preocupação com o sigilo e a integridade dessas informações.

Para prover os recursos de segurança necessários à Arthron para o domínio de telemedicina, foi criado o Grupo de Trabalho Ambiente de Vídeo Colaboração em Saúde (GTAVCS), programa de grupos de trabalho da RNP em uma parceria do Laboratório de Aplicações de Vídeo Digital (LAVID) com o objetivo de adaptar a Arthron para suprir as necessidades exigidas pelo contexto de telemedicina e aplicar uma estratégia que utiliza métodos de criptografia para garantir a confidencialidade e integridade dos dados. Essas modificações levaram ao desenvolvimento de uma nova versão da Arthron, a Arthron 2.0 (VIEIRA, 2012) e, posterior, Arthron 3.0.

Esta dissertação foi desenvolvida com base no projeto do GTAVCS (GTAVCS, 2012) com o objetivo de criar uma estratégia de segurança que possa ser aplicada a Arthron, onde foi possível analisar e aplicar técnicas de autenticação, criptografia e codificação de fluxos de mídia. O restante desse capítulo descreve os trabalhos correlatos na instituição, como o problema foi identificado, os objetivos, as contribuições do trabalho e, por fim, como a dissertação está estruturada.

1.1 Trabalhos Correlatos na Instituição

O Grupo de Trabalho de Mídias Digitais e Artes (GTMDA, 2012) fase 1 e 2 foi executado em uma parceria do LAViD e da RNP e teve como foco oferecer formas mais avançadas para Interação Humano Computador (IHC), as quais permitam a interação de agentes humanos e sintéticos em espaços midiáticos compartilhados, distribuídos e em tempo real, através de redes de computadores de alta velocidade fazendo uso da transmissão de grande volume de informação. Essa convergência de Arte e Tecnologia é uma área que emerge da união entre a arte e as novas mídias digitais, investigando como acontece essa nova forma de pensar e fazer Arte

com tal suporte tecnológico (MELO, 2010a). A ideia central foi a construção de uma ferramenta de gerenciamento que concentre ao máximo o controle de todos os dispositivos de hardware e software envolvidos para execução de evento artístico-tecnológico.

A evolução do GTMDA tem como principal resultado a Arthron e, a partir de sua evolução, criou-se o GTAVCS que é uma iniciativa conjunta dos laboratórios LAVID, LASID (Laboratório de Sistemas Digitais) e LARQSS (Laboratório de Arquitetura e Sistemas de Software) da Universidade Federal da Paraíba (UFPB). Este grupo de trabalho foi aprovado no Edital de Grupos de Trabalho 2011-2012 da RNP e, durante sua primeira fase, foi proposta uma infraestrutura de hardware e software com gerência remota para captura e distribuição segura de múltiplos fluxos simultâneos a fim de prover suporte a diversos cenários de vídeo colaboração em saúde. Através de experimentos realizados dentro do HULW/UFPB em conjunto com outras universidades, tais como: Universidade Federal do Tocantins (UFT), demonstrou-se o potencial agregador do protótipo desenvolvido na primeira fase do GTAVCS. O serviço proposto à RNP através do projeto GTAVCS – Fase II teve como foco aprimorar e melhorar o atual o serviço de transmissão de cirurgias ao vivo (desenvolvido na Fase I) e, sobretudo, desenvolver serviços adicionais para o apoio à atividade de ensino e aprendizagem baseadas em colaboração e recuperação de informações. O público alvo deste GT é composto por acadêmicos, professores e profissionais da área de cirurgia dos hospitais escola, em particular, os ligados a Rede Universitária de Telemedicina (RUTE). Para Fase II deste GT, como parte do processo de avaliação dos resultados, o GT contou com o apoio dos integrantes de um SIG (Grupo de Interesse Especial da RUTE) que envolve o Hospital Universitário Lauro Wanderley (HULW) da UFPB, o Hospital Universitário da Universidade Federal do Maranhão (HUUFMA) e o núcleo RUTE da Universidade Federal de Tocantins (UFT), além de parceiros internacionais com a finalidade de avaliação do ambiente. Um marco de destaque foi a participação do GTAVCS na inauguração da nova capacidade da rede acadêmica brasileira no dia 13/07/2011 em Brasília, onde os presentes assistiram à transmissão, em tempo real, de uma cirurgia realizada no HULW, acompanhada por estudantes e profissionais de Medicina da Universidade Federal de São Paulo (UNIFESP) e da UFT. Para realizar tal experimento foi

utilizada a ferramenta Arthron adaptada para Telemedicina de forma integrada ao equipamento de videoconferência Tandberg para transmissão aos demais pontos via Unidade de Controle Multiponto (*Multipoint Control Unit* – MCU - que tem a finalidade de unir os fluxos em um único e distribuir aos destinos para prover transmissões com múltiplos pontos). Geralmente esse conjunto de equipamentos necessários tem valor expressivo, se comparado a computadores pessoais, infraestrutura utilizada pela RUTE.

1.2 Identificação do Problema

Dentre os cenários em que a transmissão de fluxos de mídia se aplica, para determinados contextos é necessário garantir a segurança na transmissão dos fluxos pela rede, tendo como exemplo de contexto a telemedicina. De acordo com Lima et al. (2011), entre as diversas modalidades da telemedicina, incluem-se as videoconferências, que permitem a integração, em tempo real, recebendo e enviando áudio e vídeo de alta qualidade entre pontos geograficamente distribuídos. Para tanto, é necessário utilizar mecanismos de segurança que garantam a transmissão segura desses dados.

Na Arthron uma transmissão envolve a captura e a distribuição de diferentes fluxos caracterizada 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 em um ambiente de telemedicina, a fonte pode ser uma câmera (webcam ou câmera convencional ligada a uma placa de captura), a saída de dispositivos de ultra-som ou raios X ou, ainda, 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. Um exemplo de cenário pode ser visualizado na Figura 1, onde é possível observar uma sala de cirurgia com:

- 1) Câmeras para captura de vídeos
- 2) Microfone para captura de áudio
- 3) Sensores para captura de dados
- 4) Computador com módulo de captura e transmissão
- 5) Articulador (módulo da Arthron) para o gerenciamento dos fluxos de mídia

- 6) Sala de telemedicina, possível local para acompanhamento de todos os fluxos
- 7) Outro possível local para acompanhamento dos fluxos
- 8) Tela que exibe outro profissional de medicina interagindo com o cirurgião

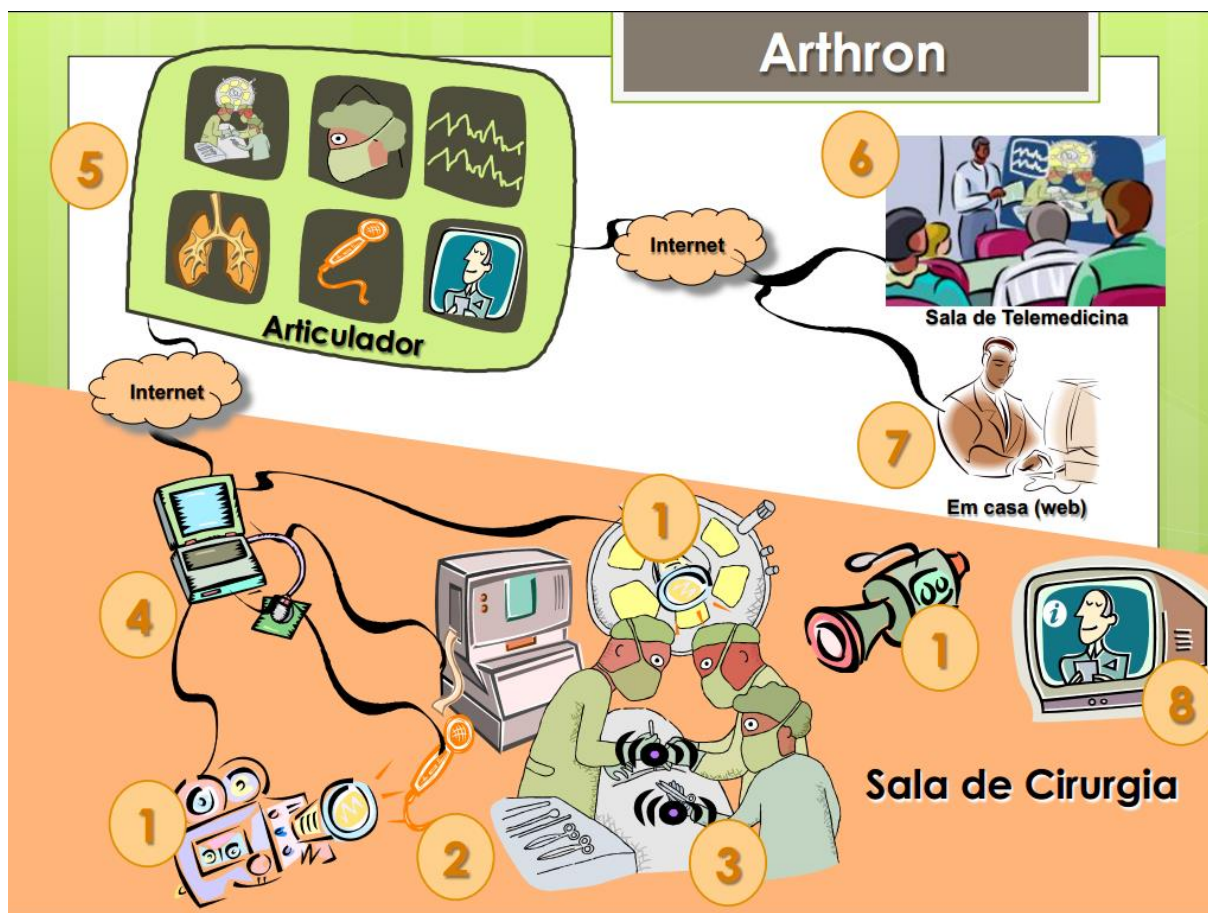


Figura 1. Componentes da Arthron em seus respectivos locais em um ambiente cirúrgico.

É perceptível que a Arthron se aplica para gerenciamento e controle distribuído desses fluxos como uma solução de que atende às necessidades de transmissão de fluxos que a telemedicina impõe, visto que permite a captura de diversos dispositivos, como os apresentados, e a transmissão multiponto desses dados. Porém, imagens e dados clínicos de pacientes são transmitidos nesses fluxos e uma preocupação surge: a segurança, requisito que não foi imposto pelos cenários em que a Arthron foi aplicada nas suas primeiras versões e que se torna um fator crucial nesse novo contexto. Conforme a resolução nº 1.643/2002¹ do Conselho Federal de Medicina (CFM), é determinado, com força de lei, a adoção de medidas de segurança na telemedicina. Faz-se necessária a inserção de medidas

¹ Disponível em: http://www.portalmédico.org.br/resolucoes/CFM/2002/1643_2002.pdf

para prover a integridade e confidencialidade dos dados, da origem e do destino, reforçada pela resolução de nº 1.718/2004² do CFM que veda ao médico, sob qualquer forma de transmissão de conhecimento, ensinar procedimentos privativos de médico a profissionais não médicos. A autenticação, portanto, ajuda neste sentido e uma forma de prover isso é a utilização da autenticação federada, uma maneira de disponibilização e compartilhamento de serviços entre parceiros, mutuamente confiáveis, que exigem apenas uma autenticação de um sujeito na federação de origem e o acesso é dado a os serviços de todas as federações, garantida pela relação de confiança entre as federações. Uma representante desse tipo de autenticação é a Comunidade Acadêmica Federada (CAFe) (CAFE, 2012) da RNP, que interliga redes de instituições de ensino brasileiras.

Para a utilização no contexto de telemedicina, a Arthron deve atender a tais requisitos de segurança, garantindo a confidencialidade e integridade dos dados transmitidos de pacientes, médicos e das práticas profissionais envolvidas. Esse é o problema tratado por essa dissertação.

Diante desse escopo, algumas decisões tomadas são norteadas de modo a se encaixarem no contexto e atenderem aos requisitos impostos pela Arthron, como, por exemplo, a utilização de Java, a fim de poder se integrada ou essa ferramenta e a utilização da CAFe, mantida pelo mesmo financiador da Arthron. Por esse motivo alguns pontos desse trabalho acabaram se tornando análise, definição e implementação de requisitos do projeto que desenvolveu a ferramenta.

1.3 Objetivos

O objetivo geral dessa dissertação é uma estratégia de segurança para criptografia de conteúdo multimídia em alta definição baseada na autenticação de sujeitos, na transmissão de fluxos multimídia criptografados, integrada a CAFe e que possa ser utilizada pela Arthron.

Os objetivos específicos são:

- Um modelo de segurança para a autenticação e distribuição de chaves de criptografia para sujeitos devidamente autenticados;
- Um serviço baseado no modelo;

² Disponível em: http://www.portalmedico.org.br/resolucoes/cfm/2004/1718_2004.htm

- Criptografia e transmissão de fluxos multimídia entre sujeitos autenticados;
- Adaptação da Arthron para utilização do serviço;
- Verificação do serviço implementado.

1.4 Contribuição do Trabalho

O levantamento dos trabalhos correlatos levou ao desenvolvimento de uma estratégia de segurança compreendida em duas partes: um servidor de autenticação e gerenciamento de usuários e grupos que foi integrado à Arthron, possibilitando a utilização dessa solução por apenas sujeitos autorizados e, por ter sido projetado como um serviço, pode ser utilizado como fonte de segurança para outros fins; a segunda parte consiste de um conjunto de refletores (ANDREEV, 2003) multimídia para a transmissão em tempo real de mídias criptografadas que também foi integrado a Arthron e isso possibilitou a realização de transmissão de fluxos de mídia em alta definição com criptografia e múltiplas codificações. Seus resultados, expressos na seção 6.2, indicam que esses refletores podem ser aplicados, tanto ao contexto proposto, quanto em outros contextos. A definição de refletores pode ser encontrada na seção 2.3 e a descrição de sua utilização pode ser encontrada na seção 5.1.

Também se pode destacar a potencial contribuição em futuros trabalhos que venham a utilizar os resultados dessa dissertação, uma vez que foi feita uma revisão de alguns serviços e aspectos operacionais particulares e que podem ser aplicadas em outros contextos, como pode ser observado no CAPÍTULO 2:.

1.5 Estrutura da Dissertação

No CAPÍTULO 2: é exposta uma fundamentação teórica em que são mostrados conceitos relacionados com a transmissão segura de fluxos de mídia. No CAPÍTULO 3: é exposta a Arthron, solução em que fez uso da estratégia. O CAPÍTULO 4: consiste da análise de técnicas de segurança feita em duas partes: um mapeamento sistemático dos trabalhos relacionados para dar suporte à fundamentação teórica e para encontrar lacunas que puderam ser exploradas na dissertação ou em trabalhos futuros. O CAPÍTULO 5: descreve os detalhes da estratégia. No CAPÍTULO 6: é exibido como foi feita a verificação, no CAPÍTULO 7: há resultados e discussão e, no CAPÍTULO 8:, são discutidas as conclusões e considerações finais.

CAPÍTULO 2: TRANSMISSÃO MULTIMÍDIA SEGURA

Este capítulo apresenta os conceitos teóricos que deram suporte ao entendimento e desenvolvimento do trabalho. Primeiro são definidos o que é um fluxo multimídia e alguns padrões de compressão/codificação de transmissão mais importantes e que serão utilizados mais adiante. É importante seu entendimento para compreender melhor os resultados expostos na seção 6.2.

Também são definidos os modelos de transmissão de dados *multiple unicast*, *broadcast* e *multicast* (HOLEMAN, 2002), visto que o *multiple unicast* é adotado em uma parte do trabalho.

Há uma explicação sobre refletores (ANDREEV, 2003) de um modo geral e é ilustrado o que é um refletor multimídia que utiliza o protocolo *User Datagram Protocol* (UDP) (UDP, 2012) e exemplos de aplicações, pois esses foram adotados como responsáveis por distribuir o conteúdo multimídia de forma segura e há a definição de um esquema de refletores seguros na seção 5.1.

Para a transmissão multimídia segura foi utilizada a criptografia simétrica (STALLINGS, 2008), e é feita uma explanação e comparação com a criptografia assimétrica (STALLINGS, 2008) e a assimilação desses conceitos e suas diferenças é um ponto chave para a análise do mapeamento sistemático e dos trabalhos correlatos descritos nas seções 4.1 e 4.2, respectivamente. Como representante da cifra simétrica o *Advanced Encryption Standard* (AES) (STALLINGS, 2008) é descrito e tem sua ampla utilização tanto nos trabalhos correlatos quanto na definição da estratégia.

Outro ponto de destaque são as funções de *hash* que são importantes tanto em assinaturas quanto em estratégias de autenticação e essas tem suas características definidas nesse capítulo, além de um algoritmo representante, o *Secure Hash Algorithm* (SHA) (STALLINGS, 2008). Essas funções tem utilização pelo trabalho de Sandosh (2010), que faz uso para autenticação periódica e pela estratégia descrita nesse trabalho.

Por fim é descrita a importância de federações e autenticações federadas, em que é citada a CAFé, uma federação de instituições de ensino brasileiras.

2.1 Fluxo Multimídia e Codificações

O termo multimídia designa a combinação de texto, gráficos, imagens, vídeo, áudio e qualquer outro meio pelo qual a informação possa ser representada, armazenada, transmitida e processada digitalmente, onde há ao menos uma mídia estática (texto, gráficos, ou imagens) e uma mídia dinâmica (vídeo, áudio) (CHAPMAN, 2000). Para a transmissão ou armazenamento multimídia, é necessária uma compressão dos dados e é nisso que as técnicas de compressão entram como um ponto chave, pois é o seu poder de compressão que irá otimizar o uso dos recursos, seja de rede ou seja de espaço em disco. Os modelos de compressão multimídia são chamados de codificações e há vários padrões diferentes, cada um com suas vantagens e desvantagens. Um bom modelo de compressão multimídia consegue comprimir minimizando as perdas e provendo uma recuperação similar ao arquivo original e podem ser classificadas em duas categorias: armazenamento e transmissão.

Alguns padrões de compressão/codificação de vídeo importantes são descritos abaixo (MELO, 2010b):

- MPEG-2 – utilizada nos DVDs (*Digital Vídeo Disc*) além de na maioria das transmissões de TV digital disponíveis;
- MPEG-4 (Parte 2) – permite o uso de diferentes *profiles*, estabelecendo valores diversos de taxas de compressão. É muito utilizado em transmissões na Internet, por possuir uma ótima qualidade mesmo a baixas taxas de transmissão, permitindo a visualização das imagens do vídeo não importando a capacidade do meio de transmissão (Internet de banda larga ou linha discada, por exemplo);
- MPEG-4 (Parte 10) – (*Advanced Video Coding* ou H.264 ou MPEG-4 Part-10) Padrão de codificação de vídeo desenvolvido inicialmente pelo VCEG (sob a sigla H.26L) e, posteriormente, pelo JVT, sendo também conhecido como AVC ou MPEG-4, Parte 10.

Alguns padrões de compressão de áudio são descritos abaixo (MELO, 2010b):

- AAC: *Advanced Audio Coding* (Codificação Avançada de Áudio) – Um dos formatos de compressão de áudio usados nos padrões MPEG-2 e MPEG-4;

- MP3: MPEG-1, Layer3 (MPEG-1, Camada 3) – Um dos formatos de compressão de áudio com perdas usado no padrão MPEG-1. Alcançou grande popularidade na codificação de música para distribuição pela Internet e para armazenamento em computadores e dispositivos pessoais de áudio.

Para a transmissão multimídia, formatos utilizados geralmente são desenvolvidos com base em alguns aspectos inerentes às transmissões. O fato de que um cliente poder acessar uma transmissão em qualquer parte da fonte transmitida (ao contrário de um arquivo, onde o acesso é geralmente feito no início) cria a necessidade de uma estratégia capaz de decodificar a informação iniciando, também, em qualquer parte da fonte, que é denominada decodificação de segmentos. Para viabilizar a sincronização do fluxo faz-se necessária a utilização de mecanismos de transporte sinalizadores. Um dos objetivos é minimizar a utilização dos recursos, tais como: rede, processamento e memória (MELO, 2010b).

Alguns protocolos de transmissão podem ser utilizados combinados com o padrão de compressão, onde cada combinação se adequa melhor para cada contexto. A seguir alguns padrões de transmissão:

- RTSP (Real Time Streaming Protocol) - é um protocolo que permite a interação cliente-servidor entre a fonte do fluxo de mídia e o usuário com uma taxa constante (RTSP, 2012);
- RTP (*Real Time Protocol*) - é um protocolo de comunicação ponto a ponto ou na faixa reservada para endereços *multicast* utilizado para o transporte de mídias contínuas de tempo real (RTP, 2012);
- HTTP (*Hypertext Transfer Protocol*) – é um protocolo que surgiu com o intuito de facilitar a distribuição de conteúdo entre clientes e servidores da Web. Para isso foi necessário uma padronização para prover essa comunicação e é responsável pelo tratamento de pedidos e respostas entre esses lados. (HTTP, 2012).
- UDP (*User Datagram Protocol*) – é um protocolo que permite que uma aplicação escreva um datagrama encapsulado em um pacote IPv4 ou IPv6 e enviar ao destino, mas sem as confirmações existentes em protocolos TCP, por isso ele é mais rápido e se adequa a transmissões de fluxos de vídeo ao vivo, porém não há garantias que o pacote chegue ao destino final (UDP, 2012).

O esquema geral de uma transmissão multimídia pode ser visualizado na Figura 2, onde é apresentado o codificador e seus elementos: a captura, a codificação, a bufferização e o envio, por parte do remetente. No decodificador o processo ocorre com o recebimento dos pacotes, a bufferização, a decodificação e, por fim a exibição.

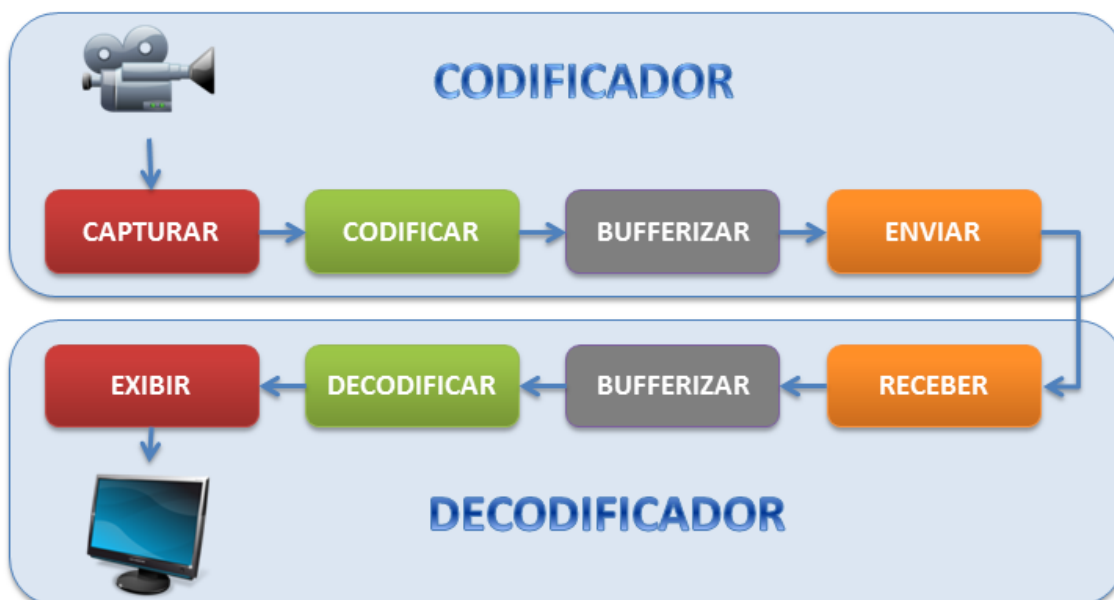


Figura 2. Esquema geral de uma transmissão multimídia

A estratégia apresentada nesse trabalho faz uso de diferentes codificações de áudio e vídeo par fluxos multimídia e utiliza o protocolo UDP para as transmissões.

2.2 Transmissão *Multiple Unicast*, *Broadcast* e *Multicast*

Uma transmissão caracteriza-se por, ao menos, dois pontos: um que envia e outro que recebe. Porém a transmissão pode ser compreendida por vários pontos, o que se caracteriza um grupo. Segundo Holeman (2002), as transmissões em grupos podem ser classificadas em três categorias: *multiple unicast*, *broadcast*, *multicast*.

Multiple unicast caracteriza-se por um grupo de sujeitos que faz transmissões entre si, onde o envio é feito ponto-a-ponto (*unicast*) de mensagem para cada membro do grupo. Para n remetentes e r receptores, o número de mensagens enviadas é $n * r$ (HOLEMAN, 2002), como é ilustrado na Figura 3.



Figura 3. Transmissão Multiple Unicast

Embora este assegure que cada membro do grupo receba a mensagem, a desvantagem óbvia é a falta de escalabilidade e os resíduos de largura de banda que ocorre quando uma mensagem é enviada várias vezes ao longo de links que podem potencialmente ser compartilhados entre vários membros do grupo (HOLEMAN, 2002).

Broadcasting é uma forma de enviar uma mensagem para todos da rede, interessados ou não. Para n remetentes, n mensagens são enviadas e cada entidade recebe uma mensagem, mesmo se a entidade não está interessada. No caso de radiodifusão, a vantagem é que todos os membros do grupo recebem a comunicação com pouco ou nenhum encaminhamento. No entanto, não é eficiente em termos de uso da rede desde que a mensagem é enviada para membros e não membros do grupo (HOLEMAN, 2002). A Figura 4 exibe o esquema desse tipo de transmissão.



Figura 4. Esquema de Transmissão Broadcast

Multicasting foi desenvolvido como um caminho para enviar uma mensagem para mais do que um membro enquanto com a conservação de recursos, propagando a mensagem apenas a medida que ela precise ir para chegar a cada membro do grupo e apenas uma vez ao longo de cada caminho. Em uma comunicação *multicast*, cada remetente transmite apenas uma cópia que é replicada dentro da rede e entregue aos vários receptores. Por esta razão, *multicasting*, tipicamente requer menos banda do que várias mensagens *unicast* para cada receptor (HOLEMAN, 2002). A Figura 5 ilustra como funciona a transmissão *multicast*.



Figura 5. Esquema de Transmissão Multicast

A estratégia proposta faz uso de refletores multimídia construídos no modelo multiple unicast.

2.3 Refletor Multimídia para Transmissão UDP

Um refletor recebe uma cópia de um fluxo e envia múltiplas cópias para outros destinos, que podem ser outros refletores, ou seja, quem deve se preocupar com a distribuição do *stream* de vídeo é a rede da máquina onde o refletor está sendo executado (ANDREEV, 2003).

Um refletor multimídia UDP é um refletor especializado para recebimento e redistribuição de fluxo multimídia utilizando o protocolo UDP. A Figura 6 ilustra o esquema de um refletor que recebe fluxo UDP e a faz a reflexão desse fluxo também utilizando o protocolo UDP.



Figura 6. Esquema de um Refletor Multimídia para Transmissão UDP.

A utilização de refletores para distribuição de conteúdo multimídia pode ser aplicado em diferentes contextos, visto que é uma solução para a replicação de conteúdo. Um exemplo dessa aplicação pode ser facilmente visualizado no Cinema Digital, onde é possível fazer a transmissão de filmes a serem exibidos, em tempo real, em cinemas geograficamente distribuídos e conectados digitalmente.

Uma vantagem de sua utilização é sua flexibilidade, pois é possível montar um esquema de otimização de transmissões colocando refletores geograficamente e estrategicamente distribuídos, com o objetivo de minimizar a quantidade de banda utilizada (MELO, 2010a). Essa otimização é possível fazendo que um refletor envie um fluxo para outro e assim por diante, buscando enviar um único fluxo até atingir o

destino final, o que torna essa estratégia muito parecida com a transmissão multicast (descrita na seção 2.2), porém em software e não dependente de estratégias de rede, o que dá mais flexibilidade. A Figura 7 ilustra esse processo, onde um remetente na Paraíba distribui, em apenas um fluxo, dados para todo o Brasil.



Figura 7. Refletores geograficamente distribuídos otimizando uma distribuição *multiple unicast* de forma similar à *multicast*

Aliado com estratégias de criptografia, a estratégia proposta usa refletores para a transmissão multimídia utilizando o protocolo UDP.

2.4 Criptografia de Chave Simétrica e Assimétrica

Segundo Stallings (2008), uma mensagem original é conhecida como texto claro e uma mensagem codificada é conhecida como texto cifrado. O processo de converter um texto claro em um texto cifrado chama-se criptografia e o processo inverso, ou seja, converter texto cifrado em texto claro chama-se deciptografia.

O método de criptografia simétrica é um tipo de criptossistema em que a criptografia e a deciptografia são realizadas utilizando uma mesma chave, transformando o dado claro em um dado cifrado usando uma chave secreta e um algoritmo de criptografia. Da mesma maneira, a mesma chave e um algoritmo de

decriptografia são utilizados para transformar de volta o dado cifrado em um dado claro (STALLINGS, 2008). A Figura 8 ilustra o modelo de cifra simétrica.

