Autenticação Biométrica em Redes de Telecomunicação Aeronáutica

Rafael de Amorim Silva[1,2], **Angelo Zanini**[1]

[1]Departamento de Eletrônica - Instituto Tecnológico de Aeronáutica (ITA)
– São Jose dos Campos – SP – Brasil

{amorim,azanini}@ita.br

[2]Instituto de Computação
Universidade Federal de Alagoas (UFAL) – Maceió, AL – Brasil

rafael@ic.ufal.br

Abstract. *This paper proposes a network architecture that supports biometric authentication on aeronautical networks to provide more confident services related to air passenger communication. The chosen authentication process is the single logon. This architecture is based on overlay protocol between application and transport layers, obtaining agents that negotiate the authentication process. As a result, the architecture enables the development of various applications to assure information trafficked by aeronautical networks.*

Resumo. *Este artigo propõe uma arquitetura de rede que auxilie a autenticação biométrica em redes aeronáuticas para prover serviços mais confiáveis relacionados a comunicação para passageiros aéreos. O processo de autenticação adotado é o* single logon*. A arquitetura é baseada em um protocolo overlay entre as camadas de aplicação e transporte, possuindo agentes que negociam o processo de autenticação. Como resultado, a arquitetura permite o desenvolvimento de diversas aplicações para assegurar a informação trafegada em redes aeronáuticas.*

1. Introdução

Uma rede de telecomunicação aeronáutica é capaz de se comunicar com uma aeronave através de vários