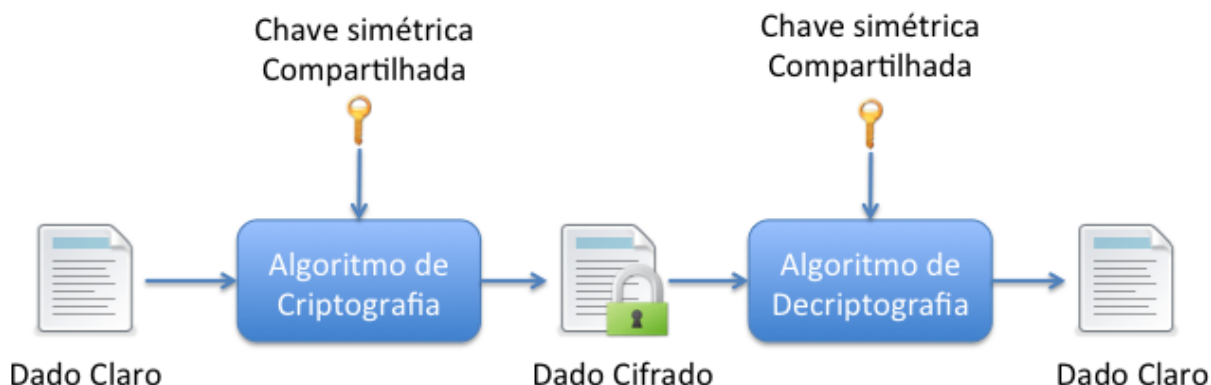


Figura 8. Esquema do Modelo de Cifra Simétrica

A criptografia de cifras simétricas é também conhecida como criptografia de chave privada e possui dois algoritmos clássicos: o *Data Encryption Standard* (DES) (STALLINGS, 2008) e o *Advanced Encryption Standard* (AES) (AES, 2011). Apesar dos esforços para fortalecer o DES, com a utilização do 3DES (uma maneira de aplicar o DES três vezes), este algoritmo se tornou obsoleto e vem sendo substituído pelo AES.

O método de criptografia assimétrica é um tipo de criptossistema em que a criptografia e decriptografia são realizadas utilizando diferentes chaves, chamadas de chave pública e chave privada. A criptografia utiliza uma das chaves e um algoritmo de criptografia, já a decriptografia é feita utilizando a outra chave e um algoritmo de decriptografia (STALLINGS, 2008). A Figura 9 ilustra o esquema da cifra assimétrica.



Figura 9. Esquema do Modelo de Cifra Assimétrica

A criptografia de cifras assimétricas é também conhecida como criptografia de chave pública e o algoritmo mais utilizado na criptografia assimétrica é o RSA (RSA,

2011), sigla que denota o nome de seus criadores: Rivest, Shamir e Adleman (STALLINGS, 2008). Contudo, Hankerson (2004) apresenta o *Elliptic Curve Cryptography*, um algoritmo de cifra assimétrica que afirma ser tão seguro quanto o RSA 1024 bits, porém mais eficiente.

Uma das deficiências da criptografia simétrica é a necessidade de ter uma chave compartilhada entre a origem e o destino, já que isso pode ser uma brecha para ataques. Esse problema não existe na criptografia assimétrica, onde é previsto que uma das chaves será pública e será utilizada para a criptografia, enquanto uma das chaves é privada e utilizada para a decryptografia. A criptografia assimétrica, por sua vez, tem um desempenho muito inferior em relação à criptografia simétrica e é inviável sua utilização para um grande volume de dados. Na prática os dois modos são utilizados de forma combinada, onde a criptografia assimétrica é utilizada para a troca de uma chave simétrica e a criptografia simétrica é utilizada para a criptografia dos dados (STALLINGS, 2008).

Por conta do grande volume de dados a ser transmitido pelas transmissões expostas nesse trabalho, o desempenho é um fator crucial e a escolha da criptografia simétrica foi imprescindível. O algoritmo utilizado foi o AES.

2.5 AES como Cifra de Fluxo no Modo Contador

Uma cifra de fluxo é aquela que codifica um fluxo de dados digital um bit ou byte de cada vez, enquanto uma cifra de bloco é aquela em que um bloco de texto claro é tratado como um todo e usado para produzir um bloco de texto cifrado com o mesmo tamanho (STALLINGS, 2008).

Nativamente o AES é uma cifra de bloco e, para criptografia de fluxos de mídia, mudanças são necessárias para que este se torne uma cifra de fluxo. Desse modo, cada bloco deixa de ser criptografado em função de si mesmo para ser criptografado em função dos blocos anteriores (DWORKIN, 2012). O modo do AES utilizado por este trabalho é o Modo Contador, onde o próximo bloco é gerado por intermédio da criptografia de sucessivos valores de um “contador”. Qualquer função que produza uma sequência que não se repetirá por um longo tempo pode ser utilizada como contador, embora um contador simples seja a solução comumente utilizada. A Figura 10 mostra a criptografar do AES no Modo Contador.

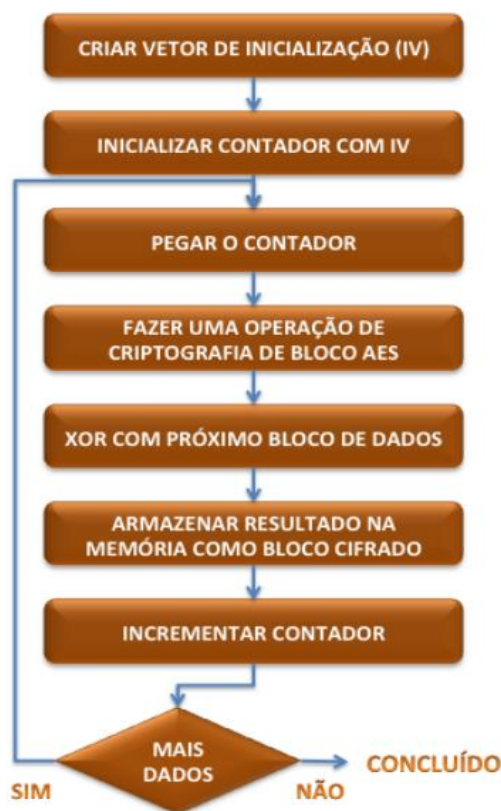


Figura 10. Esquema de encriptação do AES no Modo Contador (VIEIRA, 2011)

2.6 Funções de HASH e o Algoritmo SHA

Uma função de *hash* mapeia uma mensagem de tamanho variável em um valor de *hash* de tamanho fixo (STALLINGS, 2008), ou seja, uma mensagem A é mapeada para um valor *hash* B e não é possível, a partir de B , voltar para a mensagem A .

Segundo Stallings (2008), um valor de *hash* h é gerado por uma função H , a partir de uma mensagem M , da seguinte forma: $h = H(M)$, onde H tem as seguintes características:

- H pode ser aplicado a um bloco de dados de qualquer tamanho;
- H produz uma saída de comprimento fixo;
- $H(x)$ é relativamente fácil de calcular para qualquer x ;
- Para qualquer valor h dado, é computacionalmente inviável encontrar x ;
- Para qualquer bloco dado x , é computacionalmente inviável encontrar y , tal que $H(x) = H(y)$;
- É computacionalmente inviável encontrar qualquer par (x, y) , tal que $H(x) = H(y)$.

Um algoritmo de *hash* que foi amplamente utilizado foi o *Message-Digest Algorithm5* (MD5) que produz valor de *hash* de 128 bits e sua utilização vem sendo substituída pelo *Secure Hash Algorithm* (SHA) versão 1 que produz valor de *hash* de 160 bits. Este, por sua vez, já vem sendo substituído por outras versões de 256, 384 e 512 bits de tamanhos de *hash*, porém seguem basicamente a mesma estrutura do SHA-1 (STALLINGS, 2008). A Tabela 1 faz um comparativo entre todas as versões do SHA e é possível observar que as mudanças mais significativas são relacionadas à segurança.

Tabela 1: Comparação dos Parâmetros do SHA. Adaptado de STALLINGS (2008)

	SHA-1	SHA-256	SHA-384	SHA-512
Tamanho do resumo da mensagem	160	256	384	512
Tamanho da mensagem	$<2^{64}$	$<2^{64}$	$<2^{128}$	$<2^{128}$
Tamanho do bloco	512	512	1024	1024
Tamanho da palavra (word)	32	32	64	64
Número de etapas	80	64	80	80
Segurança	80	128	192	256

2.7 Autenticação Federada e a CAFe

A autenticação federada permite que um sujeito se autentique em sua federação e possa usufruir de serviços providos por um Provedor de Serviços (*Service Provider*) fora de sua instituição, mas pertencente a federação, pois existe uma relação de confiança entre as entidades federadas, ou seja, há uma autenticação no Provedor de Identidade (*Identity Provider*) da entidade federada de origem e isso dá acesso a todos os serviços das entidades integrantes da federação. Esse modelo de autenticação e oferta de serviços tem se tornado amplamente utilizado porque já se mostrou muito confiável, seja por evitar inúmeros cadastros e senhas aos sujeitos participantes, uma vez que um único cadastro na federação de origem é necessário. Sua utilização facilita a distribuição de qualquer serviço que esteja disponível em qualquer federação integrante.

No Brasil um dos principais representantes do modelo de autenticação federada é a Comunidade Acadêmica Federada (CAFe) (CAFÉ, 2012), que é uma federação de identidade constituída por instituições de ensino brasileiras, que permite a qualquer usuário manter as suas informações em sua própria instituição, podendo

ter acesso a serviços que podem ser oferecidos por outras instituições que participam da federação.

Cada instituição pertencente pode atuar como provedora de identidade (IdP) e/ou como provedoras de serviço (SP). A RNP é responsável pela gestão do serviço e por manter o repositório centralizado com dados sobre integrantes da federação.

Uma das vantagens da CAFé é possibilidade do usuário ter uma única conta em sua instituição, e essa conta é válida para todos os serviços oferecidos à toda a federação. Para isso, é necessária uma relação de confiança entre instituições participantes da Federação, o que permite que um usuário se autentique unicamente em sua instituição de origem e tenha sua identidade reconhecida pelos serviços das demais instituições. Os serviços de ensino a distância e atividades de colaboração são os que mais se beneficiam com essa infraestrutura.

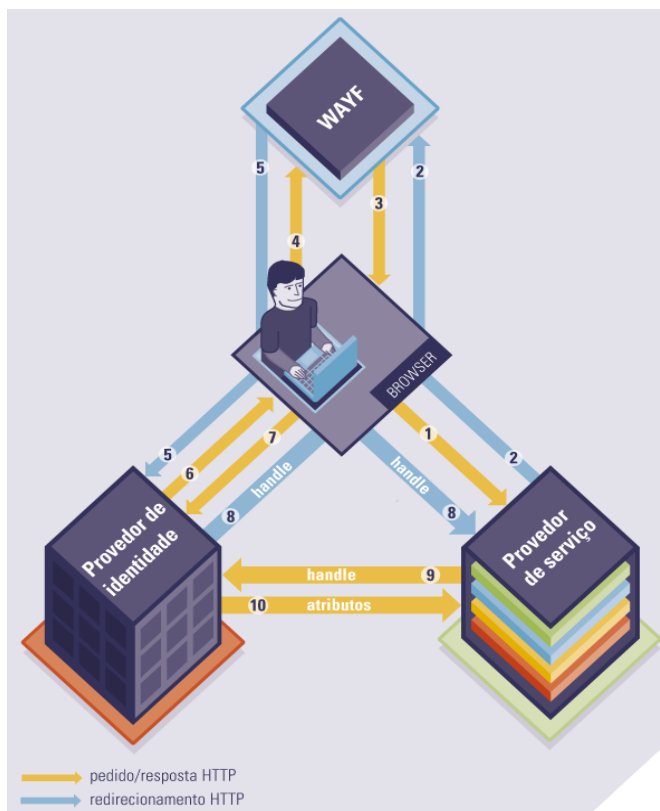


Figura 11. Funcionamento da CAFé (CAFE, 2012)

A Figura 11 ilustra o funcionamento da CAFé e este é descrito pelos seguintes passos:

1. O usuário direciona seu navegador para a página do serviço desejado.
2. O servidor redireciona o navegador para o serviço de descoberta da federação (WAYF).

3. O serviço de descoberta apresenta ao usuário as instituições que oferecem provedores de identidade para a federação.
4. O usuário seleciona uma instituição, e seu navegador envia ao serviço de descoberta os dados dessa seleção.
5. O serviço de descoberta redireciona o navegador para a instituição selecionada.
6. O provedor de identidade da instituição envia ao navegador a página de autenticação do usuário.
7. O usuário fornece suas credenciais e o navegador as envia ao provedor de identidade.
8. O provedor de identidade gera um *handle* e o envia ao navegador, que o encaminha ao provedor de serviço, que assim obtém a prova de autenticação do usuário. Para algumas aplicações, isso é suficiente para autorizar o acesso do usuário ao serviço.
9. Opcionalmente, o provedor de serviço pode enviar um pedido de atributos ao provedor de identidade/atributos, utilizando o *handle* para especificar o usuário em questão.
10. O provedor de identidade/atributos retorna os valores dos atributos requisitados.

A estratégia usa a CAFé para que os usuários possam usufruir das vantagens de uma autenticação federada.

CAPÍTULO 3: ARTHRON 3.0

Esse capítulo apresenta a ferramenta Arthron que inicialmente foi produzida para o contexto de artes digitais e evoluiu para o contexto de telemedicina que, para esse último contexto, a versão produzida foi a 3.0. A Arthron 3.0 serviu de motivação para o desenvolvimento do trabalho e, ao final, serviu para a verificação dos métodos descritos, pois a estratégia proposta foi integrada à solução.

3.1 Arthron 1.0 e 2.0

A Arthron é uma ferramenta de gerenciamento remoto que permite a captura e a distribuição de múltiplos fluxos simultâneos de mídia em tempo real. Na sua versão 1.0 (MELO, 2010a), a ferramenta prioriza o apoio a manifestações de caráter artístico onde fluxos de áudio e vídeo são transmitidos e chaveados simultaneamente. A Figura 12 ilustra uma transmissão utilizando a Arthron, onde é possível ver a interação entre agentes humanos e sintéticos que estão geograficamente distribuídos. Todo esse conjunto artístico é controlado remotamente pela ferramenta.

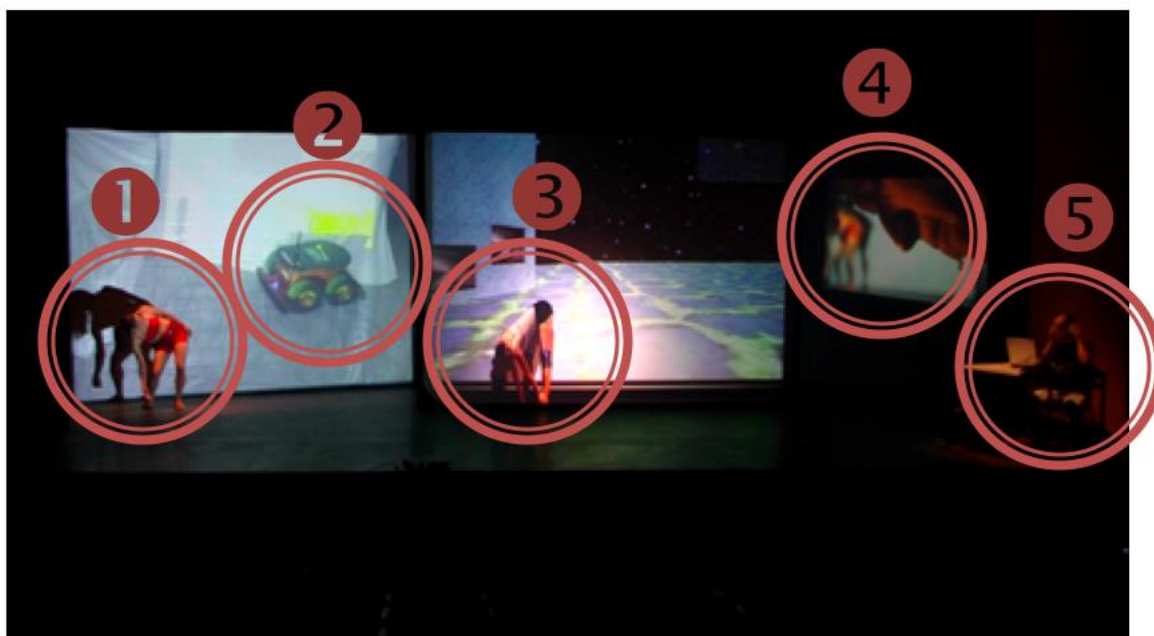


Figura 12. Evento transmitido utilizando a Arthron (MELO, 2010a)

A ampla aplicabilidade da ferramenta permite sua utilização em outros ambientes que realizem gerenciamento de fluxos de mídia de uma forma geral,

como sistemas de telemedicina, tele aulas e eventos técnico-científicos. A Figura 13 ilustra a arquitetura da Arthron 1.0.

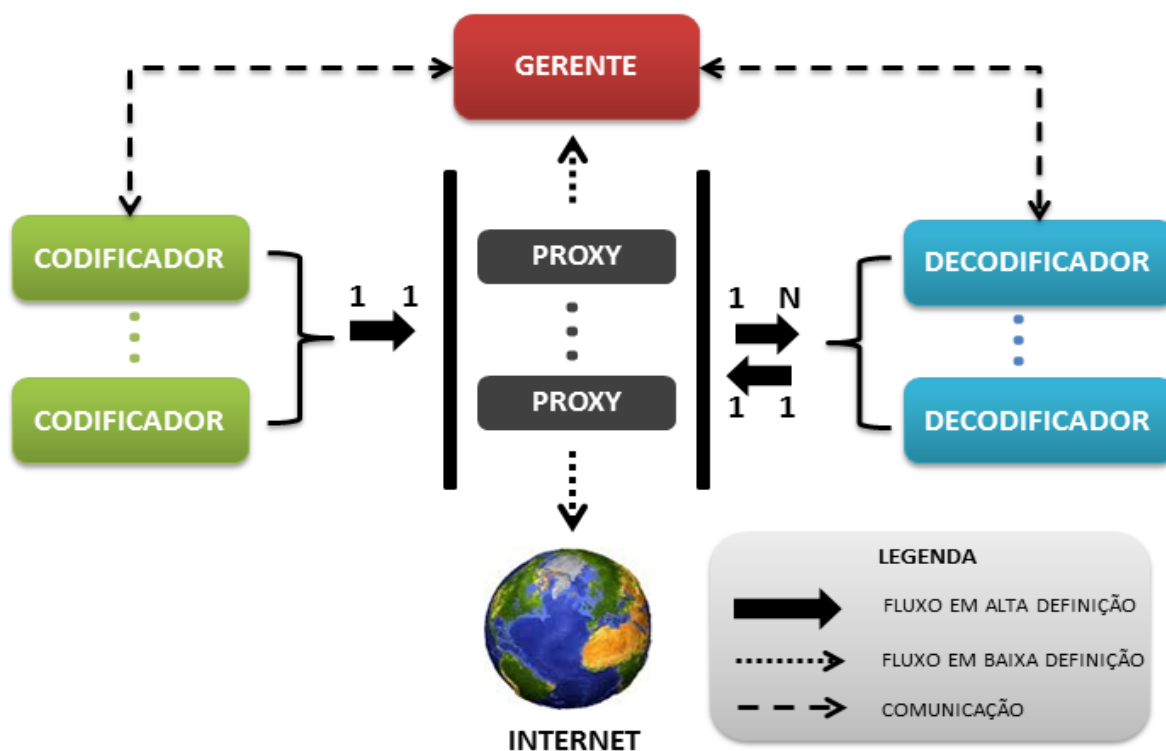


Figura 13. Arquitetura da Arthron 1.0. Adaptada de Melo (2010a)

A versão 2.0 da Arthron (VIEIRA, 2012) visa dar suporte a atividades essenciais em sistemas de telemedicina através da transmissão de cirurgias em tempo real e de forma colaborativa, com novos módulos e com uma camada de segurança em relação à versão 1.0, mas ainda como uma ferramenta. Nessa versão o *Proxy* mudou para *Reflector* porque esse nome representa de maneira mais adequada o que esse módulo realmente é. A Figura 14 ilustra a arquitetura da Arthron 2.0 e evidencia uma clara evolução em relação à arquitetura apresentada na Figura 13.

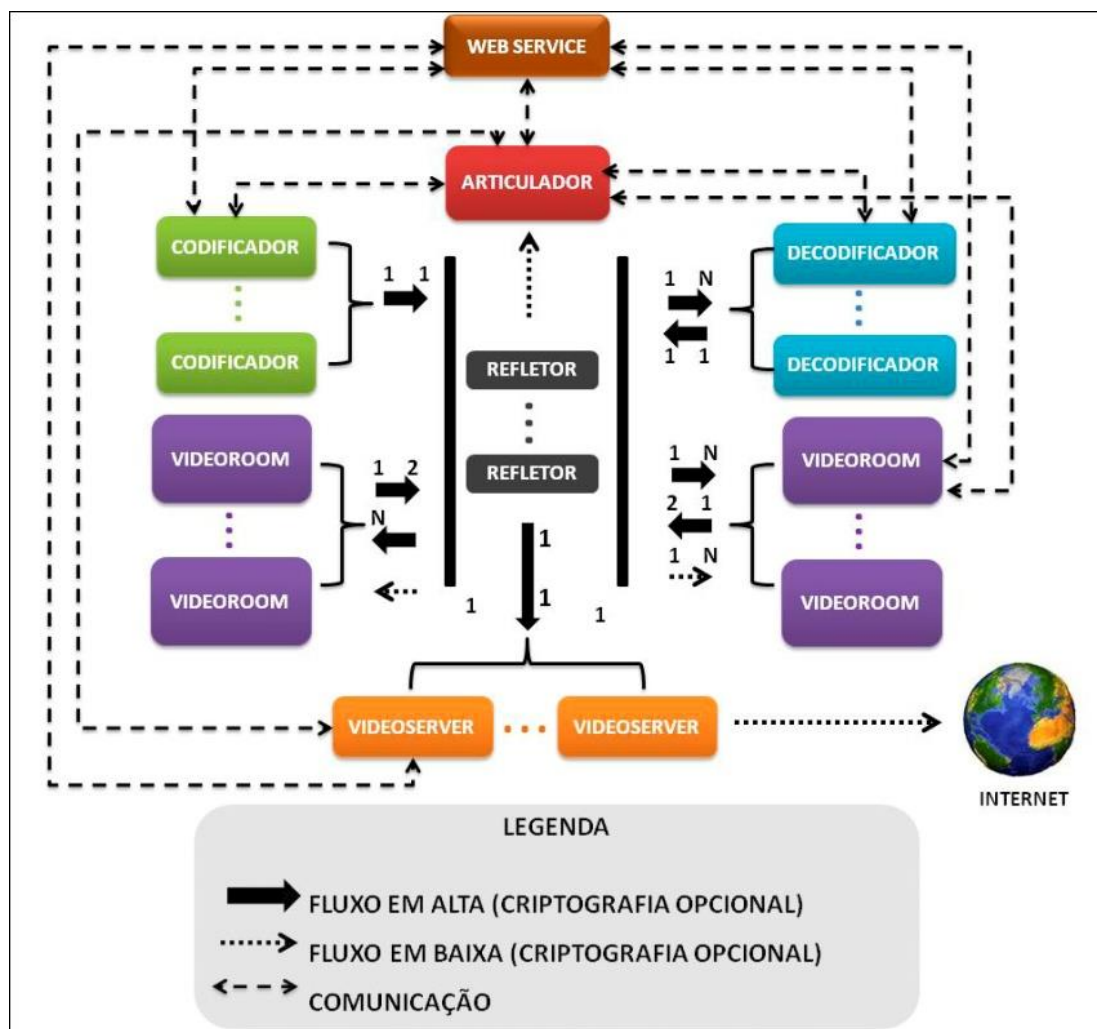


Figura 14. Arquitetura da Arthron 2.0 (VIEIRA, 2012)

A Arthron 3.0 partiu para o Paradigma Web com o intuito de se tornar um serviço da RNP e tem inovações que vão desde a sua usabilidade, a comunicação entre os componentes e com uma camada de segurança aperfeiçoada, em relação à versão 2.0, e integrada com a CAFé. Essa camada de segurança é o foco desse trabalho.

3.2 Arquitetura

Para acomodar as novas funcionalidades na Arthron 3.0 a arquitetura apresentada na Figura 14 evoluiu dando lugar a nova arquitetura, apresentada na Figura 15, onde é possível verificar os novos módulos da não mais ferramenta e sim serviço: VSecurityServer, ArthronServer e Recorder. Esses módulos são responsável pela segurança, gerenciamento dos módulos e gravação da experiência, respectivamente, e serão descritos a seguir.

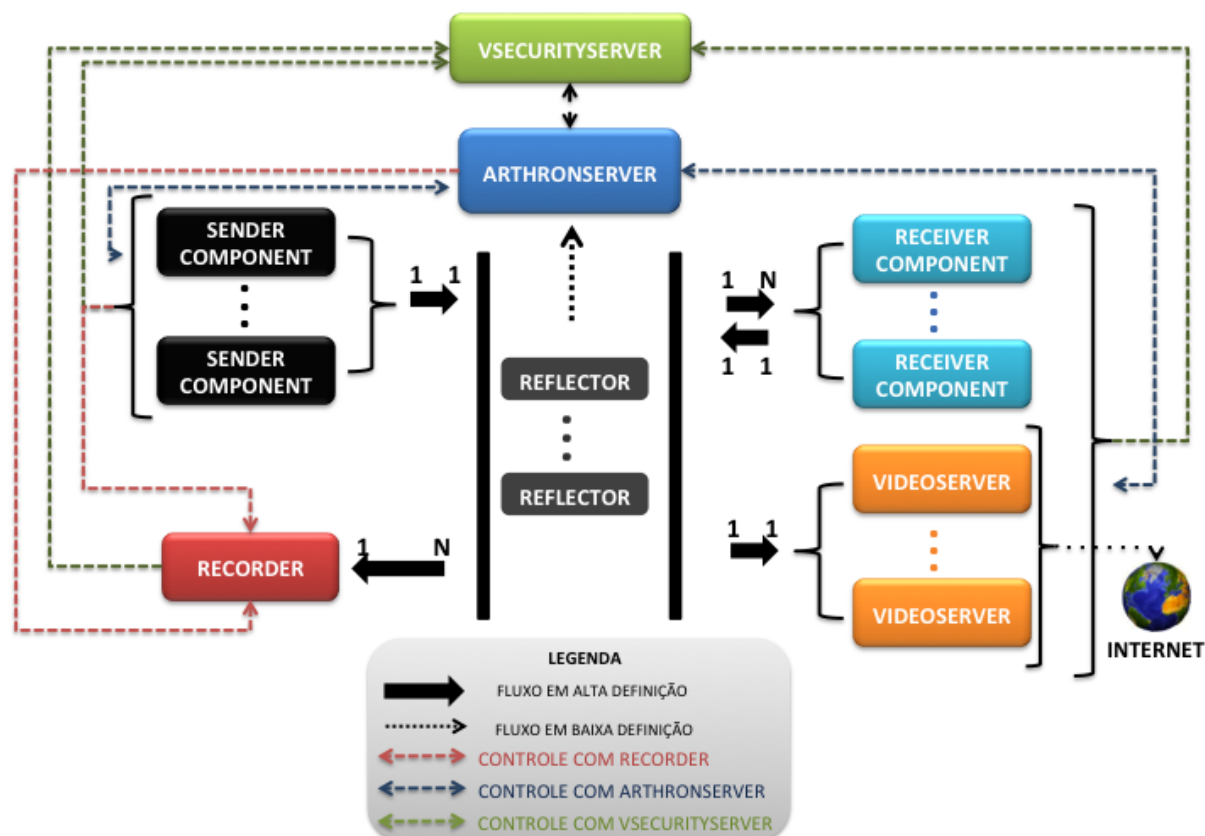


Figura 15. Arquitetura da Arthron 3.0

Nota-se também que os módulos Encoder, Decoder e VideoRoom deixam de existir e passam a ser vistos como módulos com capacidades que os representem, ilustrados por *SenderComponent* e *ReceiverComponents*, ou seja, componente com capacidade de envio e componente com capacidade de recebimento e esses módulos agora são agrupados dentro de uma dessas categorias.

3.3 Componentes

Nessa seção são descritos os componentes da Arthron 3.0.

3.3.1 ArthronServer

O ArthronServer é o componente responsável pelo gerenciamento dos componentes e pelo monitoramento do sistema, gerenciando os módulos conectados e os fluxos de mídia sendo transmitidos. Uma de suas funcionalidades também é a de criação e gerenciamento de diversas sessões (VIEIRA, 2011) de maneira simultânea, permitindo ao usuário o controle de transmissões de várias cirurgias ao mesmo tempo, sendo possível abrir, criar, fechar e moderar essas sessões.

O objetivo do ArthronServer é trazer, para o paradigma web, as funcionalidades que o Articulador (VIEIRA, 2012) possui, mas de forma adequada a esse novo contexto para possibilitar a utilização da Arthron como um serviço com prévio agendamento.

A Figura 16 ilustra o Gerenciamento de Sessões, onde é possível visualizar as sessões que um usuário possui e informações adicionais.



ID	Previsão de Início	Previsão de Término	Finalizada em	Moderada	Gravada	Status	Proprietário
13	05/07/2012 00:00	06/07/2012 00:00		Sim	Sim	Em Andamento	GTAVCS
14	05/07/2012 00:00	06/07/2012 00:00		Sim	Sim	Em Andamento	GTAVCS
8	03/07/2012 04:09	04/07/2012 00:00	04/07/2012 00:00	Sim	Sim	Terminada	GTAVCS
7	03/07/2012 04:08	03/07/2012 04:08	03/07/2012 16:08	Sim	Sim	Terminada	GTAVCS
5	30/05/2012 21:00	31/05/2012 21:00	03/07/2012 16:03	Sim	Sim	Terminada	GTAVCS

Figura 16. Gerenciamento de Sessões no ArthronServer

A Figura 17 expõe a tela de gerenciamento de fluxos no ArthronServer, onde são exibidos os componentes de envio conectados e os componentes de recebimento. Nessa tela, é possível efetuar o chaveamento de um componente de envio para um determinado componente de recebimento do fluxo, que pode ser mais de um.



Figura 17. Gerenciamento de Fluxos de uma Sessão no ArthronServer

3.3.2 SenderComponent

O *SenderComponent* agrupa todos os componentes que tem a capacidade de enviar fluxos de mídia para algum destino. Dessa forma, o ArthronServer pode gerenciar esses envios adicionando destinos para que o fluxo multimídia seja enviado. Dois componentes da Arthron 2.0 se encaixam com essa capacidade, são eles:

- Encoder: responsável pela captura, codificação e distribuição de uma fonte de mídia, fonte essa que tem como destino um ou mais *Receiver*. Sua interface gráfica é exibida na Figura 18.

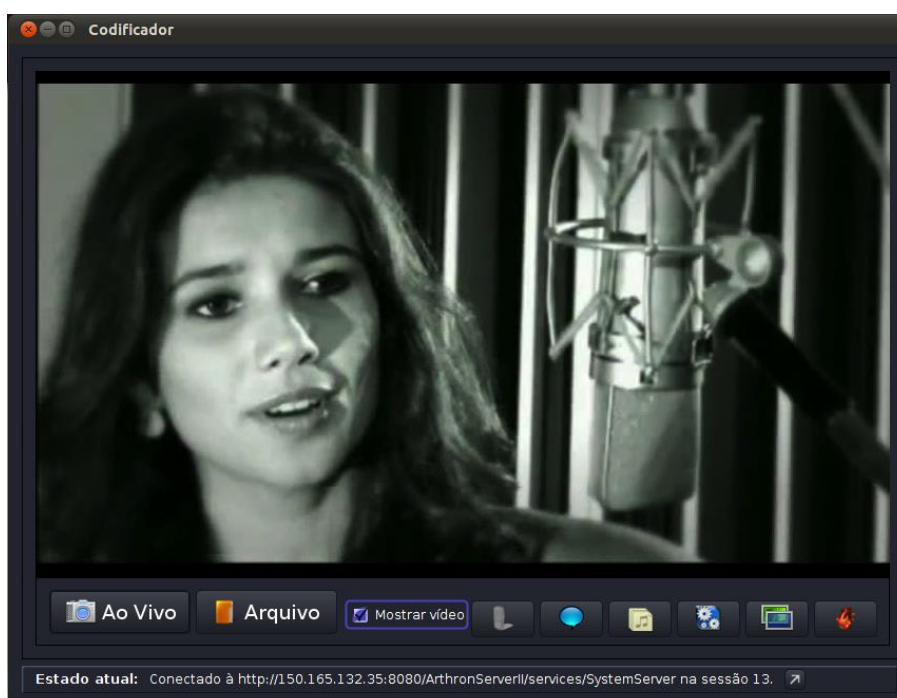


Figura 18. Interface Gráfica do Encoder

- VideoRoom: é um agente para videoconferência, composto por um Encoder e n Decoders, com a finalidade de prover a comunicação simultânea de vários usuários. Este componente permite que o usuário envie um fluxo de vídeo e receba vários outros. Os fluxos atribuídos pelo Articulador ficam dispostos na tela, de modo que o operador do componente escolha qual deles é exibido em alta definição, enquanto os outros são exibidos em baixa definição. A Figura 19 mostra a interface gráfica do VideoRoom.



Figura 19. Interface Gráfica do VideoRoom

3.3.3 ReceiverComponent

O *ReceiverComponent* agrupa todos os componentes que tem a capacidade de receber um ou mais fluxos de mídia. Esses são os destinos dados aos *SenderComponentes* pelo ArthronServer e os componentes da Arthron 2.0 que se encaixaram foram:

- VideoRoom: descrito na seção 3.3.2.
- Decoder: módulo responsável pela captura de um único fluxo de mídia, fazer a decodificação e exibição. Sua interface gráfica é ilustrada na Figura 20.

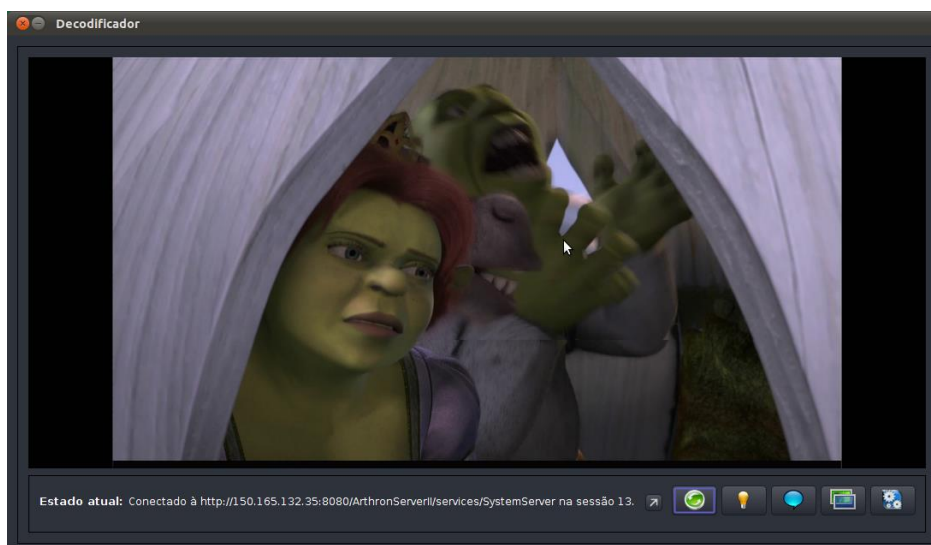


Figura 20. Interface Gráfica do Decoder

3.3.4 VideoServer

A função do VideoServer é transmitir vídeos em baixa definição e em vários formatos para clientes web. Para que isso aconteça, o componente é associado com um *SenderComponent* e é responsável por receber seu fluxo, realizar a transcodificação do conteúdo original para resoluções, taxas e codificações aceitáveis para uma transmissão HTTP para a internet e publicar potencialmente o fluxo resultante em uma página da web que pode ser gerada automaticamente pelo serviço. Sua interface gráfica é ilustrada na Figura 21.

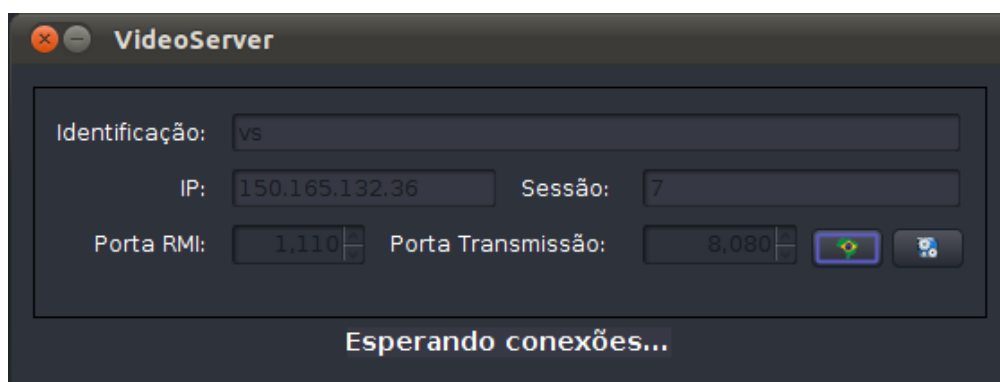


Figura 21. Interface Gráfica do VideoServer

3.3.5 Reflector

O Reflector é o módulo responsável por fazer a redistribuição de um fluxo multimídia e uma possível otimização dessa redistribuição, ou seja, esse módulo recebe um fluxo de faz sua reflexão para diversos destinos.

Este pode está interno a algum *SenderComponent* e faz o envio do fluxo da mídia sendo capturada para todos os Receivers, ou pode estar situado em um ponto estratégico próximo aos Receivers, onde apenas um único fluxo percorre a maior parte do caminho e, do Reflector, é redistribuído aos destinos finais, similar à transmissão *multicast*. A Figura 22 ilustra este módulo.

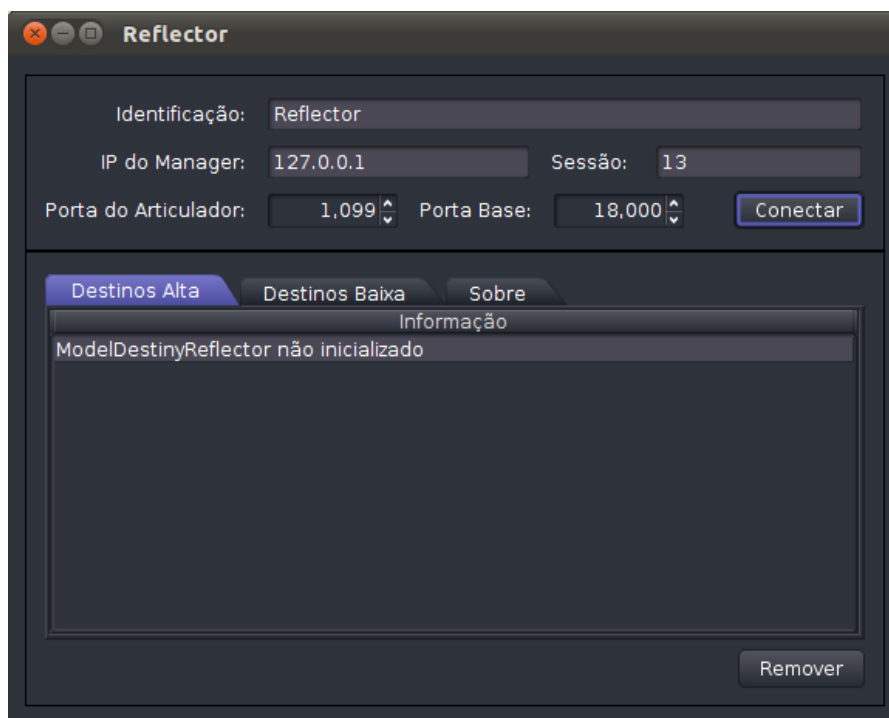


Figura 22. Interface Gráfica do Reflector

3.3.6 Recorder

Esse componente tem a finalidade de gravar todos os fluxos sendo transmitidos em uma sessão e de prover os meios para uma posterior recuperação fiel à experiência realizada. Essa gravação é efetuada com todos os *Senders* enviando uma cópia do fluxo para o Recorder, sendo registrados os chaveamentos realizados nos *Receivers*. Dessa maneira, o Recorder mantém a informação de quais fluxos um determinado *Receiver* recebeu e em qual momento, permitindo a reprodução da experiência da sessão a posteriori.

A recuperação da experiência de uma sessão ocorre de modo individual na visão de cada *Receiver*. A Figura 23 ilustra um Decoder conectado ao Recorder e recebendo a recuperação da experiência.

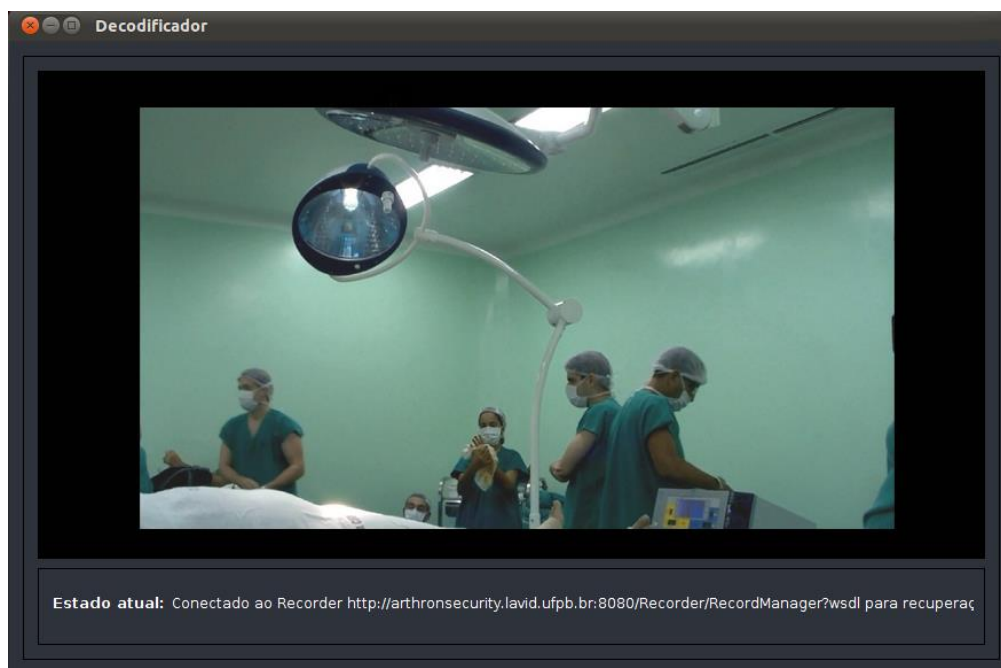


Figura 23. Recuperação da Experiência no Decoder

Outra maneira de recuperar a experiência é visualizar os vídeos individuais, na íntegra, de cada *Sender*. Essa recuperação pode ser realizada no ArthronServer, conforme ilustrado na Figura 24.



Figura 24. Recuperação da Experiência no ArthronServer

3.3.7 VSecurityServer

Esse módulo é responsável pela camada de segurança do serviço e é uma das contribuições dessa dissertação. Seus detalhes se encontram nas seções 5.2 e 6.3.

CAPÍTULO 4: AUTENTICAÇÃO DE SUJEITOS E CRIPTOGRAFIA MULTIMÍDIA

Esse capítulo descreve a análise de técnicas para autenticação e criptografia de fluxos multimídia identificadas na literatura através de um mapeamento sistemático (PETERSEN, 2008) e da análise dos trabalhos relacionados, complementando a fundamentação teórica desse trabalho.

4.1 Mapeamento Sistemático

Em busca de técnicas, clássicas e atualizadas, que permitissem a transmissão segura de fluxos multimídia foi feito um mapeamento sistemático (PETERSEN, 2008) que indicasse os caminhos a serem seguidos. O mapeamento também indicou como está o interesse do tema nos últimos anos e possíveis meios de publicação que podem ser explorados ao fim desse trabalho. Outra contribuição desse capítulo é como os trabalhos relacionados que puderam ser analisados e comparados com essa dissertação. Inicialmente é descrito o protocolo utilizado para o mapeamento e, em seguida, os resultados obtidos.

O mapeamento sistemático é um tipo de revisão sistemática em que se realiza uma revisão mais ampla dos estudos primários, em busca de identificar evidências disponíveis, bem como identificar lacunas no conjunto dos estudos primários, ponto de partida para direcionar o foco de revisões sistemáticas futuras e para identificar áreas onde mais estudos primários precisam ser conduzidos (PETERSEN, 2008).

A técnica de mapeamento sistemático foi utilizada para investigar na literatura diferentes estratégias que abordem o problema de segurança na transmissão em tempo real de múltiplos fluxos de mídia em alta definição. O processo de planejamento do estudo é discutido em detalhes por meio de um protocolo descrito a seguir.

4.1.1 Planejamento – Definição do Protocolo

Nessa seção é descrito o protocolo utilizado no mapeamento.

4.1.1.1 Descrição do Problema

Certos requisitos de segurança se tornam necessários em certos tipos de interatividade digital, principalmente no que se refere às transmissões de fluxos em

alta definição e em tempo real, como na telemedicina. Para proporcionar a segurança na transmissão desses dados, é importante estudar estratégias de segurança e suas diferentes abordagens, a fim de investigar a que se enquadre melhor nesse cenário, alcançando um melhor desempenho ao menor custo computacional.

4.1.1.2 Objetivo

O estudo do mapeamento sistemático proporcionará a análise dos algoritmos de criptografia; estratégias de distribuição de chaves; autenticação e segurança em *multicast*, *broadcast* e *multiple unicast*. Também tem o intuito de contribuir no entendimento desses conceitos e torná-los de fácil consulta e utilização para outros pesquisadores.

4.1.1.3 Questões de Pesquisa

Um levantamento de questões foi realizado a fim de respondê-las ao final da pesquisa. São elas:

Questão 1: Como estão distribuídas as publicações ao longo dos anos?

Questão 2: Que tipos de criptografia estão sendo utilizadas?

Questão 3: É possível distribuir as publicações seguindo uma taxonomia? Se sim, como está esta distribuição?

Questão 4: Quais estratégias de distribuição de chaves de criptografia são predominantes?

Questão 5: Qual o algoritmo de criptografia mais utilizado?

4.1.1.4 Palavras chaves e Strings de Busca

Para a busca de publicações do mapeamento, as strings de busca foram baseadas em: segurança, criptografia, *multicasting*, transmissão de fluxo, fluxo de mídia e alta definição; *security*, *cryptography*, *multicasting*, *streaming*, *media stream* e *high definition*. Essas palavras foram escolhidas por estarem no contexto do tema e serem frequentemente utilizadas em publicações da área.

Foram utilizados oito engenhos de busca que foram selecionados por permitirem acesso gratuito pela rede da UFPB. As strings de busca foram construídas em inglês e português e são as seguintes:

- IEEEXplorer³
 - (“Security” OR “Cryptography”) AND (“Multicasting” OR “Streaming” OR “Media Stream”) AND “High Definition”
 - (“Segurança” OR “Criptografia”) AND (“Multicasting” OR “Streaming” OR “Fluxo de Mídia”) AND “Alta Definição”
- ACM Digital Library⁴
 - (“Security” OR “Cryptography”) AND (“High Definition” OR “Stream” OR “Multicast” OR “Media Stream”)
 - (“Segurança” OR “Criptografia”) AND (“Alta Definição” OR “Streaming” OR “Multicast” OR “Fluxo de Mídia”)
- Google Scholar⁵
 - (“Security” OR “Cryptography”) AND (“Multicasting” OR “Streaming” OR “Media Stream”) AND (“High Definition”)
 - “Segurança” OR “Criptografia”) AND (“Multicasting” OR “Streaming” OR “Fluxo de Mídia”) AND (“Alta Definição”)
- Scielo⁶
 - (“Security” OR “Cryptography”) AND (“High Definition” OR “Stream” OR “Multicast” OR “Media Stream”)
 - (“Segurança” OR “Criptografia”) AND (“Alta Definição” OR “Stream” OR “Multicast” OR “Fluxo de Mídia”)
- Science Direct⁷
 - title-abs-key((Security OR Cryptography) and ({High Definition} OR Stream OR Multicast OR {Media Stream}))
 - title-abs-key((Segurança OR Criptografia) and ({Alta Definição} OR Stream OR Multicast OR {Fluxo de Mídia}))

³ Disponível em: ieeexplore.ieee.org

⁴ Disponível em: dl.acm.org.ez15.periodicos.capes.gov.br

⁵ Disponível em: scholar.google.com.br

⁶ Disponível em: www.scielo.org

⁷ Disponível em: www.sciencedirect.com.ez15.periodicos.capes.gov.br

- Springer Link⁸
 - (“Security” OR “Cryptography”) AND (“High Definition” OR “Stream” OR “Multicast”)
 - (“Segurança” OR “Criptografia”) AND (“Alta Definição” OR “Fluxo” OR “Multicast”)
- Science⁹
 - (Security OR Cryptography) and (“High Definition” OR Stream OR Multicast OR “Media Stream”)
 - (Segurança OR criptografia) AND (“Alta Definição” OR Stream OR Multicast OR “Fluxo de Mídia”)
- Scopus¹⁰
 - title-abs-key((Security OR Cryptography) and ({High Definition} OR Stream OR Multicast OR {Media Stream}))
 - title-abs-key((segurança OR criptografia) AND ({Alta Definição} OR Stream OR Multicast OR {Fluxo de Mídia}))

4.1.1.5 Método utilizado para pesquisa de Fontes Primárias

O método utilizado para o levantamento de fontes primárias compreendeu a realização de buscas nos oito engines, resultando em 190 publicações. A Figura 25 apresenta os resultados obtidos em cada engine utilizado.

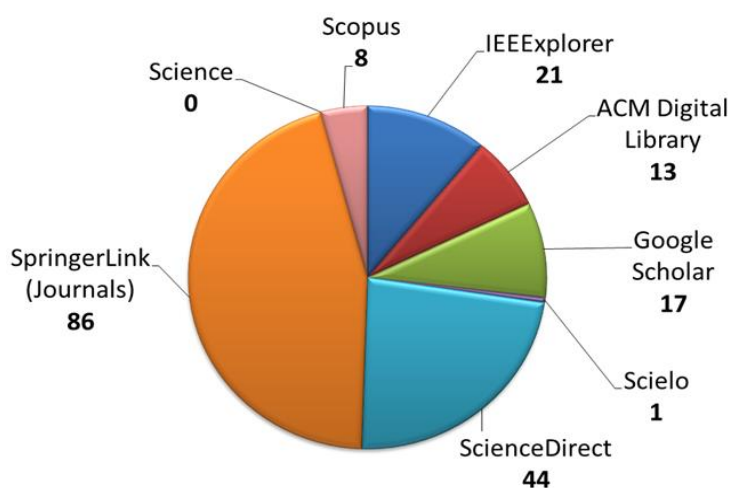


Figura 25. Contribuição de Publicações dos Engenhos de Busca.

⁸ Disponível em: www.springerlink.com.ez15.periodicos.capes.gov.br

⁹ Disponível em: www.sciencemag.org.ez15.periodicos.capes.gov.br

¹⁰ Disponível em: www.scopus.com.ez15.periodicos.capes.gov.br

4.1.1.6 Critério para Inclusão dos Estudos

Os critérios definidos para inclusão dos estudos são apresentados a seguir na Tabela 2.

Tabela 2. Critérios de Inclusão de estudos no Mapeamento Sistemático.

Estudos escritos em português ou em inglês.
Trabalhos que abordem aplicação de criptografia.
Trabalhos que apresentem alguma das strings de busca em seu título, resumo/abstract ou palavras-chave.
Trabalhos relacionados a métodos de segurança de fluxos de mídia.
Trabalhos que abordem estratégias de distribuição de chaves.

4.1.1.7 Critério para Exclusão dos Estudos

Os critérios definidos para exclusão dos estudos são apresentados a seguir na Tabela 3.

Tabela 3. Critérios de Exclusão de estudos no Mapeamento Sistemático.

Estudos duplicados, ou seja, que já tiverem sido publicados em mais de uma conferência/jornal.
Pesquisas com ênfase em algoritmos de criptografia, com poucos detalhes sobre estratégias de segurança e sua aplicação.
Trabalhos que não abordem streaming nem multicasting.
Pesquisas que não tenham foco na segurança em questão.
Estudos que não estejam acessíveis na web.
Estudos que apliquem segurança para um formato específico de vídeo/ambiente.

4.1.1.8 Método de Extração dos Dados

A extração dos dados foi realizada como descrito abaixo:

- Uma busca manual por artigos foi realizada a fim de validar as palavras-chave que serão utilizadas para a pesquisa dos trabalhos. Com essa busca, dois artigos foram computados.
- A inclusão dos estudos foi efetuada por meio da leitura do título, do resumo/abstract, das palavras-chave validadas anteriormente e das

conclusões, tendo como foco identificar os critérios de inclusão estabelecidos. Após esta etapa foram incluídas 189 publicações.

- Na última etapa de refinamento, foram aplicados os critérios de exclusão. Assim, 27 estudos foram contabilizados.
- Os estudos incluídos como resultados da pesquisa foram revisados por outro pesquisador.
- Os resultados foram revisados por todos os pesquisadores envolvidos e quaisquer desacordos foram discutidos e resolvidos.

4.1.1.9 Método de Síntese dos Dados

Uma análise sobre os dados quantitativos dos estudos foi realizada. Os dados dos estudos selecionados foram comparados, com a finalidade de agrupar as similaridades e diferenças de acordo com as questões da pesquisa.

4.1.2 Apresentação, Análise e Discussão dos Resultados

Nesta seção são expostas as respostas para as questões do mapeamento mencionadas no planejamento do protocolo na seção 4.1.1.3.

4.1.2.1 Resultados obtidos para a Questão 1

Quando se refere à quantidade de publicações, a Figura 26 mostra que, nos anos de 2005 a 2008, houve um declínio na produção de artigos, mas que, apesar de uma pequena irregularidade, o interesse nessa área vem se demonstrando sempre superior desde 2010.

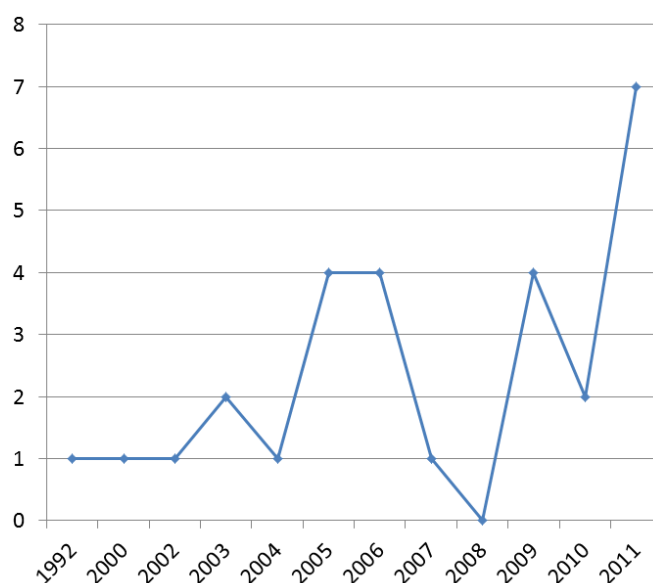


Figura 26. Distribuição anual das publicações do mapeamento sistemático

A tendência é continuar crescendo, visto que, o mercado necessita cada vez mais da segurança na transmissão de seus dados, principalmente na telemedicina, que se faz presente em um número cada vez maior na RUTE.

4.1.2.2 Resultados obtidos para a Questão 2

Após a leitura minuciosa dos artigos, verificou-se a utilização de sete tipos de criptografia, envolvendo diferentes estratégias de distribuição de chaves e em diferentes contextos. Observou-se que a criptografia simétrica prevalece, mas a criptografia assimétrica também é utilizada, tanto para criptografia do fluxo, quanto para troca de uma chave simétrica. Outro fator importante é a criptografia seletiva, que se mostrou eficiente e, mesmo não criptografando todo o fluxo, deixa-o incompreensível. A Figura 27 ilustra todos os resultados.

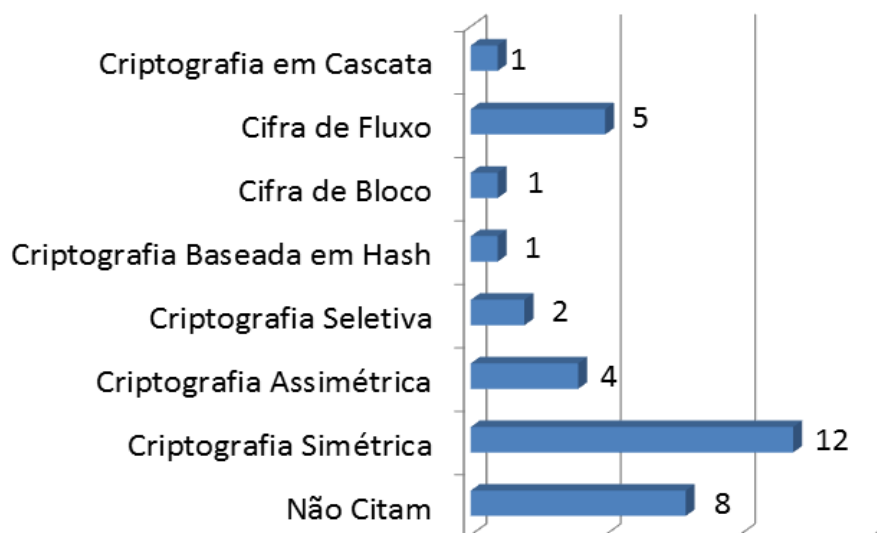


Figura 27. Tipos de criptografia utilizados pelos estudos do mapeamento

4.1.2.3 Resultados obtidos para a Questão 3

A taxonomia utilizada para classificar os trabalhos investigados pode ser dividida em duas categorias. Desta forma, dois aspectos são analisados: faceta de pesquisa, ou seja, o que a publicação pesquisou e a faceta de contribuição, que indica qual foi o resultado do trabalho (WIERINGA, 2006; PETERSEN, 2008). Cada uma dessas tem cinco *tags* e cada publicação foi categorizada em uma *tag* de cada faceta.

- Faceta de Pesquisa
 - Validação: As técnicas investigadas são novas e ainda não foram implementadas na prática. As técnicas usadas são para experimentos, ou seja, o trabalho realizado no laboratório.

- Avaliação: As técnicas são aplicadas na prática e uma avaliação da técnica é conduzida. Isto significa que ele é mostrado como a técnica é aplicada na prática (implementação) e quais são as consequências da implementação em termos de vantagens e desvantagens (avaliação de implementação). Isto também inclui a identificação problemas no setor.
- Proposta: Uma solução para um problema é proposto, podendo ser nova ou uma significativa extensão de uma técnica já existente. Os potenciais benefícios e a aplicabilidade da solução são indicados por um pequeno exemplo ou uma boa linha de argumentação.
- Artigo de Opinião: Estes documentos expressam a opinião pessoal de alguém, se uma determinada técnica é boa ou ruim, ou como deveriam ser realizadas.
- Artigo de Experiência: Explicam o que e como algo foi feito na prática. É dado como a experiência pessoal do autor.
- Faceta de Contribuição
 - Métrica: A medida de uma característica particular do desempenho de um programa ou eficiência. Uma métrica é usada às vezes direta e às vezes como um elemento em um algoritmo.
 - Ferramenta: Dispositivo, mecanismo físico ou intelectual utilizado para realizar alguma tarefa.
 - Modelo: Uma representação de um sistema que permite a investigação de suas propriedades e, em alguns casos, a previsão de resultados futuros. Modelos são frequentemente utilizados em análise quantitativa e análise técnica e, às vezes, também na análise fundamental.
 - Método: Um conjunto de regras básicas de como se deve proceder a fim de produzir conhecimento, quer seja este um novo conhecimento quer seja este fruto de uma integração, correção (evolução) ou uma expansão da área de abrangência de conhecimentos pré-existentes.
 - Processo: Sequência de procedimentos interdependentes e vinculado que, em cada etapa, consomem um ou mais recursos (tempo empregado) para converter as entradas (dados) em saídas. Estas saídas, então, servem como insumos para a próxima fase até uma meta conhecida ou até o resultado final ser alcançado.

O resultado dessa classificação pode ser vista na Figura 28, onde é possível destacar a falta de Artigos de Opinião e Artigos de Experiência e o grande número de Propostas de Solução. Também há poucas Validações e Avaliações e nenhum trabalho abordando uma Ferramenta. Esses dados deixam claras várias lacunas que podem ser exploradas.

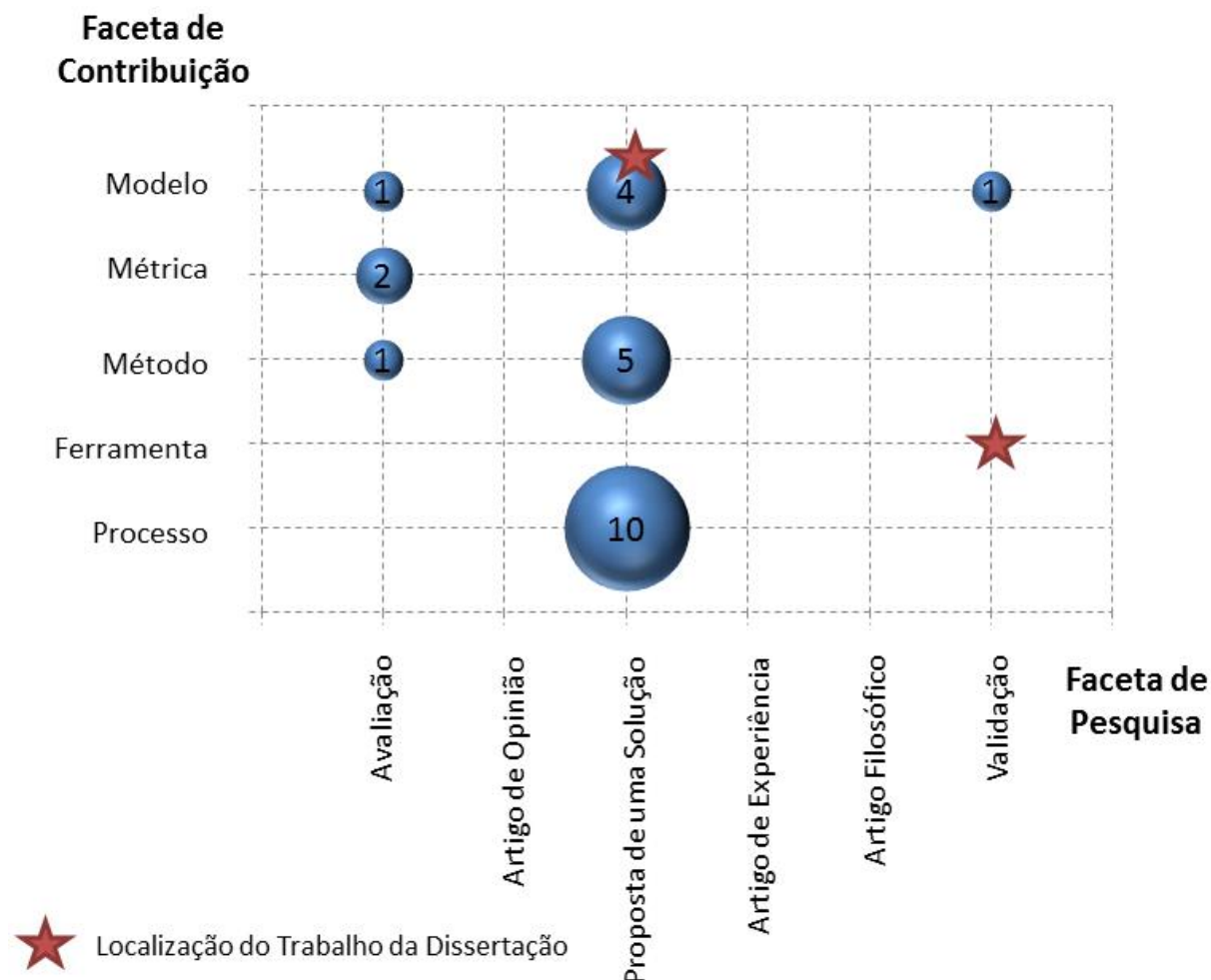


Figura 28. Gráfico de bolhas do mapeamento sistemático

4.1.2.4 Resultados obtidos para a Questão 4

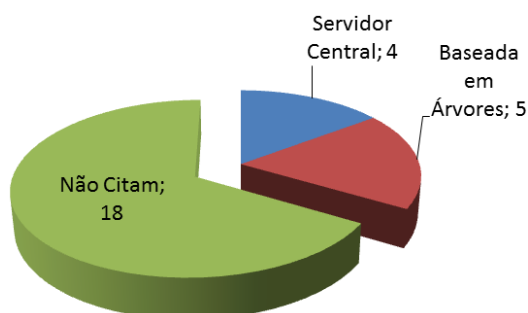


Figura 29. Estratégias de distribuição de chave utilizadas pelos trabalhos do mapeamento

A Figura 29 mostra que a estratégia de distribuição de chave predominante é a baseada em árvores. Uma abordagem árvore-chave é utilizada por Dondeti (2000) com hierarquia de subgrupos de membros do grupo *multicast* para garantir escalabilidade. Cada subgrupo é gerenciado pelo gerente de subgrupo (SGM) que auxilia na distribuição de chaves, bem como no controle de acesso ao grupo. Já algumas estratégias, como a de Holeman (2002), aderem a ter uma entidade central responsável por criar e gerenciar a distribuição de chaves entre os membros de um grupo.

Um ponto de destaque é que muitos autores não citam uma estratégia de distribuição de chaves e seu foco acaba sendo na descrição do modelo de criptografia e proteção dos dados transmitidos.

4.1.2.5 Resultados obtidos para a Questão 5

Como pode ser observado na Figura 30, dos algoritmos de criptografia conhecidos, há a predominância do AES nos estudos analisados. Porém, na maioria dos trabalhos, o autor utiliza um algoritmo de criptografia próprio baseado em algum algoritmo clássico ou em alguma estratégia, como a *Chaos Theory* utilizada por Fan (2011) e Pande (2011).

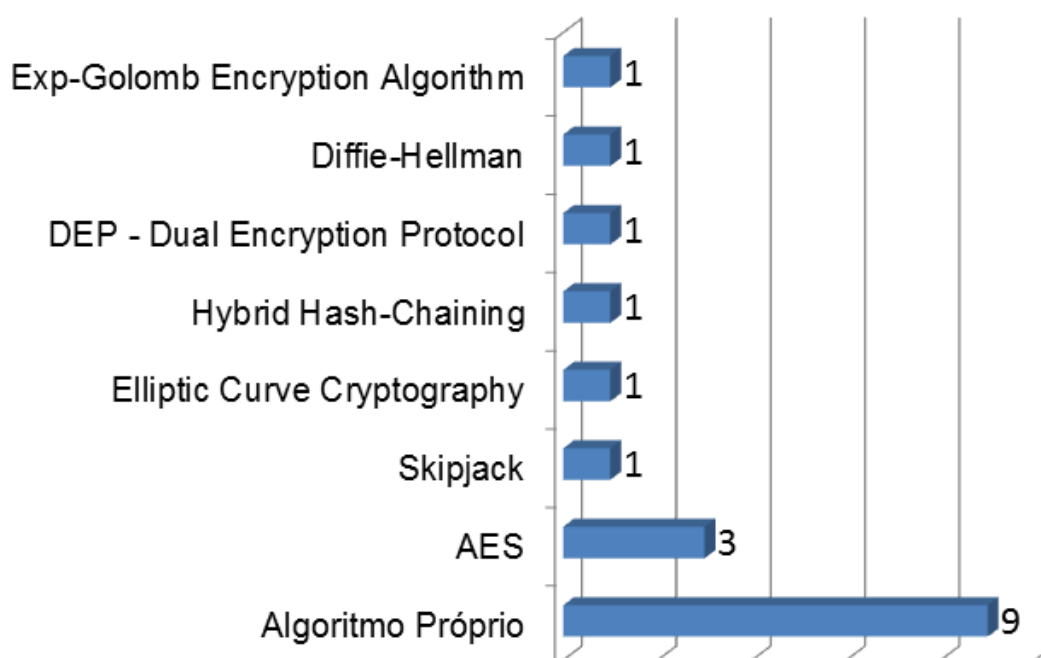


Figura 30. Algoritmos de criptografia utilizados pelos estudos do mapeamento sistemático

4.2 Trabalhos Relacionados

Nesta seção são descritos alguns trabalhos relacionados com a estratégia que possam ter alguma contribuição significativa. Os trabalhos foram selecionados após uma leitura completa e análise das publicações dadas como relevantes no mapeamento sistemático, descrito na seção 4.1. Foram selecionados utilizando um critério heurístico com o objetivo de investigar as melhores técnicas, atuais ou clássicas, que expusessem métodos de criptografia para fluxos de mídia eficientes e de distribuição de chaves de forma segura entre o remetente e o destinatário.

Os trabalhos expostos nesse capítulo tiveram seus pontos fortes e pontos fracos relacionados com o tema desse trabalho destacados, de forma a deixar claras as técnicas e conceitos que possam ser ou não ser utilizados, além de ser feita uma comparação destes pontos chave com o objetivo de extrair as melhores práticas que possam ser empregadas na estratégia.

4.2.1 A Novel Scheme for HD Video Stream Encryption (FAN, 2011)

Fan (2011) propõe uma estratégia para criptografia de fluxos de mídia em alta definição e afirma que a criptografia de todo o vídeo é seguro, mas tem baixa eficiência. A ideia é criptografar apenas frames importantes, denominados I-Frames, e isso garante a confidencialidade da mídia por completo, fazendo assim uma criptografia seletiva. Para a identificação dos I-frames é introduzido um padrão de reconhecimento baseado no sistema do caos e visa reduzir a quantidade ao menor número possível mantendo ilegibilidade do vídeo criptografado.

O esquema é feito através de algoritmos e estratégias de encriptação em várias camadas e a aplicação consiste de um sistema de encriptação de vídeo em alta resolução composto por um Servidor de Criptografia de Fluxo e um Decriptografador/Reprodutor de Fluxo. O servidor, núcleo do esquema, funciona como explanado a seguir: o Módulo Demultiplexador de Alta Definição, encarregado de separar o vídeo do áudio, repassa as informações visuais para o Módulo Criptografador, o qual usa os modelos de caos *Logisticmap* e *Chebyshev* implementados em quatro níveis, além de contar com uma autenticação do usuário, que, repassada às camadas, pode gerar quatro sub-chaves passadas para o sistema de caos (FAN, 2011).

O Módulo de Envio de Streaming de Alta Definição implementa os protocolos de transmissão de fluxos padrão, tais como RTSP, RTP, RTCP, SIP; além de tratar eventos do usuário como pausar, *resume*, avanço rápido, retroceder rápido, *drag*. Analogamente, o Decriptografador/Reprodutor de Fluxo usa três módulos: Demultiplexador, Decriptografador, e Decodificador, fazendo os processos inversos à rotina do servidor (FAN, 2011).

A Figura 31 ilustra a sequência do algoritmo de encriptação onde o fluxo em alta definição é recebido e cada frame é analisado se está de acordo com o padrão inserido previamente. Apenas os I-Frames são encriptados e o processo só acaba quando não há mais I-Frames (FAN, 2011).

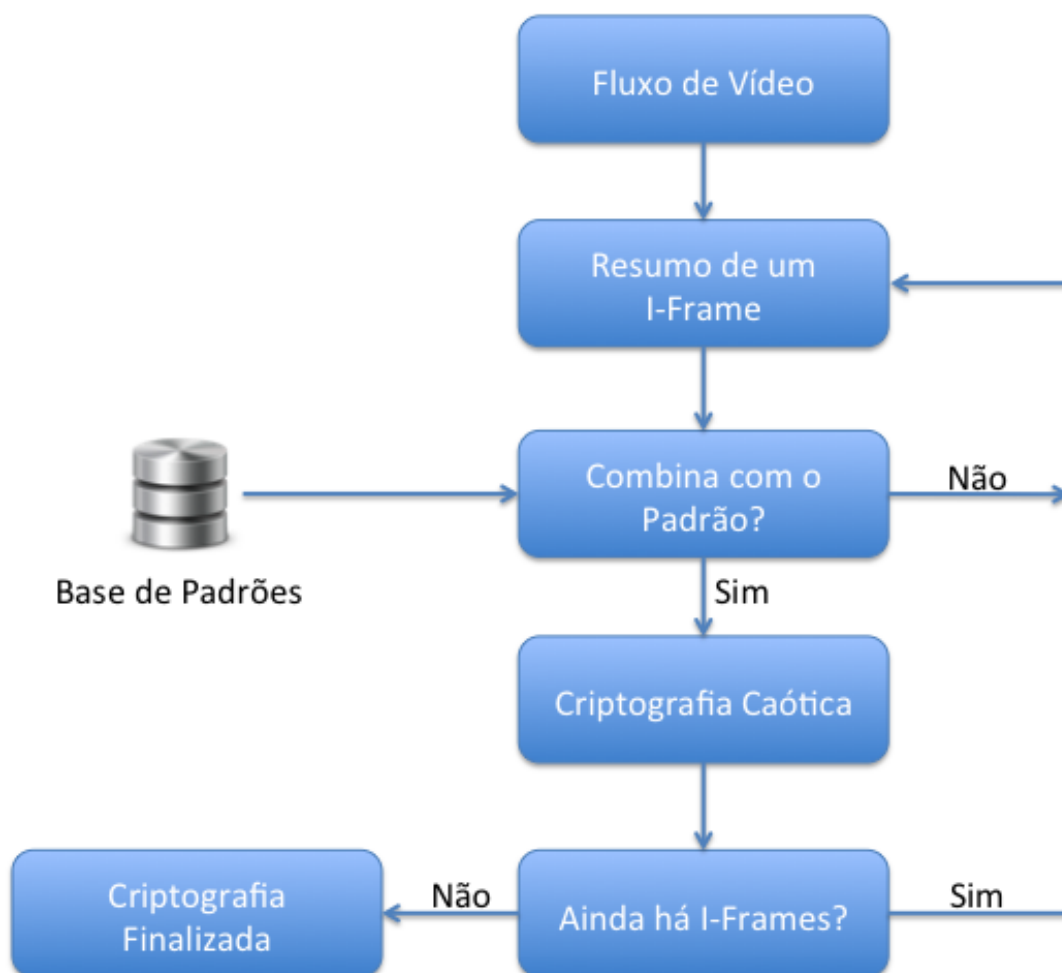


Figura 31. Sequência do algoritmo de encriptação do fluxo. Adaptado de Fan (2011)

O resultado da estratégia de Fan (2011) pode ser visualizado na Figura 32.



Fluxo Original



Fluxo Criptografado

Figura 32. Resultado da estratégia de Fan (2011). Adaptado de Fan (2011)

4.2.2 Secure Decentralized Group Key Management through Progressive Approach (SANDOSH, 2010)

Sandosh (2010) propõe uma estratégia para segurança em *multicast* baseada em grupo de usuários onde há uma chave para o grupo que tem seu gerenciamento de forma descentralizada. O autor afirma que a principal vantagem de sua estratégia é ter uma autenticação periódica dos membros do grupo.

O gerenciamento do grupo é feito pelo *Group Server* (GS) e cada usuário que deseja ingressar no grupo precisa autenticar-se nele. Após a autenticação, o usuário recebe duas chaves, a chave do grupo (*Group Key* – GK), para criptografia e decifração do conteúdo transmitido no grupo e uma chave individual, para comunicação com o GS. Quando um membro entra ou sai do grupo uma nova GK é gerada e distribuída entre os membros (SANDOSH, 2010).

Para evitar o acesso de intrusos aos dados do grupo, Sandosh (2010) propõe que os usuários tenham uma autenticação periódica e isso é feito em uma estratégia baseada em *hash*. O GS envia periodicamente um texto aleatório para cada membro utilizando a chave individual que tem com cada um. O membro deve calcular o *hash* desse texto e enviar de volta para o GS também utilizando a chave individual. O GS faz a comparação se o *hash* está correto e averigua se é um membro autenticado. Caso o membro não esteja autorizado, o GS encerra a comunicação com ele. A Figura 33 ilustra esse processo.

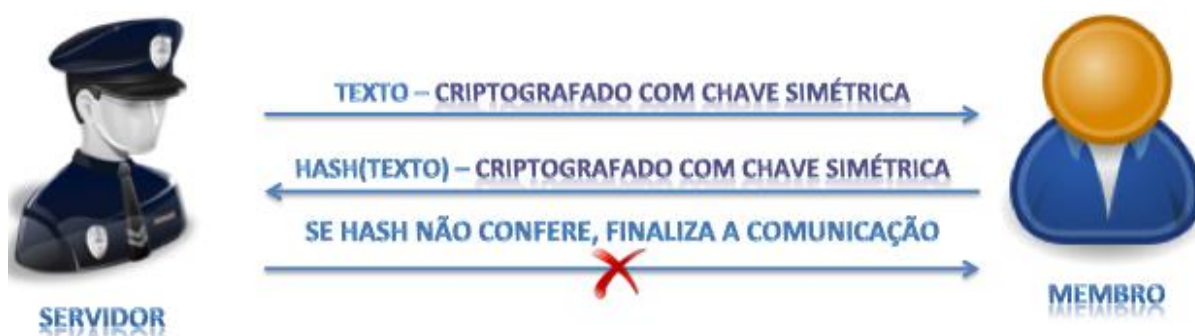


Figura 33. Processo de verificação de membros autorizados de Sandosh (2010)

4.2.3 A Secure Media Streaming Mechanism Combining Encryption, Authentication and Transcoding (MOU, 2009)

Dados transmitidos por diversos canais da rede podem ser alvo de ataques, como por exemplo, por *Eavesdropping*, técnica que consiste em uma leitura não autorizada dos pacotes (DONDETI, 2000). Desta forma, Mou (2009) destaca dois aspectos de grande importância: a confidencialidade dos dados transmitidos e a sua autenticidade. A confidencialidade é bem feita quando o conteúdo da mídia é criptografado e mantido em texto cifrado durante a sua distribuição. Assim, apenas usuários autorizados podem ter acesso aos dados protegidos. Autenticidade diz respeito ao conteúdo de mídia ser confiável em termos de sua integridade e remetente alegado.

Diversas questões a respeito de criptografia unida ao protocolo de comunicação RTP (RTP, 2012) para prover segurança e autenticidade na transmissão de fluxos entre origem e destino são tratadas. Neste trabalho, é citado o algoritmo *Elliptic Curve Cryptography* (HANKERSON, 2004) que utiliza os conceitos de chave pública e privada e é tão seguro quanto o RSA (RSA, 2012) de 1024 bits, porém tem inferior custo computacional. Em um componente denominado *Seed*, os

pacotes RTP são modificados inserindo-se dois campos: um *stream id* (4 bytes) que é a identificação do fluxo e é um valor único, e uma assinatura digital (48 bytes) baseada na chave privada do originador, como pode ser observado na Figura 34. Essa inserção é feita até mil vezes por segundo sob as condições informadas (MOU, 2009).



Figura 34. Estrutura dos pacotes RTP modificados. Adaptado de Mou (2009)

Todo o fluxo é intermediado por um componente chamado *Multimedia Application Routing Server* (MARS) que é um *Mid Network Proxy* (MOU, 2009) inteligente. Este componente faz a análise do fluxo e verifica a autenticidade de cada pacote RTP recebido, verificando a assinatura digital que foi incluída em cada pacote. É nele que também é analisado o id de cada pacote RTP para verificar a qual *stream* ele pertence. Os pacotes que tiverem assinatura ou id inválido são descartados e apenas os válidos são encaminhados ao destino. Essa verificação ocorre até cinquenta vezes por segundo sob as condições informadas, alcançando um limite de bitrate de 400 Kbps ($50 * 8 \text{ Kb}$) (MOU, 2009). Um esquema geral pode ser visto na Figura 35.



Figura 35. Esquema geral do Modelo descrito por Mou (2009)

A criptografia é seletiva, ou seja, apenas uma parte do fluxo é criptografada. São criptografadas apenas as informações inerentes à informação do fluxo em si, ou

seja, os quadros do vídeo. Os metadados (informações de bitrate, codificação etc.) não são criptografados. Baseada na não encriptação dos metadados, os MARS fazem a adaptação do fluxo permitindo que seja dividido em vários fluxos de taxas diferentes e sejam enviados a diversos destinos. Essa adaptação se dá alterando as meta informações e eliminando quadros para que se adeque à nova taxa (MOU, 2009).

4.2.4 H2A: Hybrid Hash-chaining scheme for Adaptive multicast source authentication of media-streaming (CHALLAL, 2005)

Uma adaptação do *Hash Chaining* (ROSARIO, 1997, 2001) é feita por Challal (2005). Na abordagem original, um pacote era assinado pelo pacote enviado anteriormente, ou seja, o primeiro pacote assina o próximo e assim por diante. Um problema existente nessa abordagem é que, na perda de algum pacote, todos os pacotes seguintes não poderão ter suas assinaturas verificadas e, conseqüentemente, serão descartados. A mudança na abordagem tenta amenizar essas perdas criando grupos de pacotes que tem uma assinatura dependente um do outro. Se um pacote se perder, apenas os pacotes até o próximo grupo serão perdidos.

O tamanho do grupo de pacotes é definido baseado em respostas dadas pelo destino, uma espécie de *acknowledgement* (ACK) do TCP, chamado de pacote QoR. Caso estejam ocorrendo poucas perdas, os grupos vão ficando maiores, caso contrário, os grupos vão ficando menores (CHALLAL, 2005). O esquema pode ser visto na Figura 36.

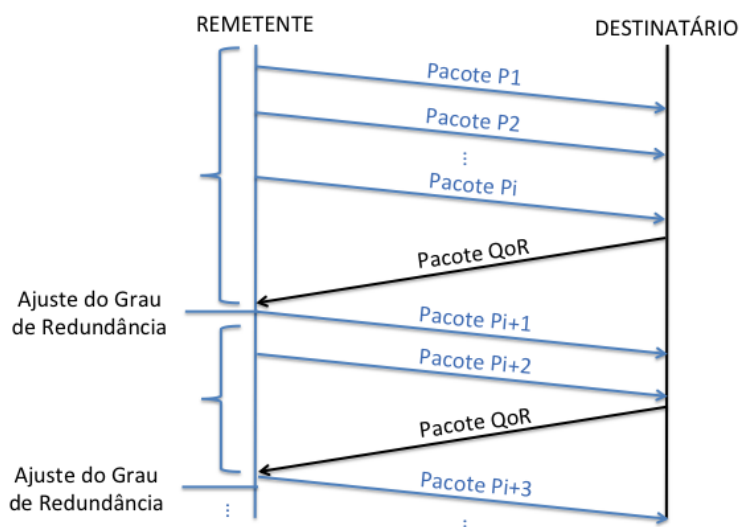


Figura 36. Esquema do envio de pacotes e QoRs. Adaptado de Challal (2005)

4.2.5 Differentially secure multicasting and its implementation methods (HOLEMAN, 2002)

Uma das contribuições de Holeman (2002) é a definição dos três tipos de transmissões em grupo: *multicast*, *broadcast* e *multiple unicast*. Essas definições foram descritas na seção 2.2.

No artigo, seu modelo é descrito baseado no modelo de Bell-Lapadula (BELL, 1976). Empregam em sua estratégia os conceitos de Controle de Acesso Compulsório (MAC) e utiliza os níveis do modelo de Bell-Lapadula para descrever o que será criptografado, além de verificar quem pode ter o acesso a determinadas informações. O nível 0 (não classificado) contém as informações que todos tem acesso, ou seja, são públicas e não precisam receber qualquer tipo de segurança (criptografia). Um conceito importante tratado é o de grupos, onde há uma chave para a comunicação entre seus membros, a qual precisa ser trocada sempre que um usuário entra ou sai (Holeman, 2002).

4.2.6 Efficient security mechanisms for overlay multicast based content delivery (ZHU, 2007)

O conceito de grupo para a comunicação entre os usuários também é utilizado por Zhu (2007), que descreve dois tipos de chaves, sendo uma para a criptografia da comunicação do grupo (*Data Encryption Key - DEK*) e outra para distribuir a chave de comunicação entre os participantes (*Key Encryption Key - KEK*). No artigo, ele descreve três entidades que são servidoras, cada uma com uma função:

- *Key Server*: provê inscrição de serviços por usuários;
- *Data Server*: é encarregado de criptografia e assinaturas sobre os dados transmitidos;
- *Distribution Server*: é responsável por distribuir o conteúdo.

A Figura 37 ilustra o esquema da interação dos usuários com os servidores.

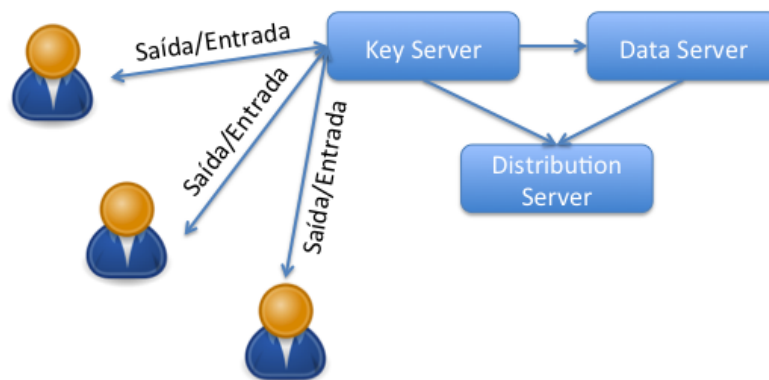


Figura 37. Interação de Usuários e Servidores. Adaptado de Zhu (2007)

O modelo de Zhu (2007) é denominado “A *certificate revocation based group rekeying scheme*” (CRBR) que prevê as seguintes ações:

- Registro do nó: gera um certificado de chave pública sempre que um membro entra no grupo;
- *Security Update Generation*: O Key Server gera um novo *certificate revocation list* (CRL) e uma nova DEK para todo grupo que fizer regeneração de chave;
- *Security Update Distribution*: Cada nó pode verificar a autenticidade da chave de grupo a partir da verificação de assinatura, depois de feita a distribuição da nova chave.

Os certificados que permitem a verificação de autenticidade dos integrantes tem prazo de expiração e precisam ser renovados quando isso acontece. Quem distribui a chave do grupo para um novo usuário são os próprios usuários (ZHU, 2007).

4.2.7 Quasi-commutative watermarking and encryption for secure media content distribution (LIAN, 2009)

Lian (2009) propõe uma maneira de enviar vídeos criptografados com assinaturas para cada destino. Essa estratégia tem resultados similares aos da criptografia seletiva (FAN, 2011; MOU, 2009; LIAN, 2006).

Criptografia em multimídia transforma dados multimídia em formas ininteligíveis sob o controle de uma chave, que protege a confidencialidade do conteúdo multimídia e apenas o cliente autorizado que tem a chave certa pode recuperar dados de multimídia corretamente. Comparada com a criptografia de texto, a criptografia de vídeo tem requisitos especiais (LIAN, 2006), tais como a segurança de percepção e eficiência (LIAN, 2009).

Em primeiro lugar, a segurança da criptografia de vídeo inclui dois aspectos, a segurança criptográfica e a segurança de percepção. Entre elas, a segurança criptográfica denota a segurança contra ataques criptográficos, enquanto a segurança de percepção refere-se a inteligibilidade do conteúdo do vídeo criptografado. Em segundo lugar, o algoritmo de criptografia de vídeo deve ser de tempo eficiente, com o objetivo de atender às aplicações em tempo real. Isso ocorre porque o vídeo tem, muitas vezes, um grande volume de dados que não podem sofrer atrasos significativos (LIAN, 2009).

O ponto chave do trabalho de Lian (2009) é assinar cada vídeo para o seu destinatário, com a possibilidade de verificação dessa assinatura. Diferente de métodos tradicionais que assinam o vídeo antes da criptografia (Figura 38), a proposta é ter primeiro a criptografia e depois a assinatura (Figura 39).

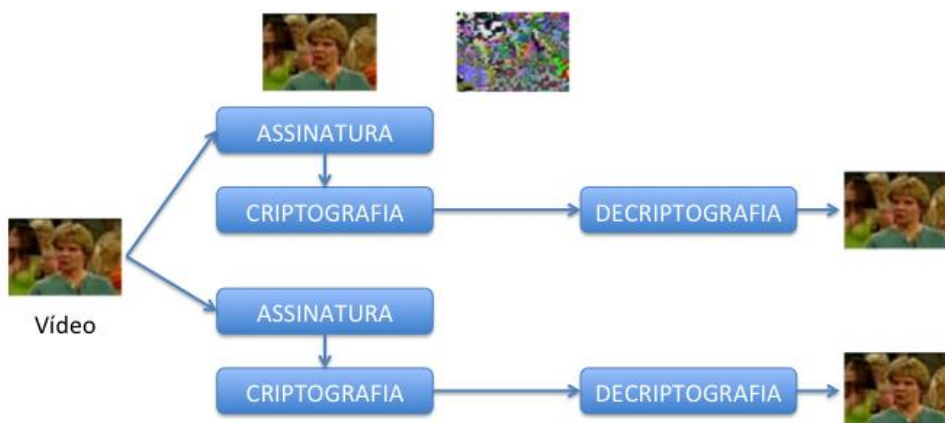


Figura 38. Criptografia e assinatura de vídeos utilizando método tradicional. Adaptado de Lian (2009)

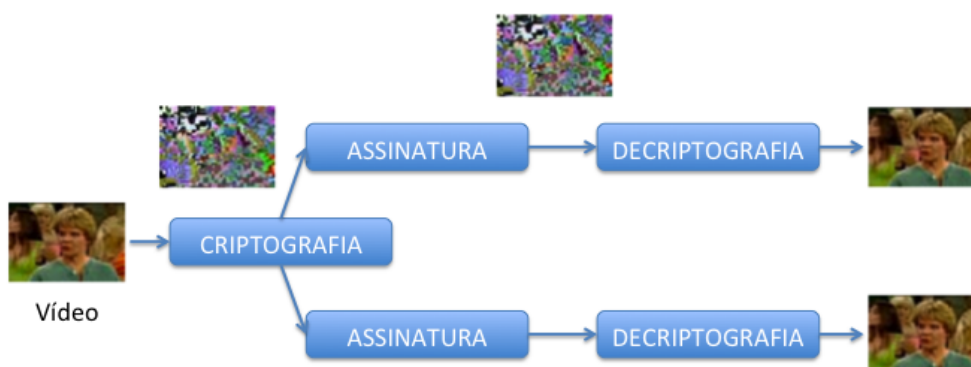


Figura 39. Criptografia e assinatura de vídeos utilizando método proposto por Lian (2009). Adaptado de Lian (2009)

4.2.8 A Secure Scheme for Video Streaming Using SRTP AES and DH (ASGHAR, 2010)

Asghar (2010) propõe 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 e 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 40 ilustra esse processo.



Figura 40. Esquema de segurança de transmissão segura de conteúdo multimídia. Adaptado de Asghar (2010)

4.2.9 Secure Advanced Video Coding Based on Selective Encryption Algorithms (LIAN, 2006)

A Codificação de Vídeo Avançada (*Advanced Video Coding – AVC*) é amplamente utilizada, mas nem sempre a segurança é levada em consideração. Para solucionar

esse problema, Lian (2006) propõe uma estratégia de codificação e criptografia seletiva para transmissão de vídeo. O autor cita que vários algoritmos são propostos para serem utilizados, tais como o DES, RSA e AES, mas são ineficientes para aplicações em tempo real. Para ter uma maior eficiência, é necessário fazer uma criptografia seletiva e parâmetros de sensibilidade da percepção do vídeo criptografado que definem o quão legível ele estará. A dificuldade se emprega na seleção dos dados corretos e no ajuste desses parâmetros (LIAN, 2006).

A codificação utilizada por Lian (2006) é a MPEG1/2 e um algoritmo próprio é proposto para a criptografia seletiva dos vídeos e faz uma comparação de seu método com o método proposto por Ahn (2004). Os resultados dessa comparação podem ser visualizados na Figura 41, onde:

- (a), (b), (c) – vídeos originais;
- ©, (d), (e) – resultados de Ahn (2004);
- (e), (f), (g) – resultados de Lian (2006).

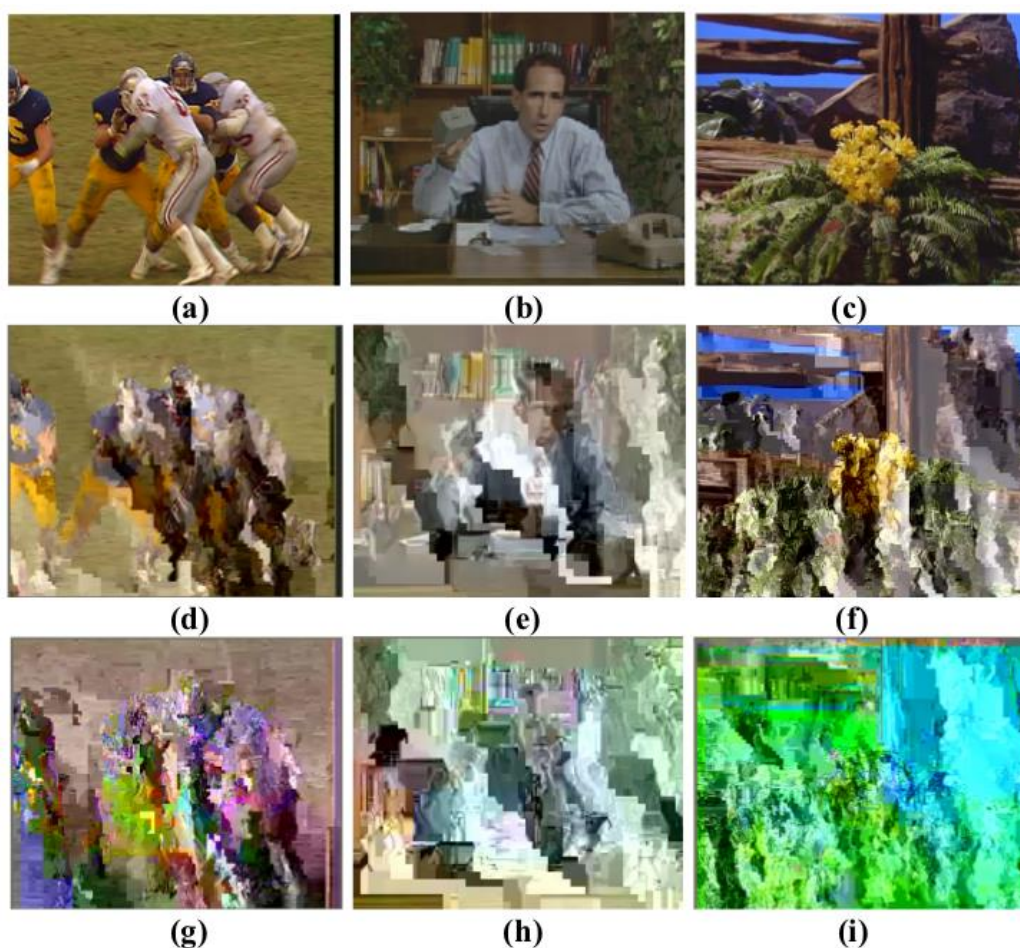


Figura 41. Resultados. (LIAN, 2006)

4.3 Análise Comparativa

No intuito de comparar os trabalhos correlatos foi utilizado o resultado do mapeamento sistemático que resultou nos trabalhos elencados na Tabela 4. Nessa tabela os trabalhos são comparados quanto ao tipo de criptografia, distribuição de chaves e algoritmo de criptografia. Uma característica observável é que a criptografia simétrica e o uso do AES são predominantes.

Tabela 4. Comparação dos trabalhos do mapeamento sistemático

Trabalho	Tipo de Criptografia	Distribuição de Chaves	Algoritmo de Criptografia
Fan (2011)	Simétrica, Seletiva	Não cita	Próprio
Sadosh (2010)	Simétrica	Servidor Central	Skipjack
Mou (2009)	Assimétrica	Não cita	Elliptic Curve Cryptography, AES
Challal (2005)	Baseada em Hash	Não cita	Hybrid Hash-Chaining
Zhu (2007)	Simétrica	Servidor Central	AES
Lian (2006)	Simétrica	Não cita	Próprio

O trabalho descrito por Mou (2009) cria uma arquitetura eficiente para criptografar o fluxo e verificar a autenticidade, inserindo uma assinatura digital em cada pacote do RTP. Contudo, essa verificação é lenta, o que limita sua utilização a vídeos com baixa definição. Também descreve a criptografia seletiva, que permite a adaptação do mesmo fluxo em diferentes contextos, mas essa adaptação se dá apenas na alteração de seu bitrate, o que não é, de fato, uma adaptação completa.

A estratégia de Challal (2005) pode acarretar o descarte de pacotes devidamente autenticados, caso um pacote se perca no caminho entre a origem e o destino, e o restabelecimento normal do recebimento dos dados só será feito quando o grupo de pacotes acabar e o próximo grupo for enviado. Isto inviabiliza sua utilização em transmissões de tempo real, onde a transmissão seria interrompida temporariamente durante esse processo.

Holeman (2002) explicitou claramente o seu escopo e definiu as diferentes maneiras de fazer distribuição de fluxo: *Multiple Unicast*, *Broadcast* e *Multicast* e,

assim como Zhu (2007), descreve o conceito de grupo de forma que deve haver uma chave para comunicação segura entre os usuários e que essa chave deve ser regenerada sempre que um usuário sai ou entra do grupo. O trabalho define permissões dos usuários e também que nem todo o conteúdo precisa ser criptografado, ou seja, o conteúdo recebe uma classificação.

Zhu (2007) agrega o conceito de existir uma chave para o grupo (DEK) e outra chave para a distribuição da chave do grupo entre os usuários (KEK), da mesma maneira que Sandosh (2010). Sempre que um usuário entrar ou sair, a nova DEK é gerada e distribuída utilizando a KEK. Esta abordagem se torna frágil pelo fato de os usuários que já deixaram o grupo poderem capturar a informação de redistribuição de uma nova DEK e obter a informação decriptografando com a KEK, que nunca muda. No trabalho são bem definidas as entidades e suas responsabilidades, além de ações que acontecem no decorrer do grupo e como elas devem se comportar.

Mou (2009), Zhu (2007) e Asghar (2010) utilizam o AES para a criptografia dos dados transmitidos entre a origem e o destino, enquanto que os outros não citam qual o melhor algoritmo se aplica. Outro ponto a ser destacado no trabalho de Mou (2009) é a descrição do *Elliptic Curve Cryptography* que é tão seguro quanto RSA de 1024 bits e tem custo computacional menor.

Foi possível observar que, diferente dos outros, os trabalhos de Fan (2011) e Lian (2006) aplicaram-se no contexto de transmissão de vídeos em alta definição e esse dado pode indicar uma lacuna pouco explorada. Lian (2006) também teve a preocupação com a transmissão em tempo real e muitas dessas estratégias não podem ser aplicadas nesse contexto, como é o caso de Challal (2005) que esses dados podem ter uma grande quantidade de perdas.

A criptografia seletiva foi um tema bastante abordado nos trabalhos de Fan (2011), Mou (2009), Lian (2009) e Lian (2006) e é uma técnica que pode ser muito útil para um grande volume de dados, como é a transmissão de vídeo em alta definição.

Praticamente todos os trabalhos abordam os conceitos de grupo com chave compartilhada entre os membros, mas Sandosh (2010) foi o único que se preocupou em fazer autenticação periódica dos usuários de um grupo e faz isso através de uma

técnica com *hash*. Esse trabalho não aborda autenticação periódica e isso está como planos para os trabalhos futuros.

CAPÍTULO 5: REFLETORES PARA CRIPTOGRAFIA MULTIMÍDIA E SERVIDOR VSECURITYSERVER

Para atender as necessidades expostas ao longo dos objetivos aliados aos conceitos discutidos na fundamentação teórica, este trabalho foi dividido em duas partes com intuito de suprir os problemas levantados com uma solução adequada para cada contexto.

A primeira parte deste capítulo descreve um conjunto de refletores capazes de fazer transcodificações e criptografia para transmissões de fluxos multimídia em tempo real utilizando o protocolo UDP e o algoritmo de criptografia AES. Esses refletores são agregados de forma a compor um único refletor capaz de atender essas necessidades.

Como a transmissão com o refletor utiliza a criptografia simétrica, é necessário que uma chave de criptografia seja compartilhada entre a origem e o destino. Além do que, há a possibilidade de ter mais de uma origem e mais de um destino em uma transmissão, o que caracteriza um grupo com seus respectivos membros e uma chave de criptografia simétrica precisa ser designada para o grupo e distribuída entre esses. Diante dessas necessidades, alguns pontos precisam ser considerados: autenticação dos membros, um gerenciamento dos grupos e distribuição da chave entre os membros autorizados. Para supri-la, foi criado o VSecurityServer, um servidor que é descrito na segunda parte do capítulo.

5.1 Refletores para Codificação e Criptografia em Tempo Real

Nesta seção, é descrito um conjunto de refletores que tem por objetivo atender às necessidades do envio de fluxos multimídia com múltiplas codificações e criptografia. São apresentados os modelos conceitual, arquitetural e tecnológico e cada refletor foi criado para suprir uma necessidade e solucionar um problema específico e, sua composição, permite a transmissão segura de fluxos multimídia em tempo real utilizando a criptografia simétrica com o algoritmo AES.

5.1.1 Modelo Conceitual

Para uma transmissão de fluxo, foi concebido o esquema geral ilustrado na Figura 2, com os passos que vão desde a captura no remetente até a exibição no destinatário. Para a transmissão segura do fluxo, dois passos são inseridos: criptografia, no

remetente; decryptografia, no destinatário. Esse esquema pode ser visualizado na Figura 42.



Figura 42. Framework geral para transmissão segura de fluxo (VIEIRA, 2011)

Para promover adaptabilidade em termos de uso dos refletores associados a diferentes combinações de codificadores, é proposto um refletor híbrido para criptografia e codificação. Este refletor tem por objetivo atender às necessidades de enviar fluxos para diversos destinos com diferentes codificações e com a aplicação de criptografia. Para tanto, o refletor precisa ser capaz de aplicar transcodações e refletir esses novos fluxos para seus respectivos destinos.

A Figura 43 ilustra a visão esquemática do funcionamento do refletor híbrido de criptografia e codificação, onde é possível observar os diferentes cenários possíveis, onde, em (a), observa-se quando um fluxo não criptografado é recebido e o refletor deve gerar fluxos criptografados e não criptografados em diferentes codificações e, em (b), observa-se quando um fluxo criptografado é recebido e a saída gerada deverá contemplar fluxos criptografados e não criptografados em diferentes codificações.

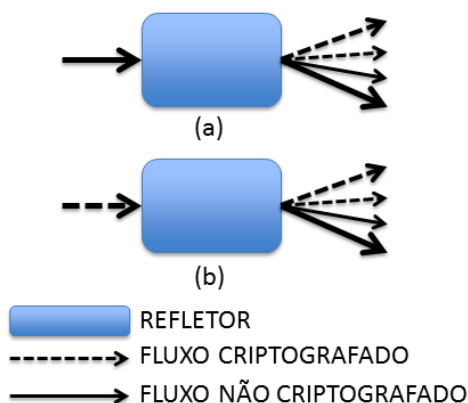


Figura 43. Visão Geral do Refletor Híbrido de Criptografia e Codificação. A largura da seta indica a qualidade da definição do fluxo

Para gerenciar as combinações possíveis de uso do refletor híbrido, é necessário saber qual o tipo de fluxo sendo recebido (criptografado ou não) para avaliar a necessidade de sua decryptografia. Um fluxo não criptografado precisa ser enviado para cada *transcoder* responsável por aplicar as transcodificações desejadas, esses *transcoders* enviam esse novo fluxo para a criptografia e, enfim, para seu destino final.

Um detalhamento desse cenário pode ser visto na Figura 44, que descreve a sequência de passos necessária para a múltipla codificação e criptografia no cenário em que um fluxo é recebido criptografado e gera saídas com múltiplas codificações também criptografadas.

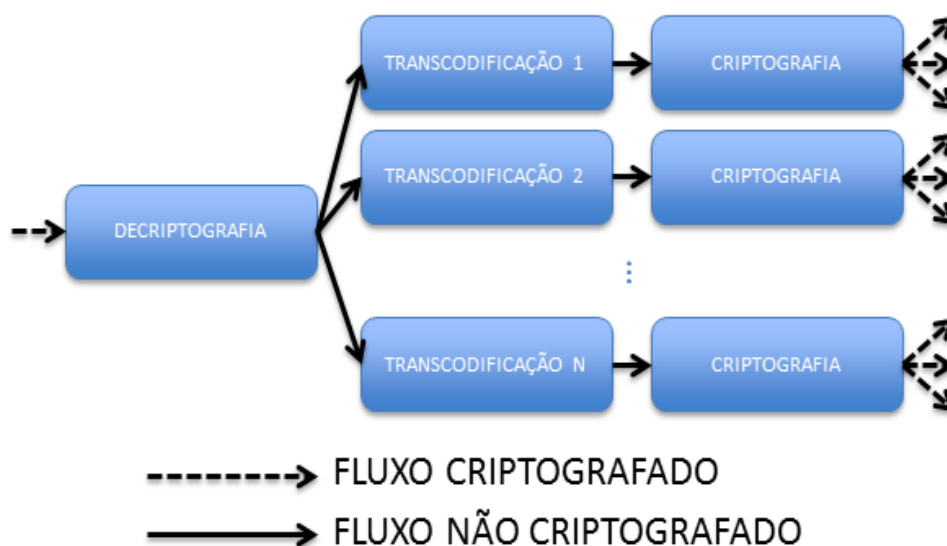


Figura 44. Sequência de passos necessária para a múltipla codificação e criptografia

Alguns desses passos podem não ser necessários em determinados casos, como, por exemplo: o fluxo recebido de forma não criptografada e isso descarta o uso de decryptografia; o fluxo não precisa ser enviado criptografado o que descarta o uso de criptografia; o fluxo precisa ser enviado da mesma forma que foi recebido o que descarta o uso tanto de decryptografia quanto da criptografia. Em ambos os casos pode ser necessária ou não o uso de transcodificação.

5.1.2 Modelo Arquitetural e Tecnológico

Para a transmissão multiponto em tempo real de fluxos de mídia com múltiplas codificações e criptografia, foi desenvolvido um conjunto de refletores capazes de desempenhar funções específicas que, em seu conjunto, permitisse adaptabilidade de formatos (codificação) e de criptografia. Para o desenvolvimento,

foi utilizado o Stylo (SILVA, 2011). O Stylo é um framework para otimizar o desenvolvimento de aplicações multimídia.

Dessa forma, são apresentadas cinco especializações de refletores, são elas: *ReflectorJ*, *AESReflectorC*, *AESReflectorJ*, *AESHybridReflectorJ* e *FullAESHybridReflectorJ*. Todas essas especializações partem do princípio de que um fluxo de dados deve entrar e ser redistribuído, criptografado ou não, dependendo do que for requisitado pelo destino. Eles todos também apresentam um esquema baseado em criptografia AES, variando sua esquematização de redistribuição interna e em que parte do sistema o módulo AES é chamado. A maioria dos refletores foi construída em Java visando a sua inserção na arquitetura da Arthron.

5.1.2.1 ReflectorJ

O *ReflectorJ* tem por função receber um fluxo de mídia encapsulado com *Transport Stream* (TS) (TS, 2012) e redistribuí-lo para diversos destinos. Sua descrição foi definida na interface *ReflectorIF* e o esquema desse refletor pode ser visualizado na Figura 5. A tecnologia utilizada para implementação deste refletor é Java (JAVA, 2012).

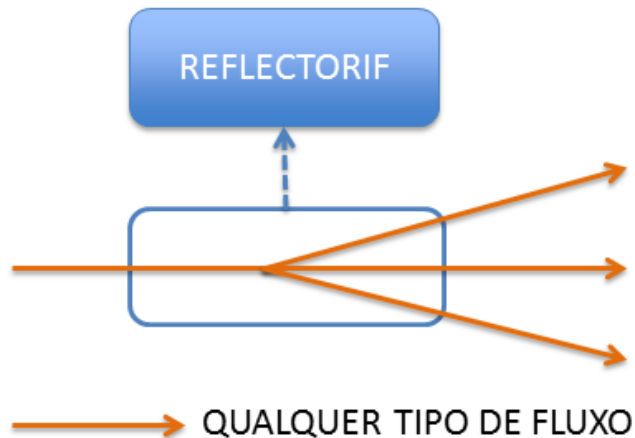


Figura 45. Esquema do ReflectorJ

5.1.2.2 AESReflectorC

Como um dos objetivos é ter a possibilidade da utilização de fluxos de mídia FULL HD, o refletor estará lidando com um grande volume de dados e um bom desempenho faz-se necessário. Para otimizar esse processo, um dos pontos mais críticos foi desenvolvido em C da criptografia.

Para tanto foi criado o refletor *AESReflectorC*, com a finalidade de receber um fluxo para criptografá-lo ou decriptografá-lo. A Figura 46 ilustra o recebimento de um

fluxo não criptografado, onde os pacotes TS são enviados para a criptografia utilizando o algoritmo AES e uma chave. Os pacotes são então enviados a um destino de forma criptografada.

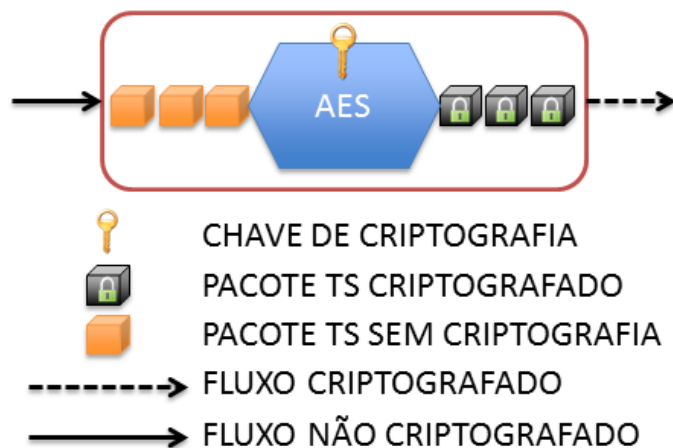


Figura 46. Esquema de Criptografia do AESReflectorC

A Figura 47 ilustra o recebimento de pacotes criptografados e sendo enviados para a decryptografia utilizando o algoritmo AES e uma chave. Os pacotes não criptografados são enviados a um destino.

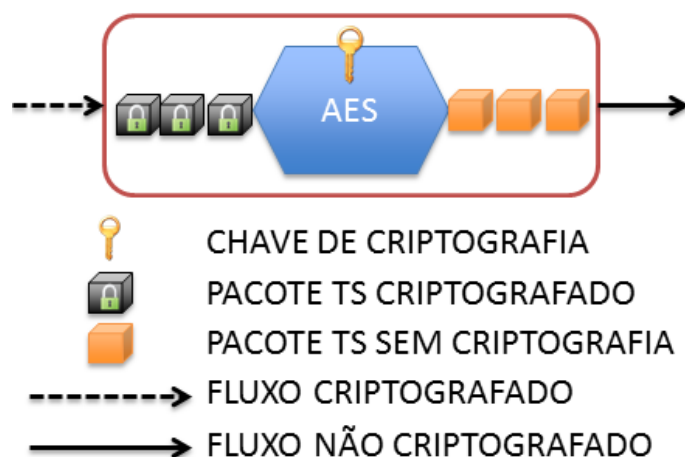


Figura 47. Esquema de decryptografia do AESReflectorC

5.1.2.3 AESReflectorJ

Este refletor tem por finalidade fazer a inversão do fluxo recebido, ou seja, se não estiver criptografado, é feita a criptografia; se estiver criptografado é feita a decryptografia. A Figura 48 ilustra o funcionamento do refletor recebendo um fluxo não criptografado, fazendo sua criptografia e redistribuindo para diversos destinos.

O refletor *AESReflectorJ* foi construído em Java e integrado com o *AESReflectorC* através da utilização de *Java Native Interface* (JNI) (JNI, 2012), onde o fluxo é recebido por ele, é enviado ao ReflectorJ que redistribui o fluxo.

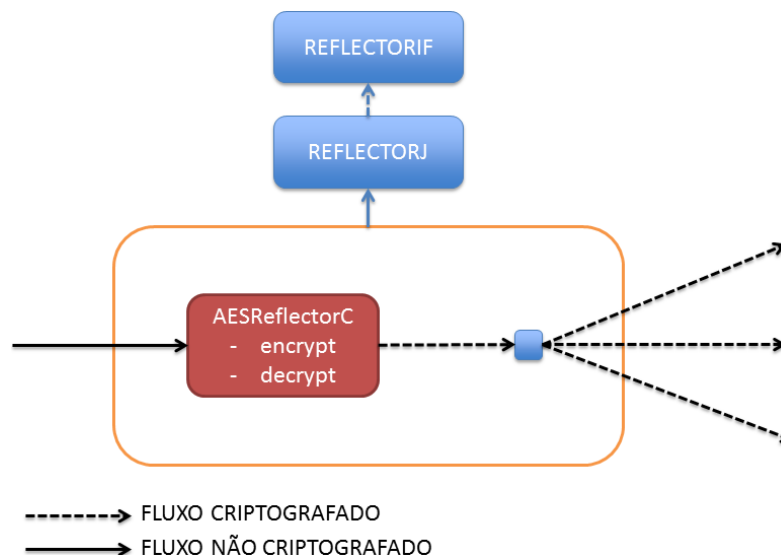


Figura 48. AESReflectorJ recebendo fluxo não criptografado e criptografando-o

A Figura 49 ilustra o refletor recebendo um fluxo criptografado, decryptografando-o e enviando esse fluxo para diversos destinos.

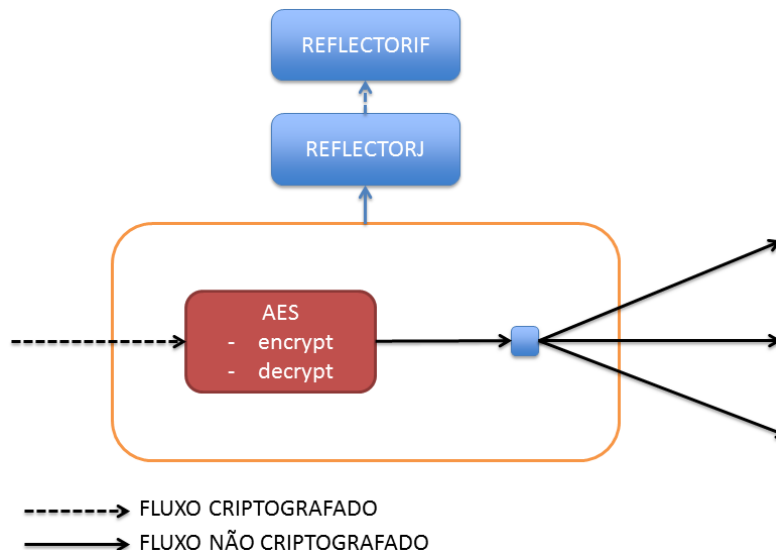


Figura 49. AESReflectorJ recebendo fluxo criptografado e decryptografando-o

5.1.2.4 AESHybridReflectorJ

Foi observada a necessidade de ter um refletor que tivesse a possibilidade de: ora receber criptografado e decryptografar, ora receber decryptografado e criptografar, além de ter a possibilidade de enviar fluxos criptografados e não criptografados.

Para tal funcionalidade foi criado, em Java, um refletor híbrido de criptografia denominado *AESHybridReflectorJ*.

A Figura 50 ilustra o refletor recebendo fluxo não criptografado e enviando fluxos criptografados e não criptografados. É possível observar que os fluxos não criptografados são apenas refletidos. Um fluxo é enviado a uma instância do *AESReflectorJ* para ser feita a criptografia e posterior envio de fluxos criptografados.

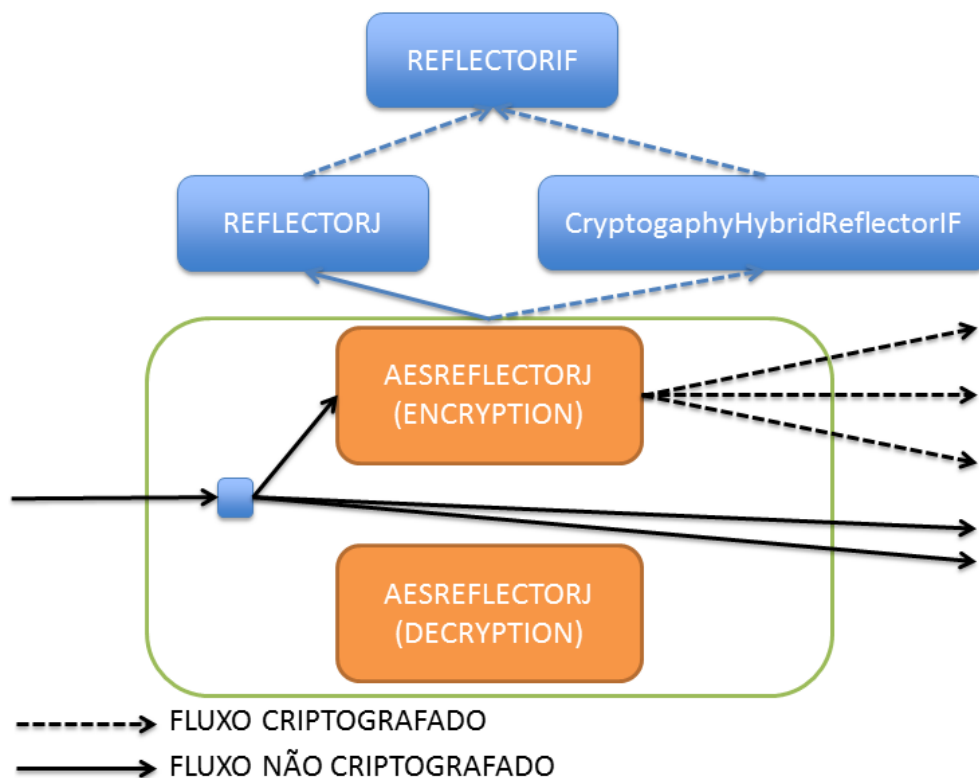


Figura 50. Esquema do AESHybridReflectorJ recebendo fluxo não criptografado

A Figura 51 mostra o *AESHybridReflectorJ* recebendo fluxo criptografado e enviando fluxos criptografados e não criptografados. Analogamente ao recebimento não criptografado, o envio de fluxos criptografados tem o fluxo apenas refletido e o envio de fluxos não criptografados é feito pela instância do *AESReflectorJ* responsável por fazer a decryptografia e redistribuir.

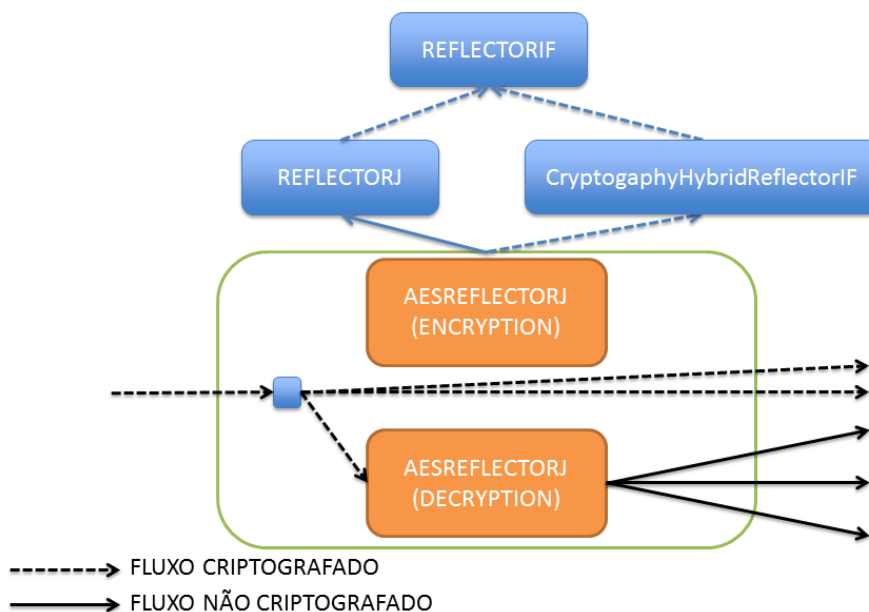


Figura 51. Esquema do AESHybridReflectorJ recebendo fluxo criptografado

É possível utilizar o mesmo *AESHybridReflectorJ* para receber tanto fluxos criptografados quanto fluxos não criptografados, sendo necessário apenas informar ao refletor qual o tipo de fluxo sendo por ele recebido para que os chaveamentos ilustrados da Figura 50 para a Figura 51 sejam realizados internamente e de forma abstraída.

5.1.2.5 FullAESHybridReflectorJ

Esse refletor permite a utilização de múltiplas codificações e a aplicação de criptografias no envio dos fluxos, ou seja, ele é híbrido para criptografia e codificação.

Sua construção utilizou várias instâncias do *AESHybridReflectorJ*, responsável pela criptografia, integrados com instâncias do *VlcjEncoderStylo* (SILVA, 2011), que tem uma codificação associada e é responsável pela transcodificação do fluxo.

Ao adicionar destinos, escolhe-se a codificação a ser aplicada (se desejar) e se o fluxo será criptografado ou não. O chaveamento dos fluxos é realizado internamente, independentemente do fluxo recebido ser criptografado ou não, para que o fluxo final atenda ao requisito desejado. Fluxos são enviados para *VlcjEncoderStylo* fazer a transcodificação; estes enviam um fluxo para uma instância associada do *AESHybridReflectorJ* responsável por fazer a criptografia e redistribuir fluxos criptografados e não criptografados. Fluxos que não precisam da aplicação de

codificação são apenas refletidos de forma criptografada ou não. É possível receber fluxos criptografados e não criptografados, bastando apenas informar o tipo do fluxo recebido ao refletor. A Figura 52 ilustra seu funcionamento interno.

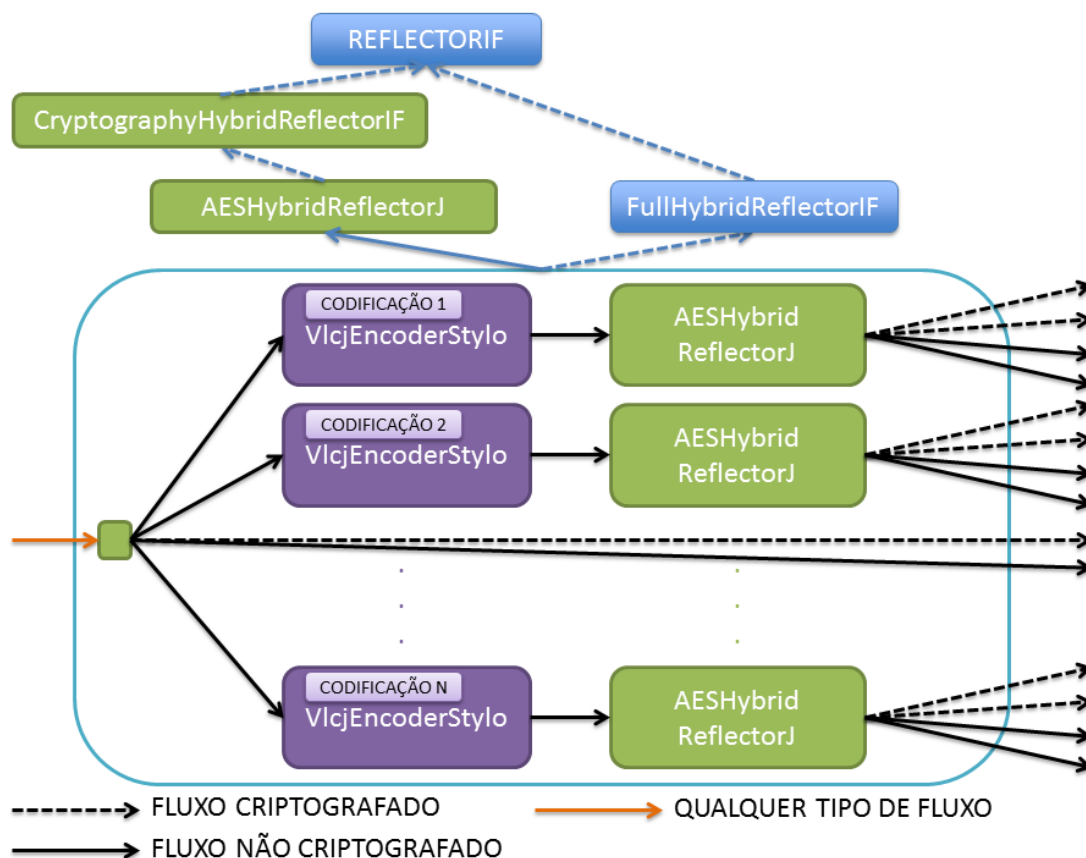


Figura 52. Esquema modular do FullAESHybridReflectorJ

Podem ser vistos um caso ótimo de utilização do refletor e um caso de maior *stress* possível. O caso ideal se caracteriza pela chegada de um fluxo, criptografado ou não, que deve ser passado a uma saída que está preparada para receber um fluxo passado do mesmo modo da entrada. O refletor apenas repassa o fluxo para a saída sem realizar nenhuma operação, servindo apenas como um caminho de comunicação/distribuição. O caso mais exigente de recursos de processamento e memória é visto quando se tem um fluxo de entrada criptografado e que necessita ser enviado para o canal de saída também criptografado, mas com codificação distinta da original. Esta exigência dá-se porque o framework *Stylo* aceita apenas fluxos sem criptografia, o que força o *FullAESHybridReflectorJ* a primeiro decriptografar o fluxo, para enviá-lo ao *VlcjEncoderStylo* e, depois de codificado de acordo com os padrões escolhidos, aplicar sobre ele uma operação de criptografia usando o AES para, finalmente, enviá-lo.

Com esse refletor, é possível criar aplicações que demandem o uso de criptografia ou de múltiplas codificações. As dificuldades de implementação na utilização desses requisitos foram abstraídas e isso possibilita um foco no objetivo final. Um exemplo de uso é demonstrado no CAPÍTULO 6:, quando o esse conjunto de refletores foram aplicados à Arthron.

5.2 VSecurityServer

O VSecurityServer (VSS) é um servidor que centraliza as atividades de autenticação e distribuição de chaves para membros de um grupo. O VSS foi integrado à Arthron e faz parte de sua versão 3.0. Nessa seção será apresentado seu modelo conceitual, arquitetural e tecnológico de forma a prover a segurança necessária para a transmissão de múltiplos fluxos multimídia.

A notação utilizada pelos conceitos descritos a seguir será a mesma utilizada por Stallings (2008), como pode ser vista na Tabela 5.

Tabela 5. Notação utilizada pelo trabalho. Adaptado de Stallings (2008)

Símbolo	Expressão	Significado
D, K	$D(K, Y)$	Decriptografia simétrica do texto cifrado Y usando a chave secreta K.
D, PR_A	$D(PR_A, Y)$	Decriptografia assimétrica do texto cifrado Y usando a chave privada de A.
D, PU_A	$D(PU_A, Y)$	Decriptografia assimétrica do texto cifrado Y usando a chave pública de A.
E, K	$E(K, X)$	Criptografia simétrica do texto claro X usando a chave secreta K.
E, PR_A	$E(PR_A, X)$	Criptografia assimétrica do texto claro X usando a chave privada de A.
E, PU_A	$E(PU_A, X)$	Criptografia assimétrica do texto claro X usando a chave pública de A.
K		Chave secreta
PR_A		Chave privada de A
PU_A		Chave pública de A
$\parallel$	$X \parallel Y$	X concatenado com Y

5.2.1 Modelo Conceitual

Para uma transmissão de dados segura, é necessário ter uma criptografia desses dados transmitidos, por exemplo, utilizando a estratégia descrita na seção 5.1. Nessa estratégia, é utilizado o modo de criptografia simétrica e, como descrito na seção 2.4, uma chave de criptografia entre o originador e o destinatário precisa existir para que o originador criptografe e o destinatário decifre corretamente. Uma maneira de fazer isso é ter ambos os lados da comunicação com um par de chaves pública e privada e fazer uma troca de chave simétrica utilizando a criptografia de chave pública a fim de estabelecer um canal seguro para troca.

Porém, um originador pode enviar o mesmo fluxo para mais de um destinatário e, em um cenário ideal, esse originador trocaria uma chave simétrica diferente com cada destinatário e faria uma criptografia para cada fluxo a ser enviado. A Figura 53 ilustra esse cenário onde um originador criptografa o mesmo fluxo três vezes com três chaves diferentes e o envia para seus destinos.



Figura 53. Cenário ideal para transmissão de múltiplos fluxos criptografados

Essa estratégia se torna ineficiente diante de três aspectos:

- À medida que mais destinos são adicionados, mais recursos são necessários para a criptografia;
- Com a utilização de fluxos em alta definição, ou seja, maior quantidade de dados, mais recursos são necessários para a transmissão dos dados;
- Um originador pode ser também destinatário e vários fluxos podem ser enviados e recebidos por cada um, o que demandaria uma gerência de

chaves que aumenta a complexidade à medida que a quantidade de fluxos cresce.

Para contornar essa limitação, o conceito de grupos abordados por diversos trabalhos no mapeamento sistemático, descrito na seção 4.1, como o de Sandosh (2010) e Holeman (2012) é uma alternativa que se adéqua bem a esse contexto. Na primeira versão da estratégia, o grupo foi denominado Sessão (VIEIRA, 2011) e, para uma melhor adequação, passa a ser chamada de Sessão Colaborativa (SC), visto que há sempre mais de um participante interagindo e isso caracteriza um mínimo de colaboração entre eles. Uma SC tem características próprias e, quando 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 54 ilustra este último cenário, atribuindo à SC uma chave simétrica compartilhada entre os seus membros. Desta forma, a criptografia é realizada uma única vez e o fluxo criptografado é distribuído a os destinos desejados.



Figura 54. Cenário de criptografia de múltiplos fluxos utilizando Sessão

Outros aspectos ainda necessitam ser expostos, como a geração e a distribuição dessa chave, que precisam ser realizadas por uma entidade em que todos os usuários confiem; e a possibilidade de ter múltiplas sessões acontecendo simultaneamente, com a entrada e saída de novos usuários durante uma sessão. Diante disso, uma solução é a estratégia de um servidor central com a responsabilidade de criação e gerenciamento de sessões e geração e distribuição

de chaves para os usuários, assim como descrito nos trabalhos de Sandosh (2010), Holeman (2012) e Zhu (2007). A inclusão de membros em uma SC e a distribuição de chaves para eles só pode ocorrer para membros autorizados, o que demanda uma prévia autenticação.

Para melhor representar um membro de um grupo, este será tratado como sujeito, que representa um usuário humano ou uma entidade que atua em nome dele. A Figura 55 ilustra o processo de autenticação, criação de SC e posterior distribuição da chave da sessão para um sujeito. Pode-se observar o Sujeito 1 se autenticando, criando uma SC e inserindo o Sujeito 2 nela, o que dá permissão ao Sujeito 2 para ter acesso à chave de criptografia. O Sujeito 2 se autentica e solicita a chave de criptografia da SC.



Figura 55. Autenticação, criação de Sessão e distribuição de chave em um Servidor Central

5.2.2 Modelo Arquitetural e Tecnológico

Para atuar como Servidor Central, foi criado o VSecurityServer (VSS), que é responsável por fazer o cadastro de sujeitos, autenticação, criação de SCs, geração de suas chaves e distribuição a sujeitos autorizados a participar dela, ou seja, há um gerenciamento de permissões. Para permitir a utilização de múltiplas tecnologias

distintas o VSS foi criado como um Webservice (WEBSERVICE, 2012) em Java e a comunicação com os sujeitos ocorre de forma segura utilizando *Secure Sockets Layer* (SSL) (SSL, 2012).

A Tabela 6 detalha os campos mínimos para o cadastro de uma SC, mas novos campos podem ser inseridos dependendo da necessidade e do contexto empregado.

Tabela 6. Descrição dos dados da Sessão Colaborativa armazenados no Servidor

DADO	DESCRIÇÃO
Identificador	Identificação única
Data de Início	A data de início
Data de Fim	A data de finalização
Criador	O usuário criador
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 de criptografia
Modo	Designa se é moderada. Quando moderada, apenas usuários convidados pelo criador podem acessar

Para haver uma adequação com a arquitetura da Arthron para com o seu módulo Recorder, mais um campo foi inserido para indicar se uma Sessão é gravada ou não, ou seja, se ela terá seus vídeos gravados para permitir uma posterior recuperação.

A Tabela 7 detalha os campos mínimos para o cadastro de um sujeito.

Tabela 7. Descrição dos dados do usuário armazenados no Servidor

DADO	DESCRIÇÃO
Nome	Nome
Nome de Usuário	Identificador do usuário
Email	E-mail do usuário
Tipo de Perfil	Define permissões
Hash da Senha	O <i>hash</i> da senha utilizado para autenticação

A autenticação de um sujeito cria um Token entre ele e o VSS. O Token é um hash que serve para a proteção da senha do sujeito, em uma não utilização do SSL ou em uma possível quebra dessa segurança, onde a senha jamais é transmitida entre ambas as partes e tem o objetivo também de servir de autenticação entre os sujeitos. A Figura 56 ilustra o processo de criação do Token, que tem seu início com a solicitação de um número aleatório (*nonce*) (passo 1) por parte do sujeito, recebimento do *nonce* (passo 2) que usa o *hash* de sua senha para criar outro *hash* computado a partir da concatenação dele com o *nonce* recebido (passo 3). O Token é enviado de volta ao VSS (passo 4) que repete o processo, visto que conhece o *hash* da senha do usuário e o *nonce* enviado e faz a comparação entre o Token gerado por ele e o Token enviado pelo usuário: se forem iguais o usuário é autenticado.

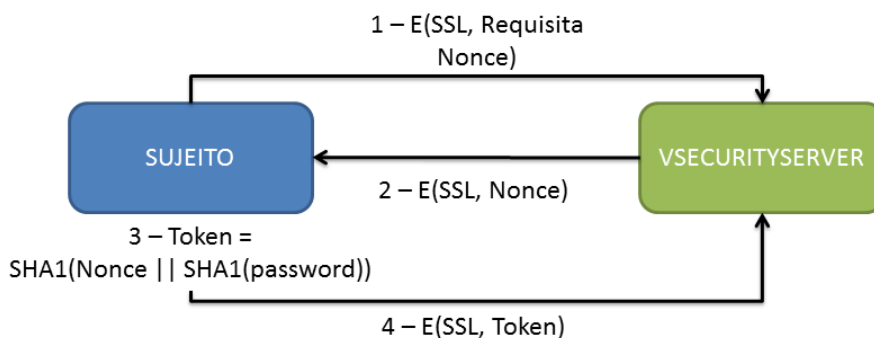


Figura 56. Criação do Token de uma autenticação de um sujeito no VSecurityServer

O processo de utilização do Token protege a senha do sujeito visto que a cada autenticação um Token diferente será gerado e apenas com o conhecimento da senha que um Token correto será utilizado. Vale destacar que, com a utilização de um certificado digital, tem-se uma autenticação mútua, ou seja, o VSS se autentica com o usuário (provando ser quem diz ser) e o sujeito se autentica com a estratégia descrita.

A importância da autenticação federada se faz presente no VSS e o processo de autenticação foi integrado a CAFé, logo o VSS passou a utilizar os conceitos de Provedores de Identidade (IdP) e há a possibilidade da autenticação ser delegada a um IdP da café, sendo a autenticação local, descrita anteriormente, tratada como um IdP interno. A Figura 57 ilustra o primeiro passo que é a requisição dos IdPs válidos por um sujeito. Essa é uma etapa pública que é feita antes da autenticação do usuário, ou seja, não é necessário estar autenticado para fazer essa requisição.

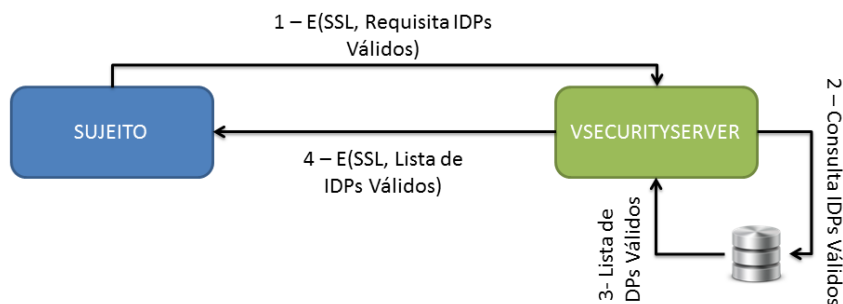


Figura 57. Requisição de IdPs de um sujeito ao VSecurityServer

A Figura 58 ilustra o processo de autenticação de um usuário na CAFe. Após receber a lista de IdPs válidos, o sujeito faz uma solicitação de autenticação enviando seu usuário, sua senha na CAFe e o IdP escolhido (passo 1). O VSS encaminha a solicitação a café (passo 2) e recebe de volta uma *Security Assertion Markup Language* (SAML) com informações do usuário autenticado (passo 3). Nem todos os usuários da CAFe terão permissão de utilizar o sistema, que pode ser restrito apenas a médicos, residentes e pessoas autorizadas a trabalhar com telemedicina, por exemplo, portanto um usuário precisa ser previamente autorizado no VSS e essa verificação de autorização do usuário é feita no passo 4 e 5. O passo 6 consiste no encaminhamento do SAML ao sujeito caso ele esteja autenticado e com permissões para a utilização do serviço.

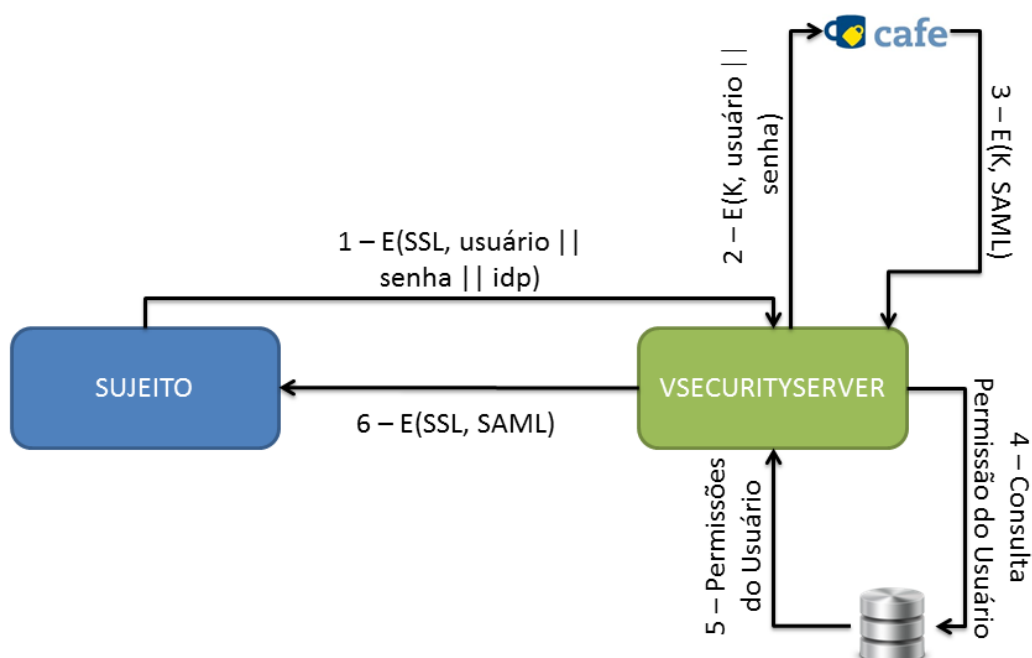


Figura 58. Autenticação de um sujeito na CAFe utilizando VSecurityServer como intermediador

O processo de autenticação local, nesse esquema, é análogo, sendo que no passo 1 é enviado o Token no lugar da senha e não é realizado o encaminhamento

da solicitação a CAFe. Em vez disso, é aplicada a estratégia de comparação do Token.

O intermédio entre o VSS e a CAFe foi feito utilizando um framework cedido pelo Grupo de Trabalho Serviços para Transposição de Credenciais de Autenticação Federadas (STCFed) (STCFED, 2012). Para facilitar o desenvolvimento e a manutenção, foi incluído um esquema de logs utilizando o Log4J (LOG4J, 2012).

Além da transmissão de fluxos entre sujeitos de uma sessão, esses sujeitos também podem trocar outros tipos de dados em pares, como informações de controle e comunicação. Esses dados são de um volume bem menor e não há problemas em cada par de usuários terem uma chave simétrica para essa comunicação. Para isso uma chave precisa ser gerada e distribuída para cada par de usuários e essa geração e distribuição da chave é feita pelo VSS. A Figura 59 ilustra esse processo, no qual, primeiro o sujeito 1 solicita uma chave simétrica com o sujeitos 2 ($K_{1,2}$) ao VSS (passo 1), que gera essa chave e envia para o sujeito 1 (passo 2). O Token gerado para autenticação é também utilizado para confirmar autenticidade com outros sujeitos, concatenando o Token com a identificação do sujeito 2 e aplicando uma função de *hash*, tendo assim um Token entre ambos ($Token_{1,2}$), que é ilustrado no passo 3. O $Token_{1,2}$ é então enviado criptografado com a $K_{1,2}$. O sujeito 2 ainda não tem a $K_{1,2}$ e faz a solicitação e recebe-a do VSS (passos 5 e 6). O sujeito 2 decriptografa o $Token_{1,2}$ e envia ao VSS para a averiguação se é um Token válido para a comunicação entre o sujeito 1 e o sujeito 2 (passo 7), que tem sua resposta dada no passo 8. A partir da validação do $Token_{1,2}$ o sujeito 2 aceita ou não a conexão com o sujeito 1 e inicia um processo de comunicação segura utilizando a $K_{1,2}$.

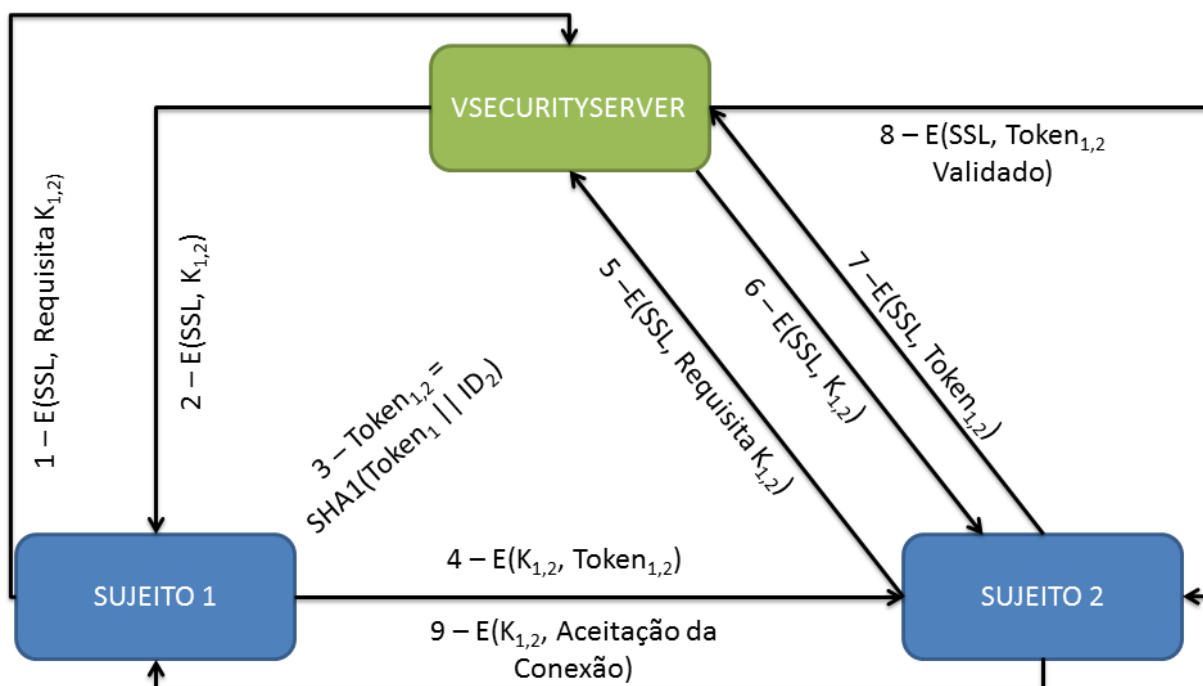


Figura 59. Processo de iniciação de comunicação segura entre dois sujeitos utilizando o VSecurityServer

É importante destacar que o $\text{Token}_{1,2}$ só é válido entre o sujeito 1 e o sujeito 2. O $\text{Token}_{2,1}$ (caso o sujeito 2 iniciasse a comunicação) é diferente do $\text{Token}_{1,2}$. Outro fator importante é que o $\text{Token}_{1,2}$ que o sujeito 1 compartilhou com o sujeito 2 não é válido com nenhum outro sujeito que não seja o sujeito 2, ou seja, o sujeito 2 não consegue se passar pelo sujeito 1 utilizando o $\text{Token}_{1,2}$ porque esse Token só é válido para o sujeito 1 iniciar uma comunicação segura com o sujeito 2. Como o Token entre sujeitos é baseado no Token de autenticação e o Token de autenticação é baseado em um *nonce* que muda a cada autenticação, todos os Tokens deixam de serem válidos assim que um sujeito faz o *logout* no VSS, isso implica em todos os $\text{Token}_{1,n}$ diferentes, visto que para uma nova autenticação o Token de autenticação será diferente.

A Figura 60 ilustra o processo em que o sujeito 3 tenta se passar pelo sujeito 1 para o sujeito 2, quando o sujeito 1 e o 2 estão devidamente autenticados. O esquema mostra que, mesmo o sujeito 3 tendo descoberto a $K_{1,2}$, sem o Token_1 ele não consegue se passar por 1 e a tentativa de comunicação forjada falha.

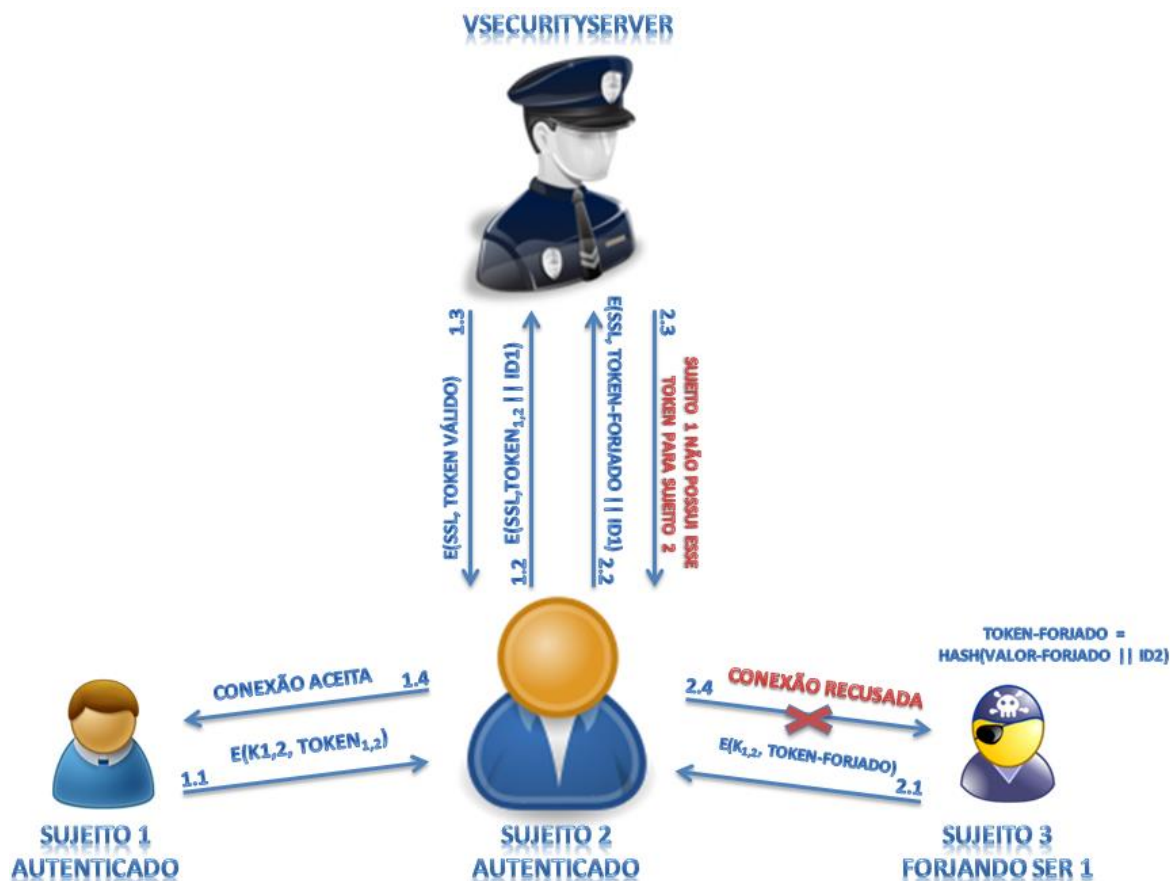


Figura 60. Tentativa de um sujeito se passar por outro em uma comunicação

Conforme descrito no modelo conceitual, a criação de SCs é feita por um sujeito devidamente autenticado que define seus campos (Tabela 6). Outro sujeito que tenha sido convidado a participar pode requisitar a chave da SC, terá acesso aos dados transmitidos e poderá transmitir dados criptografados.

Para facilitar a distribuição de informações o VSS envia e-mails com dados de Sessões Colaborativas e perfil do sujeito (exceto senhas) para seus e-mails e essa funcionalidade foi construída utilizando a JavaMail (JAVAMAIL, 2012). O sujeito para o VSS foi integrado a Arthron e, com isso, os módulos desse serviço tem a possibilidade de fazer tanto autenticações locais quanto autenticações na CAFE.

CAPÍTULO 6: VERIFICAÇÃO

Neste capítulo é apresentada a verificação do trabalho, os materiais utilizados e é feita a discussão comparando-o com os trabalhos correlatos descritos na seção 4.2. Conforme descrito no CAPÍTULO 5:, a estratégia foi dividida em duas partes e esse capítulo segue o mesmo modelo.

6.1 Materiais

Dois computadores foram utilizados para o processo de desenvolvimento e para os testes de verificação realizados sobre as duas partes desse trabalho. Suas características são apresentadas na tabela.

Tabela 8. Descrição dos computadores utilizados para desenvolvimento e testes.

Característica	Computador A	Computador B
Processador	Intel Core i7-2670QM 2.2GHz	Intel Core i5 com 3.2GHz
Memória	8 Gb DDR2 1333 Mhz	2 Gb DDR2 1333 Mhz
Sistema Operacional	GNU/Linux Ubuntu 11.04 64 bits	GNU/Linux Ubuntu 11.04 64 bits
Interface de Rede	10/100/1000	10/100/1000

Para o desenvolvimento foi utilizado o Netbeans 7.1.2 (NETBEANS, 2012), um dos principais Ambientes de Desenvolvimento Integrado (IDE) para a linguagem Java.

6.2 Refletores para Codificação e Criptografia em Tempo Real

Os resultados apresentados a seguir foram obtidos em uma sequência de experimentos com dois computadores do tipo A e B, descrito na seção 6.1.

O objetivo dos testes é identificar o *overhead* causado em fluxos de vídeos que utilizam o Refletor Híbrido de criptografia e codificação, além de identificar quais fatores mais contribuem nesse *overhead*. É necessário calcular o tempo de atraso que o refletor híbrido adiciona durante a transmissão de um fluxo de vídeo. Para obter esse tempo, será calculado o tempo de uma transmissão entre dois VLCs (Figura 61-a) e o tempo será marcado entre o Refletor1 e o Refletor2, vistos que

esses apenas repassam o fluxo e provêm recursos para tal operação. Para calcular o *delay* inserido pelo *FullAESRybridReflector*, são inseridos duas instâncias, uma para envio e outra para recepção (Figura 61-b). Calculada a diferença de tempo de execução entre esses dois casos será possível estimar o *overhead* causado pelo refletor durante o envio do fluxo pela rede.

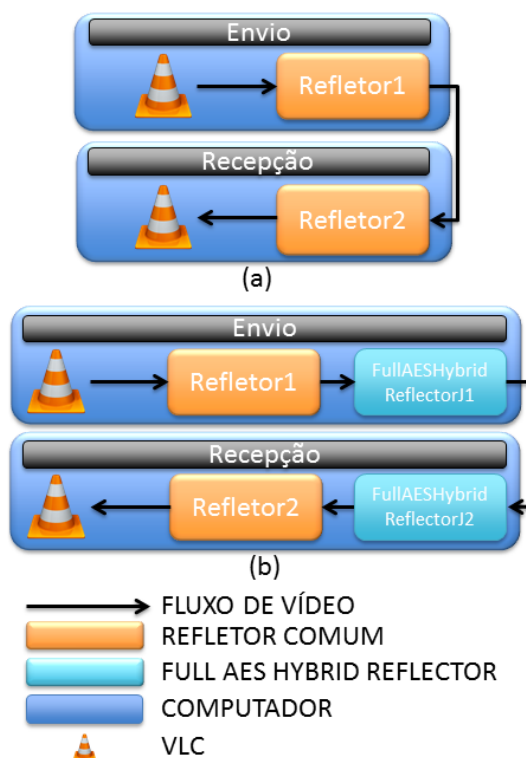


Figura 61. Esquema de realização dos testes

Para a realização dos testes foi utilizado o Método Fatorial 2^k (JAIN, 1991) com quatro fatores: criptografia, codificação, processador e qualidade do vídeo. Segundo esse método, é necessário definir os níveis 1 e -1 para cada fator, que representa o estado do fator para dois momentos distintos. A Tabela 9 ilustra os fatores e os níveis aplicados para cada fator. Com isso foi possível analisar a influência de cada fator no *overhead* causado na transmissão do fluxo.

Tabela 9. Fatores e seus níveis aplicados no modelo 2^k

Fatores	Nível 1	Nível -1
Criptografia (A)	Com criptografia	Sem criptografia
Codificação (B)	MPEG2	Sem codificação
Processador (C)	Intel Core i7	Intel Core i5
Qualidade de Vídeo (D)	Full HD (1920x1080p)	SD (720x480p)

Nos testes foram utilizados quatro vídeos do banco de dados do W6RZ (W6RZ, 2012) para testar o comportamento do esquema de refletores com mídia FULL HD (1920x1080) e mídia SD (640x480), sendo dois de cada tipo, cujas informações podem ser vistas na Tabela 10. Os vídeos SD são os mais comumente usados em transmissões por serem compactos e de qualidade razoável e os FULL HD são utilizados quando se dispõe de uma grande banda de rede para transmissão, já que a grande quantidade de informação necessária para transmissão de vídeo de altíssima qualidade demanda uma infraestrutura rápida e confiável de comunicação.

Tabela 10. Informações sobre os vídeos de teste.

Parâmetro	Vídeos SD	Vídeos FULL HD
Codec	MPEG-2	MPEG-2
FPS	30	30
Escala	1	1
Largura	720	1920
Altura	480	1080
Taxa de áudio	44100	44100

As codificações aplicadas para os vídeos podem ser vistas na Tabela 11.

Tabela 11. Codificação de áudio e vídeo dos fluxos transmitidos pelo Refletor

Parâmetro	SD	HD
Codec de Vídeo	WMV1	WMV1
Taxa de Bits	512	2048
FPS	30	30
Escala	1	1
Largura	720	1920
Altura	480	1080
Codificação de Áudio	MPGA	MPGA
Taxa de Bits de Áudio	128	128
Amostragem de Áudio	44100	44100
Canais	1	1

Seguindo os passos do modelo, foi possível criar a tabela de combinação dos fatores, conforme ilustrado na Tabela 12. Para a construção dessa tabela é necessário fazer todas as combinações possíveis de fatores o que irá gerar as colunas. Como a quantidade de fatores é quatro, as quatro primeiras colunas definem cada teste e elas são diferentes em todas as 16 linhas. Após a definição das quatro primeiras colunas de cada linha, as colunas subsequentes são obtidas a partir dessas fazendo a multiplicação dos fatores da coluna atual utilizando os valores definidos nas quatro primeiras colunas da linha corrente, por exemplo: na linha um e coluna cinco é desejado encontrar o valor para AB, sendo $A = 1$ e $B = 1$, ou seja, $A*B = 1*1 = 1$. Essa multiplicação ocorre para determinar, depois de concluídos todos os experimentos, a influência das combinações dos fatores em questão no resultado de cada experimento. A coluna tempo é o resultado de cada teste e será explicada posteriormente.

Tabela 12. Tabela do Modelo 2^k , com $k = 4$

A	B	C	D	AB	AC	AD	BC	BD	CD	ABC	ABD	BCD	ACD	ABCD	Tempo
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0.683
1	1	1	-1	1	1	-1	1	-1	-1	1	-1	-1	-1	-1	0.847
1	1	-1	1	1	-1	1	-1	1	-1	-1	1	-1	-1	-1	0.961
1	-1	1	1	-1	1	1	-1	-1	1	-1	-1	-1	1	-1	0.147
-1	1	1	1	-1	-1	-1	1	1	1	-1	-1	1	-1	1	0.767
1	1	-1	-1	1	-1	-1	-1	-1	1	-1	-1	1	1	1	0.786
1	-1	-1	1	-1	-1	1	1	-1	-1	1	-1	1	-1	1	0.285
-1	-1	1	1	1	-1	-1	-1	-1	1	1	1	-1	-1	1	0.179
-1	1	1	-1	-1	-1	1	1	-1	-1	-1	1	-1	1	1	0.564
1	-1	1	-1	-1	1	-1	-1	1	-1	-1	-1	1	-1	1	0.148
-1	1	-1	1	-1	1	-1	-1	1	-1	1	-1	-1	1	1	0.823
-1	1	-1	-1	-1	1	1	-1	-1	1	1	-1	1	-1	-1	0.521
-1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	1	-1	0.44
-1	-1	-1	1	1	1	-1	1	-1	-1	-1	1	1	1	-1	0.56
1	-1	-1	-1	-1	-1	-1	1	1	1	-1	1	-1	1	-1	0.225
-1	-1	-1	-1	1	1	1	1	1	1	-1	-1	-1	-1	1	0.185

Foram escolhidas uma margem de erro de 5% (para mais ou para menos) com um intervalo de confiança de 95%. A partir disso é necessário realizar cada teste i vezes, sendo i um valor arbitrário, e será possível descobrir quantas vezes

mais é necessário realizar esse teste novamente aplicando a seguinte fórmula: $n = ((100 * z * s) / (r * x))^2$, onde s é o desvio padrão, x é a média (s e x obtidos a partir os i testes realizados anteriormente) e z é um parâmetro que é definido a partir da margem de erro e do intervalo de confiança, que, nesse caso, é 1.96. Cada teste realizado é subtraído do tempo gasto pelo teste sem o *FullAESHybridReflectorJ* (ilustrado na Figura 61-a) e a média dos resultados são os valores ilustrados na coluna Tempo da Tabela 12.

Para cada fator e combinação de fatores (expostos na Tabela 12), é necessário calcular a média (q). Isso é feito através da soma da multiplicação do nível de cada linha do fator pelo tempo correspondente e, ao final, depois dividindo por 2^k , ou seja, 16. A partir desse resultado é possível calcular a variação total de cada fator ou combinação de fatores (SST – Total Sum of Squares), da seguinte maneira: $SST = 2^k * (\sum qi)$. O SST ilustra (em porcentagem) a influência de cada fator no resultado final. Tudo isso é ilustrado na Tabela 13.

Tabela 13. Soma, q e SST de cada fator

Fator	Soma	q	SST (%)
A	0.043	0.0026875	0.008
B	3.782	0.236375	63.8
C	-0.571	-0.0356875	1.45
D	0.689	0.0430625	2.11
AB	1.161	0.0725625	6.01
AC	-0.2929	-0.01830625	0.38
AD	-0.549	-0.0343125	1.34
BC	0.111	0.0069375	0.05
BD	0.342	0.021375	0.52
CD	-1.13	-0.070625	5.69
ABC	-0.565	-0.0353125	1.42
ABD	-1.776	-0.111	14
ACD	0.259	0.0161875	0.29
BCD	0.334	0.020875	0.49
ABCD	0.719	0.0449375	2.3

Através da análise dos resultados obtidos na Tabela 13, é possível observar que o que mais influencia para o aumento do *delay* em uma transmissão utilizando os refletores é a aplicação de codificação no vídeo, com 63.8%, sendo esse fator o ponto mais crítico e com interferência bem superior aos outros. Analisando os fatores individualmente, a qualidade do vídeo fica sem segundo lugar no ranking de influências, seguida pela escolha do processador e, por fim, a criptografia, o que mostra que esse fator, apesar de aplicado em grande quantidade de dados (como em vídeos FULL HD), se mostrou eficiente e com influência praticamente desprezível, se comparado com os outros fatores. Outro ponto importante a ser destacado é a utilização combinada dos quatro fatores (ABCD), que tem influência baixa se comparada com a combinação de apenas dois fatores, como a criptografia e codificação juntas (AB) ou o processador e a qualidade do vídeo (CD), que tem influências superiores.

É importante destacar que, mesmo criptografando todo o fluxo, o processamento utilizado para fazer esse passo é quase desprezível em relação ao gasto para fazer transcodificação e esse comportamento é observado tanto em vídeos SD quanto vídeos FULL HD, demonstrando que a criptografia total dos dados, mesmo em fluxos com grande quantidade de dados, é viável e, para o contexto utilizado nesse trabalho, isso vai de encontro ao afirmado por Lian (2006), que afirmou que a utilização da criptografia total dos dados com o AES não é eficiente. A criptografia seletiva (FAN, 2011; MOU, 2009; LIAN, 2006) precisa ser melhor investigada para ser possível uma comparação, porém é necessário que esta seja muito vantajosa (em termos de eficiência e adaptabilidade) para que sua utilização venha a ser melhor empregada na estratégia do que a utilização do AES com criptografia total.

A criptografia total dos dados utilizando o AES, assim como os trabalhos de Mou (2009), Zhu (2007) e Asghar (2010), não permite a adaptabilidade demonstrada por Mou (2009) e, por usar criptografia simétrica com uma chave compartilhada entre a origem e o destino, não permite a verificação da integridade de origem como ilustrada por Challal (2005) e Lian (2009), mas provê a integridade dos dados com uma baixa demanda de processamento.

6.3 VSecurityServer

A verificação e validação apresentadas a seguir foram obtidas utilizando computadores do tipo B, descrito na seção 6.1. O VSecurityServer foi hospedado em um Tomcat (TOMCAT, 2012), um servidor para aplicações *Java Enterprise Edition* (JEE), onde ficou acessível para responder as solicitações de sujeitos.

Através do *Web Service Definition Language* (WSDL) foi criado um cliente para a comunicação com o VSS. Esse cliente foi inserido aos módulos da Arthron que puderam fazer uso da autenticação local e na CAFe, além de ter uma comunicação segura entre eles.

A Figura 62 ilustra a tela de criação de usuário onde é possível inserir o nome, o nome de usuário, email e o tipo do perfil (que define as permissões).

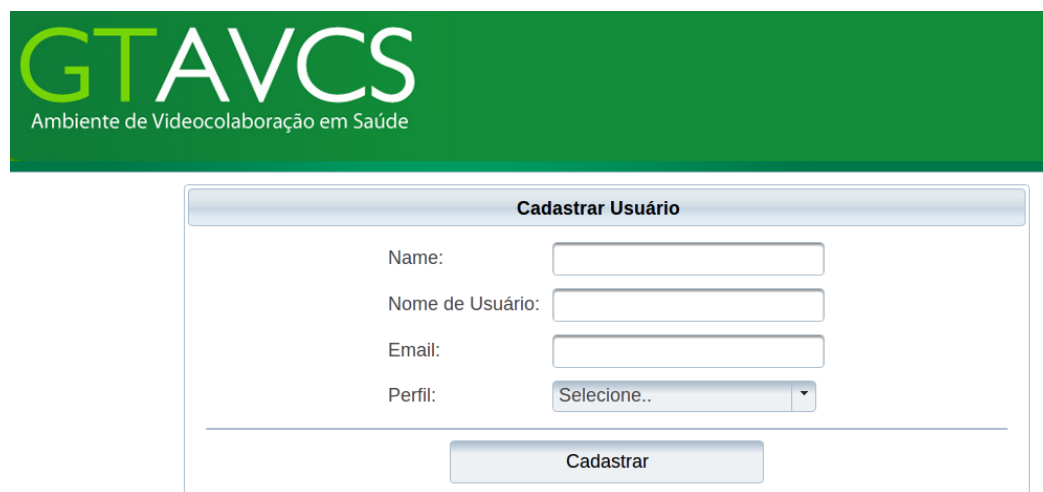


Figura 62. Cadastro de usuário no ArthronServer

O ArthronServer utiliza a criação de Sessão como agendamentos futuros e a tela de agendamento é ilustrada na Figura 63. É possível marcá-la como moderada, se ela será gravada, qual a sua data de início, qual a sua data de fim e todos os usuários participantes.

GTAVCS
Ambiente de Videocolaboração em Saúde

Agendar Sessão:

Moderada: ☒

Gravada: ☒

Começa em: * 05/07/2012 12:00

Termina em: * 05/07/2012 16:00

Adicionar Usuário (username): elenilson

Adicionar Usuário

Usuários Participantes		
Username	Nome	Email
gtavcs	GTAVCS	gtavcs.lavid@gmail.com

Agendar

Figura 63. Tela de agendamento de Sessão no ArthronServer

A Figura 64 ilustra a tela de autenticação no ArthronServer, onde é necessário inserir o nome de usuário, a senha e escolher o IdP.

Arthron Server

arthronserver.lavid.ufpb.br:8080/ArthronServerII/

GTAVCS
Ambiente de Videocolaboração em Saúde

Usuário: * gtavcs

Senha: * *****

Provedor de identidade: * Local

Entrar

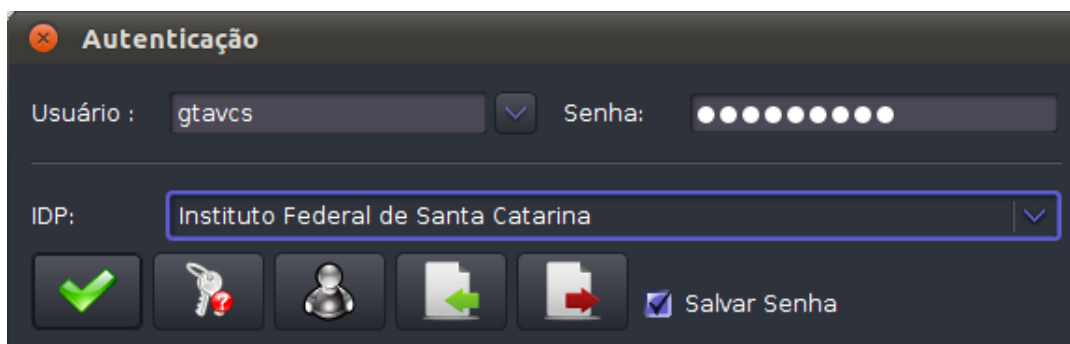
[Ajuda](#) | [Contatos](#)

Copyright © 2012, LAVID. Todos os direitos reservados

Desenvolvido por: lavid

Figura 64. Tela de autenticação no ArthronServer

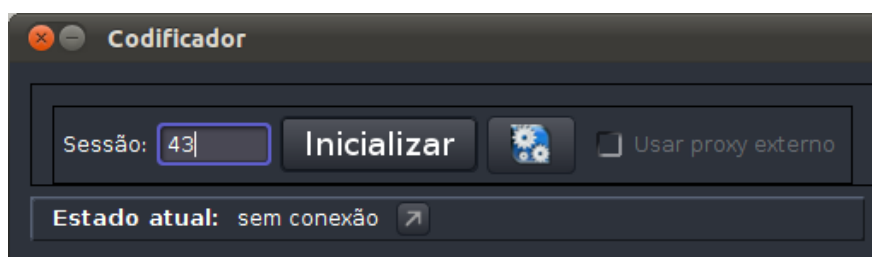
O mesmo processo de autenticação foi feito nos módulos desktop e, como pode ser visualizado na Figura 65, a tela de autenticação de um Encoder é similar a do ArthronServer, sendo necessário inserir o nome de usuário, senha e IdP.



A imagem mostra uma janela de autenticação intitulada "Autenticação". Ela possui campos para "Usuário:" (contendo "gtavcs"), "Senha:" (com pontos para mascaramento) e "IDP:" (com uma lista suspensa selecionando "Instituto Federal de Santa Catarina"). Abaixo dos campos, há uma barra de ferramentas com ícones para sucesso, erro, perfil, navegação e uma opção "Salvar Senha" marcada.

Figura 65. Tela de autenticação do Encoder

Para os módulos que desejam se conectar em um ArthronServer é necessário inserir qual a Sessão para a conexão. A Figura 66 ilustra esse processo.



A imagem mostra uma janela intitulada "Codificador". Ela contém um campo "Sessão:" com o valor "43", um botão "Inicializar", um ícone de engrenagem e uma opção "Usar proxy externo" desmarcada. Abaixo, há uma barra de status "Estado atual: sem conexão" com uma seta para cima.

Figura 66. Escolha de Sessão no Encoder

Para o gerenciamento das Sessões no ArthronServer foi criado uma tela onde é possível visualizar todas que um determinado usuário criou e é possível promover suas ações sobre elas. A Figura 67 ilustra essa lista.



A imagem mostra a interface de gerenciamento de sessões no ArthronServer. No topo, há um banner verde com o logo "GTAVCS" e o subtítulo "Ambiente de Videocolaboração em Saúde". Abaixo, há uma tabela intitulada "Minhas Sessões Agendadas" com uma barra de paginação no topo (mostrando 1 de 1 página). A tabela possui 8 colunas: ID, Previsão de Início, Previsão de Término, Finalizada em, Moderada, Gravada, Status e Proprietário. Abaixo da tabela, há uma barra de paginação e três botões: "Gerenciar", "Ver Detalhes" e "Finalizar".

ID	Previsão de Início	Previsão de Término	Finalizada em	Moderada	Gravada	Status	Proprietário
13	05/07/2012 00:00	06/07/2012 00:00		Sim	Sim	Em Andamento	GTAVCS
14	05/07/2012 00:00	06/07/2012 00:00		Sim	Sim	Em Andamento	GTAVCS
8	03/07/2012 04:09	04/07/2012 00:00	04/07/2012 00:00	Sim	Sim	Terminada	GTAVCS
7	03/07/2012 04:08	03/07/2012 04:08	03/07/2012 16:08	Sim	Sim	Terminada	GTAVCS
5	30/05/2012 21:00	31/05/2012 21:00	03/07/2012 16:03	Sim	Sim	Terminada	GTAVCS

Figura 67. Lista de Sessões de um usuário no ArthronServer

CAPÍTULO 7: RESULTADOS E DISCUSSÃO

Esse capítulo apresenta os resultados obtidos e discute as vantagens e as limitações da estratégia desenvolvida neste trabalho. Primeiramente, é feita uma análise comparativa da estratégia desenvolvida face aos trabalhos correlatos identificados na literatura (vide Capítulo 3). Em seguida, ressaltamos a aplicação da estratégia no plano prático através de um piloto integrado à Arthron e demonstrado no X Workshop da Rede Nacional de Ensino e Pesquisa. Neste piloto, foram feitas transmissões locais e foi possível observar o comportamento da estratégia na prática. Também são listadas as publicações resultantes deste trabalho em parceria com o GTAVCS. Por fim, discutimos um ponto crítico neste tipo de trabalho que é o licenciamento. Para tanto, foi feita uma análise em todas as dependências utilizadas na implementação da Arthron 3.0.

7.1 Análise Comparativa

A estratégia utilizada para a análise dos trabalhos foi feita através da comparação entre os tipos de criptografia utilizados, a estratégia de distribuição de chaves e seus algoritmos de criptografia. A estratégia proposta por esse trabalho foi concebida através da análise desses trabalhos de forma a atingir o objetivo de prover a segurança requerida, portanto, são utilizadas a criptografia simétrica por ter a criptografia aplicada em um grande volume de dados, esse tipo de criptografia se adequa, a distribuição de chaves utilizando um servidor central e o algoritmo utilizado é o AES. A comparação entre os trabalhos relacionados e a estratégia realizada pode ser visualizada na Tabela 14.

Tabela 14. Comparação dos trabalhos correlatos

Trabalho	Tipo de Criptografia	Distribuição de Chaves	Algoritmo de Criptografia
Fan (2011)	Simétrica, Seletiva	Não cita	Próprio
Sadosh (2010)	Simétrica	Servidor Central	Skipjack
Mou (2009)	Assimétrica	Não cita	Elliptic Curve Cryptography, AES
Challal (2005)	Baseada em Hash	Não cita	Hybrid Hash-Chaining

Zhu (2007)	Simétrica	Servidor Central	AES
Lian (2006)	Simétrica	Não cita	Próprio
Estratégia Realizada	Simétrica	Servidor Central	AES

A utilização de uma criptografia seletiva aliada a uma criptografia simétrica traria benefícios em termos de uso de processamento e diminuição de retardo, visto que não será mais preciso criptografar todos os dados do fluxo. Esse é um dos pontos que poderia ser incorporado e que agregaria desempenho à estratégia realizada.

7.2 Resultados Práticos

O GTAVCS apresentou os resultados do seu trabalho no X Workshop da Rede Nacional de Ensino e Pesquisa, realizado em Ouro Preto – MS nos dias 30 de abril e 1 de maio de 2012 (WRNP, 2012) que fez parte do XXX Simpósio Brasileiro de Redes de Computadores (SBRC, 2012). No WRNP 2012 foi mostrado, em primeira mão, a versão 3.0 da Arthron, foram feitas transmissões locais e uma integração com o GT de Cinema (GT CINEMA, 2012), também do LAViD.

No WRNP 2012 foram feitas três demonstrações. A Demonstração 1 consistiu em criar uma Sessão no ArthronServer, convidar usuários, conectar módulos e fazer o gerenciamento de transmissões de fluxos multimídia criptografados ou não. Todos os módulos passavam por autenticação e recebiam uma chave de Sessão Colaborativa para fazer uma transmissão segura e todos os fluxos tinham uma cópia enviada ao Recorder para posterior recuperação da experiência. A Figura 68 ilustra essa demonstração.

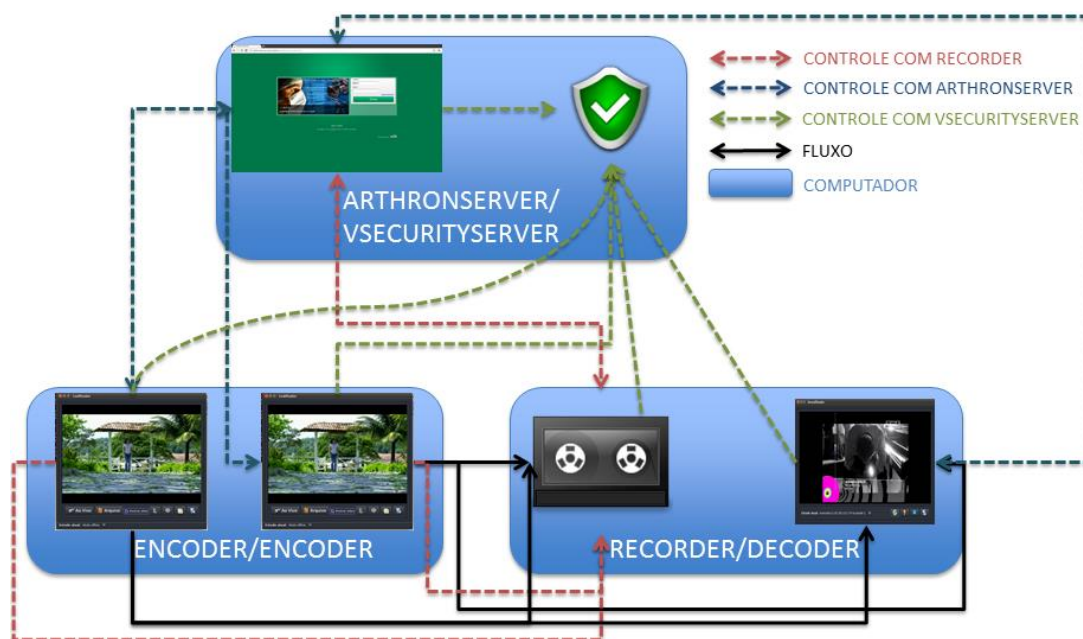


Figura 68. Demonstração 1 no WRNP 2012

A Demonstração 2 consistiu da recuperação da experiência gravada na Demonstração 1. Isso foi possível através da autenticação de um sujeito no ArthronServer e fazendo uma solicitação dos vídeos gravados ao módulo Recorder que, por sua vez, faz o processo de verificação da autenticidade do sujeito solicitante no VSecurityServer e a posterior liberação do fluxo para recuperação. A Figura 69 ilustra essa demonstração.

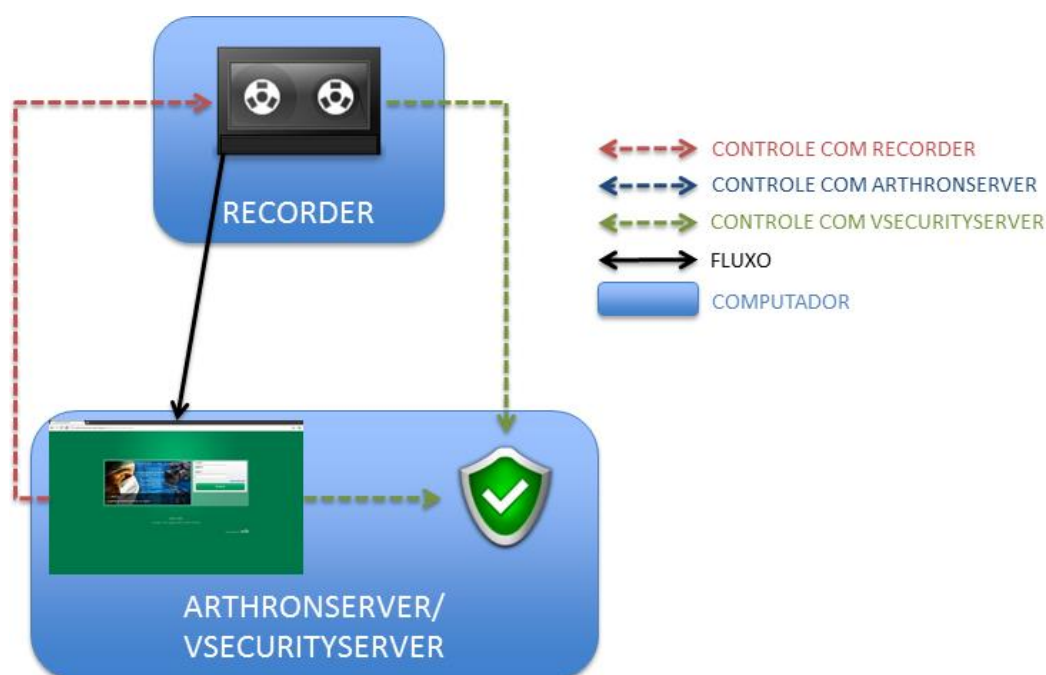


Figura 69. Demonstração 2 no WRNP 2012

A Demonstração 3 consistiu na integração com o GT Cinema, onde um Encoder no modo off-line capturava um fluxo de uma câmera ou arquivo e enviava esse fluxo para o Video Wall montado pelo outro GT que fazia sua exibição. Essa demonstração foi feita utilizando o *streamer*, desenvolvido pelo GT, denominado *Fogo Streamer*, integrado a Arthron. Esse *streamer* capturava a mídia e enviava um fluxo para o refletor, que redistribuía para o Video Wall. A Figura 70 ilustra essa demonstração.

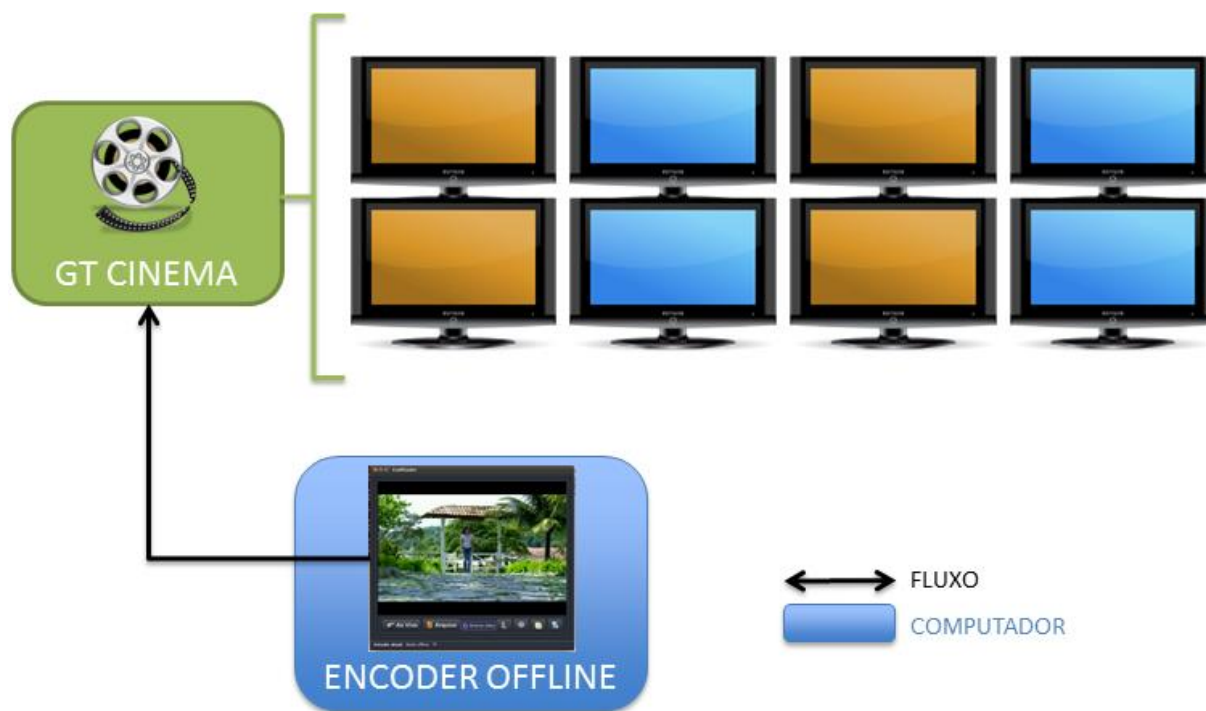


Figura 70. Demonstração 3 no WRNP 2012

Os resultados práticos dessa demonstração podem ser visualizados na Figura 71 que mostra o Video Wall do GT Cinema exibindo três fluxos oriundos do GTAVCS e uma imagem da logomarca do LAViD. As imagens são, respectivamente:

- Fluxo ao vivo;
- Fluxo da demonstração de Bruno Maia com os sensores integrados à Arthron
- Logomarca do LAViD
- Fluxo com uma entrevista com Dr. Geraldo Almeida, parceiro no HULW;



Figura 71. Video Wall do GT Cinema exibindo fluxos do GTAVCS no WRNP 2012

7.3 Publicações

Desde o início desse trabalho seis publicações foram obtidas em que tem a estratégia como parte do trabalho e duas foram especificamente sobre a estratégia. São elas:

- VIEIRA, E.; SOUZA, G.; NEVES, H.; FERREIRA, A.; MELO, E.; TAVARES, T. A. ; MOTTA, G.; SOUZA FILHO, Guido Lemos de. ISM 2012. A Strategy of Multimedia Reflectors to Encryption and Codification in Real Time. In: IEEE International Symposium on Multimedia 2012, 2012, Irvine, California USA.
- OLIVEIRA, S. S.; SANTOS, B. A.; VIEIRA, E.; PASSOS, M. G.; MELO, E. A. G.; MOTTA, G. H. M. B.; TAVARES, T. A.; SOUZA FILHO, Guido Lemos de . Experiência de Uso da Arthron na Transmissão de Cirurgias em Tempo-Real para Telemedicina. In: XII Workshop de Informática Médica, 2012, Curitiba. Anais do XII WIM, 2012.
- VIEIRA, E. ; PASSOS, M. ; SANTOS, B. A. ; OLIVEIRA, S. S. ; MELO, E. A. ; MOTTA, G. H. M. B. ; TAVARES, T. A. ; SOUZA FILHO, Guido Lemos de . Uma Ferramenta para Gerenciamento e Transmissão de Fluxos de Vídeo em

Alta Definição para Telemedicina. In: Salão de Ferramentas do Simpósio Brasileiro de Redes de Computadores 2012, 2012, Ouro Preto. Anais do Salão de Ferramentas do Simpósio Brasileiro de Redes de Computadores 2012, 2012. v. 1.

- SILVA, J. C. F. ; FERREIRA, A. ; VIEIRA, E. ; PASSOS, M. ; MELO, E. A. ; TAVARES, T. A. ; SOUZA FILHO, Guido Lemos de . Utilizando a Arthron para o Gerenciamento Remoto de Múltiplos Fluxos de Mídia. In: Patricia Vilain e Valter Roesler. (Org.). Tópicos em Banco de Dados, Multimídia e Web. 1 ed. Florianópolis: Sociedade Brasileira de Computação, 2011, v. 1, p. 149-178. Referências adicionais: Brasil/Português; Meio de divulgação: Impresso; Série: 1; Número da revisão: 1; ISBN: 9788576692653.
- VIEIRA, E. ; FERREIRA, A. ; SILVA, J. C. F. ; PASSOS, M. ; MELO, E. A. ; MOTTA, G. H. M. B. ; TAVARES, T. A. ; SOUZA FILHO, Guido Lemos de . Estratégia de Segurança para Transmissão de Fluxos de Mídia em Alta Definição. In: Simpósio Brasileiro de Sistemas Multimídia e Web. WebMedia 2011, 2011, Florianópolis. Anais do Simpósio Brasileiro de Sistemas Multimídia e Web, 2011.
- TAVARES, T. A. ; FERREIRA, A. ; VIEIRA, E. ; SILVA, J. C. F. ; MELO, E. A. ; MOTTA, G. H. M. B. . A TOOL FOR VIDEO COLLABORATION IN HEALTH. In: IADIS WWW/Internet 2011, 2011, Rio de Janeiro. Proceedings of IADIS WWW/Internet, 2011.
- SILVA, J. C. F. ; VIEIRA, E. ; PASSOS, M. ; MELO, E. A. ; MOTTA, G. H. M. B. ; TAVARES, T. A. ; SOUZA FILHO, Guido Lemos de . Uma Ferramenta para Vídeo Colaboração em Saúde. In: Congreso Argentino de Informática y Salud 2011, 2011, Córdoba – Argentina. Proceedings of CAIS 2011, 2011.
- SILVA, J. C. F. ; FERREIRA, A. ; VIEIRA, E. ; PASSOS, M. ; MELO, E. A. ; TAVARES, T. A. ; MOTTA, G. H. M. B. ; SOUZA FILHO, Guido Lemos de . A Multi-Stream Tool to Support Transmission in Surgery Applied to Telemedicine. In: International Workshop on Health and Social Care Information Systems and Technologies – HCIST2011, 2011, Algarve – Portugal. Proceedings of HCIST2011, 2011

7.4 Licenciamento

O licenciamento dos produtos e serviços desenvolvidos oriundos de pesquisas, principalmente nas universidades, raramente é levado em consideração ou feito qualquer levantamento, mas é um ponto chave que define as regras de utilização do trabalho por terceiros. Diante disso, foi feito um estudo sobre as bases desse trabalho para se ter um levantamento das licenças utilizadas diretamente e o objetivo é poder inferir a licença final da estratégia.

Dentre todas as bibliotecas utilizadas, o Stylo é a única que não tem licença definida, portanto o mesmo processo foi repetido nesse framework para poder ter uma conclusão sobre sua licença.

A estratégia faz uso de diversas bibliotecas que tiveram suas licenças pesquisadas e definidas, o que permite fazer uma análise e definição da licença da estratégia em si. O resultado desse estudo pode ser visualizado na Figura 72.

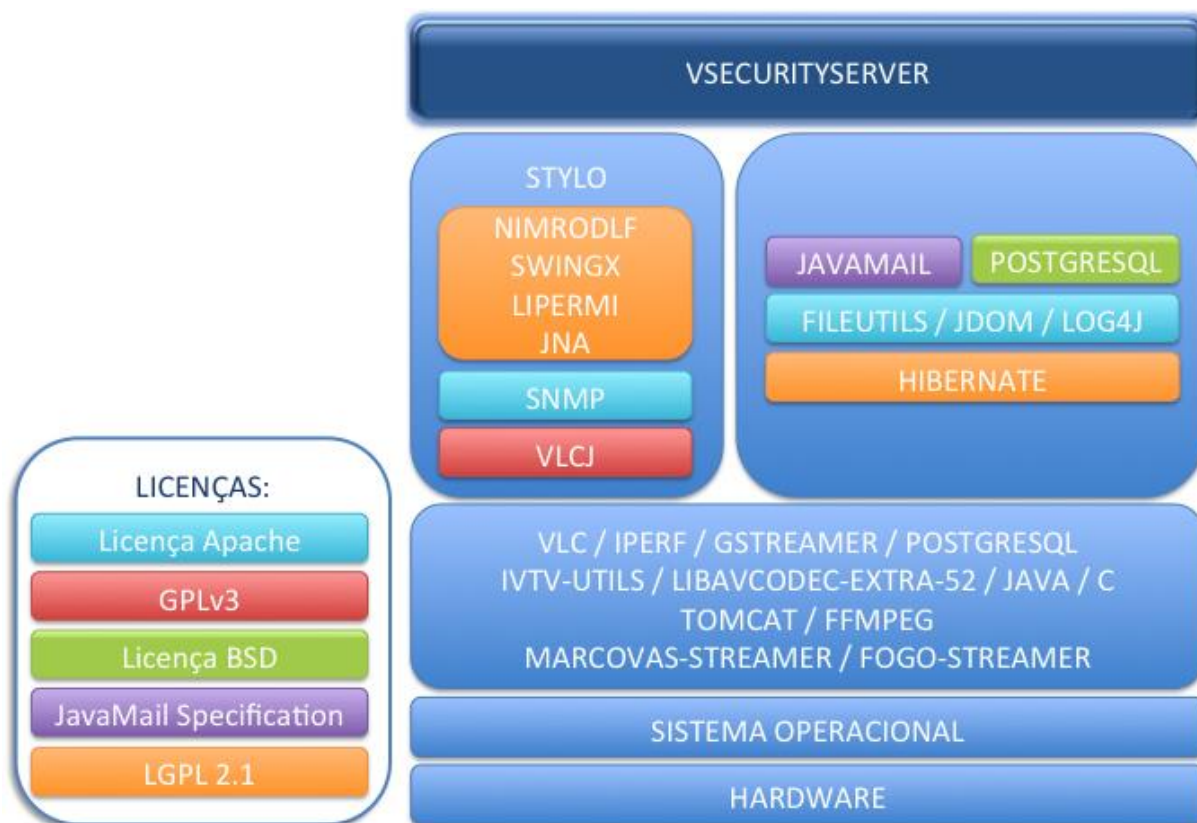


Figura 72. Bibliotecas e licenças utilizadas pela Estratégia

CAPÍTULO 8: CONSIDERAÇÕES FINAIS

O mapeamento sistemático forneceu resultados úteis para fundamentação da pesquisa, além de ter direcionado o trabalho em alguns pontos e contribuído para ilustrar pontos que puderam ser explorados. Nem todos os pontos expostos pelo mapeamento puderam ser contemplados, o que abre lacunas para possíveis trabalhos futuros preencherem e gerarem contribuição para a ciência e publicações para o pesquisador.

A análise das 27 publicações resultantes do mapeamento, aliada às respostas obtidas, servem de base para o surgimento de novas técnicas tanto para a criptografia na transmissão, seja ela *multicast*, *broadcast* ou *multiple unicast*, quanto para a distribuição de chaves para os membros do grupo em questão. Foi possível observar que muitos autores criaram algoritmos próprios baseados em algum outro. Um ponto que pode ser grande importância é a análise desses algoritmos com o objetivo de encontrar a melhor técnica para o emprego em algum desses contextos, o que poderia gerar um Artigo de Experiência ou um Artigo de Opinião, lacuna ainda não explorada na literatura no contexto apresentado.

Outro fator de grande importância é a pouca preocupação com a transmissão multimídia em tempo real, visto que essa área está em contínua expansão principalmente com a popularização dos dispositivos móveis. Poucos autores dos trabalhos obtidos do mapeamento levaram isso em consideração e a maioria sequer cita qual o contexto em que sua pesquisa poderia ser aplicada, deixando para o leitor tirar suas próprias conclusões.

A utilização de codificação influenciou bastante nos resultados dos testes, ao contrário da presença e ausência de criptografia, que apresentou uma variação de processamento bem menos significativa, ou seja, a criptografia não consome tanto processamento, mas sim a codificação. Para a utilização de múltiplas codificações, faz-se necessário que o FullAESHybridReflectorJ tenha a sua disposição um alto poder de processamento, suficiente para a sua demanda, visto que, conforme observado nos resultados, só o padrão H.264 já faz um grande aumento dessa demanda. Uma estratégia é fazer a distribuição desse processamento entre vários refletores em várias máquinas diferentes o que viabiliza sua utilização em computadores menos robustos.

É possível pressupor que a aplicação dos refletores também é destinada para centros de distribuição de vídeo com computadores mais robustos que a máquina que executou os testes descritos, portanto pode-se induzir que o Refletor atingirá um desempenho adequado ao seu escopo proposto. Mesmo assim pode-se observar na execução dos testes que os valores apresentados são aceitáveis para utilização em um computador pessoal.

A criação do VSecurityServer como *web service* possibilita a sua utilização por distintas aplicações e sua aplicação na Arthron supriu as necessidades mínimas exigidas para prover uma transmissão e troca de dados segura, principalmente na distribuição de chaves de criptografia a serem utilizadas pelos refletores. Foi possível fazer a integração com a CAFE o que contribuiu para que a Arthron tenha se tornado um serviço da RNP e que o GTAVCS fase 2 tenha sido aprovado para uma fase 3.

8.1 Trabalhos Futuros

Há muitos rumos que a continuação dessa pesquisa pode ter. Dentre elas, encontra-se a inserção de novas técnicas de criptografia que sejam mais eficientes que a criptografia total utilizando AES, como a utilização de criptografia seletiva e algoritmos de criptografia baseados na *Chaos Theory*, com o objetivo de diminuir o retardo inserido pela criptografia.

Outro ponto que merece mais atenção é a geração de uma nova chave de Sessão Colaborativa sempre que um usuário entrar ou sair. Esse é um ponto crítico visto que esse procedimento pode acarretar que, pacotes de vídeo ainda em trânsito para o destino criptografados com uma chave não possam ser decriptografados porque, quando chegarem ao final, a chave já tenha mudado. Será preciso, por exemplo, que os membros do grupo guardem um histórico das chaves e inserir um identificador de qual chave o pacote foi criptografado, para que a decriptografia seja feita corretamente. Isso irá inserir dados a serem transmitidos e, conseqüentemente, irá gerar um atraso na transmissão e o custo benefício precisa ser analisado. Esses levantamentos precisam ser investigados para uma possível inserção na estratégia ou não.

Como parte dos trabalhos, está a elaboração de um resumo do trabalho que possa ser publicado em um dos principais meios de publicação que foram mostrados

nos resultados do mapeamento sistemático. Por fim uma investigação sobre a geração e distribuição de chaves de sessão de forma não centralizada indicaria se essa solução se aplica no contexto.

REFERÊNCIAS

- AES. Disponível em: <<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>>. Acesso em: 3 fev. 2011.
- ANDREEV, K. et al. Designing overlay multicast networks for streaming. In: Proceedings of the fifteenth annual ACM symposium on Parallel algorithms and architectures. 2003.
- ASGHAR, M. SADAF, S. EIDI, K. NASEEM, A. NAWOOD, S. A Secure Scheme for Video Streaming Using SRTP AES and DH. In: European Journal of Scientific Research. 2010.
- BELL, D. LA PADULA, L. Secure computer system: Unified Exposition and Multics Interpretation. MITRE Report, ESD-TR-75-306. 1976.
- CAFE. Comunidade Acadêmica Federada. Rede Nacional de Ensino e Pesquisa. Disponível em: <<http://www.rnp.br/servicos/cafe.html>>. Acesso em: 27 jun. 2012.
- CHALLAL, Y., BOUABDALLAH, A., BETTAHAR, H. H2A: Hybrid Hash-chaining scheme for Adaptive multicast source authentication of media-streaming. In: Computers & Security Journal. 24 v, p. 57-68. DOI= 10.1016/j.cose.2004.06.012. 2005.
- CHAPMAN, Nigel e Chapman, Jenny. Digital Multimedia.s.l. : John Wiley & Sons, 2000.
- CULTURA. Ministério da Cultura. Disponível em: <<http://www.cultura.gov.br/site/2009/11/09/como-ter-cultura-se-90-das-cidades-nao-tem-um-cinema/>>. Acesso em 14 jul. 2012.
- DEBIAN. Disponível em: <<http://www.debian.org/>>. Acesso em: 28 jun. 2012.
- DONDETI, L. R. MUKHERJEE, S. SAMAL, A. "Scalable secure one-to-many group communication using dual encryption", Computer Communications 23, p. 1681–1701. 2000.
- DONDETI, L.R., MUKHERJEE, S., SAMAL, A. Scalable secure one-to-many group communication using dual encryption. In: Computer Communications Journal . 23 v. p. 1681–1701. 2000.
- DWORKIN, M. Recommendation for Block Cipher Modes of Operation. NIST Special Publication 800-38^a. 2001. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf>. Acesso em: 05 maio 2012.
- ECLIPSE. Disponível em: <<http://www.eclipse.org/>>. Acesso em: 28jun. 2012.
- FAN, W. DENG, M. HUANG, W. A Novel Scheme for HD Video Stream Encryption. In: International Conference on System Science, Engineering Design and Manufacturing Informatization. Guiyang, China. 2011.
- GT CINEMA. Grupo de Trabalho de Visualização Remota – GT Cinema. Disponível em: <<http://wiki.rnp.br/pages/viewpage.action?pageId=47547370>>. Acesso em: 29 jun. 2012.

- GTMDA. Grupo de Trabalho de Mídias Digitais e Artes. Disponível em: <<http://www.lavid.ufpb.br/gtmda>>. Acesso em: 4 jul. 2012.
- HANKERSON, D., MENEZES, A., VANSTONE, S. A. Guide to Elliptic Curve Cryptography, Springer, Berlin, 2004.
- HOLEMAN, S., MANIMARAN, G., DAVIS, J., CHAKRABARTI, A. Differentially secure multicasting and its implementation methods. Computers & Security Vol 21, No 8, pp736-749, 2002.
- HTTP. NETWORK WORKING GROUP: Hypertext Transfer Protocol. Disponível em: <<http://www.ietf.org/rfc/rfc2616.txt>>. Acesso em: 27 jun. 2012.
- INTERNET2. RNP (Brasil). Disponível em: <<http://www.rnp.br/redes/internet2.html>>. Acesso em: 5 jun. 2012.
- IPÊ. Rede Ipê. Rede Nacional de Ensino e Pesquisa. Disponível em: <<http://www.rnp.br/backbone/>>. Acesso em 14 jul. 2012.
- JAIN, R. K. Art of Computer Systems Performance Analysis Techniques For Experimental Design Measurements Simulation And Modeling. Wiley Computer Publishing, John Wiley & Sons, Inc. 1991.
- JAVA. Disponível em: <http://www.java.com/pt_BR>. Acesso em: 28 jun. 2012.
- JAVAMAIL. Disponível em: <<http://www.oracle.com/technetwork/java/javamail/index.html>>. Acesso em: 28 jun. 2012.
- JNI. Disponível em: <<http://java.sun.com/docs/books/jni/>>. Acesso em: 28 jun. 2012.
- LIAN, S. Quasi-commutative watermarking and encryption for secure media content distribution. In: Multimedia Tools and Applications Journal. 43 v. p. 91–107. DOI 10.1007/s11042-008-0258-4. 2009.
- LIAN, S. LIU, Z. REN, Z. WANG, H. Secure Advanced Video Coding Based on Selective Encryption Algorithms. In: IEEE Transactions on Consumer Electronics. 52(2) v, p. 621-629. 2006.
- LIMA, Claudio Marcio Amaral de Oliveira et al. Videoconferências: sistematização e experiências em telemedicina. RadiolBras, 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.
- LOG4J. Disponível em: <<http://logging.apache.org/log4j/>>. Acesso em: 28 jun. 2012.
- 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.
- 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. 2010a. Gramado, RS.
- MELO, E. A. G. Uma Ferramenta para Gerenciamento e Transmissão de Mídias em Performances Artístico-Tecnológicas. Universidade Federal da Paraíba. João Pessoa, Paraíba. 2010b.

- MOU, L., HUANG, T., HUO, L., LI, W., GAO, W., CHEN, X. A Secure Media Streaming Mechanism Combining Encryption, Authentication and Transcoding. Signal Processing: In: Image Communication Journal. 24 v. p. 825–833. DOI= 10.1016/j.image.2009.03.001.2009.
- NETBEANS. Disponível em: <<http://netbeans.org>>. Acesso em: 28 jun. 2012.
- PANDE, A. ZAMBRENO, J. “A chaotic encryption scheme for real-time embedded systems: design and implementation”, Journal of Telecommunication Systems. 2011.
- PETERSEN, K., FELDT, R., MUJTABA, S., MATTSSON, M. Systematic Mapping Studies in Software Engineering. In: 12th International Conference on Evaluation and Assessment in Software Engineering (EASE). 2008.
- POSTGRESQL. Disponível em: <<http://www.postgresql.org.br/>>. Acesso em: 28 jun. 2012.
- ROSARIO, G., PANKAJ, R. How to sign digital streams. In: Advances in cryptology, CRYPTO'97. 1997.
- ROSARIO, G., PANKAJ, R. How to sign digital streams. In: Information and Computation. 165 v. p. 100-116. 2001.
- RSA. Disponível em: <<http://people.csail.mit.edu/rivest/Rsapaper.pdf>>. Acesso em: 20 jan. 2011.
- RSTP.NETWORK WORKING GROUP. Real Time Streaming Protocol (RTSP). Disponível em: <<http://www.ietf.org/rfc/rfc2326.txt>>. Acesso em: 27 jun. 2012.
- RTP. NETWORK WORKING GROUP: A Transport Protocol for Real-Time Applications. Disponível em: <<http://tools.ietf.org/pdf/rfc1889.pdf>>. Acesso em: 27 jun. 2012.
- RUTE. Disponível em: <<http://rute.rnp.br/>>. Acesso em: 14 mai. 2011.
- SANDOSH, S. AKILA, V. UTHAYASHANGAR, S. Secure Decentralized Group Key Management through Progressive Approach. In: International Journal of Computer Applications. 9 v. n.10, Nov. 2010.
- SBRC. Simpósio Brasileiro de Redes de Computadores. Disponível em: <<http://sbrc2012.dcc.ufmg.br>>. Acesso em 4 jul. 2012.
- SILVA, J. C. F. PASSOS, M. TAVARES, T. A. LEMOS, G. S. F. STYLO: Um Framework Voltado para o Desenvolvimento de Aplicações Baseadas em Vídeo Digital. In: Workshop de Teses e Dissertações do WebMedia 2011, Florianópolis. Anais do Simpósio Brasileiro de Sistemas Multimídia e Web, 2011.
- SSL. Secure Sockets Layer. Disponível em: <<http://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00>>. Acesso em: 5 jul. 2012.
- STALLINGS, William. Criptografia e segurança de redes – 4. ed. – São Paulo: Pearson Prentice Hall, 2008.
- STCFED. Grupo de Trabalho Serviços para Transposição de Credenciais de Autenticação Federadas. Disponível em: <http://www.rnp.br/pd/gts2010-2011/gt_stcfed2.html>. Acesso em: 5 jul. 2012.

- TOMCAT. Disponível em: <<http://tomcat.apache.org/>>. Acesso em: 28 jun. 2012.
- TS. Transport Stream. Disponível em: <<http://www.ietf.org/proceedings/51/slides/avt-7/sld004.htm>>. Acesso em: 29 jun. 2012.
- UBUNTU. Disponível em: <<http://ubuntu-br.org/>>. Acesso em: 28 jun. 2012.
- UDP. NETWORK WORKING GROUP: User Datagram Protocol. Disponível em: <<http://tools.ietf.org/html/rfc768>>. Acesso em: 27 jun. 2012.
- VIEIRA, E. ; FERREIRA, A. ; SILVA, J. C. F. ; PASSOS, M. ; MELO, E. A. ; MOTTA, G. H. M. B. ; TAVARES, T. A. ; SOUZA FILHO, Guido Lemos de . Estratégia de Segurança para Transmissão de Fluxos de Mídia em Alta Definição. In: Simpósio Brasileiro de Sistemas Multimídia e Web. WebMedia 2011, Florianópolis. Anais do Simpósio Brasileiro de Sistemas Multimídia e Web, 2011.
- VIEIRA, E. S. F.; PASSOS, M. ; SANTOS, B. A. ; OLIVEIRA, S. S. ; MELO, E. A. ; MOTTA, G. H. M. B. ; TAVARES, T. A. ; SOUZA FILHO, Guido Lemos de . Uma Ferramenta para Gerenciamento e Transmissão de Fluxos de Vídeo em Alta Definição para Telemedicina. In: Salão de Ferramentas do Simpósio Brasileiro de Redes de Computadores. Ouro Preto, 2012.
- VLC. VideoLAN Client Media Player. Disponível em: <www.videolan.org/vlc/>. Acesso em: 14 maio de 2012.
- WEBSERVICE. Disponível em: <<http://www.w3.org/2002/ws/>>. Acesso em: 28 jun. 2012.
- WIERINGA, R. MAIDEN, N. A. M. MEAD, N. R. ROLLAND, C. Requirements engineering paper classification and evaluation criteria: a proposal and a discussion. Requirements Eng. p. 102–107. 2006.
- WRNP. Workshop da Rede Nacional de Ensino e Pesquisa. Disponível em: <<http://wrnp.rnp.br>>. Acesso em 29 jun. 2012.
- W6ZR, 2012. Disponível em: <<http://www.w6rz.net>>. Acesso em: 15 nov. 2012.
- ZHANG, F. LI, B. Medical Video Stream Transmission in Telemedicine. In: IEEE International Conference on Automation and Logistics. Jinan, China. 2007.
- ZHU, S., YAO, C., LIU, D., SETIA, S., JAJODIA, S. Efficient security mechanisms for overlay multicast based content delivery. In: Computer Communications Journal.p. 793–806. DOI=10.1016/j.comcom.2006.10.003. 2007.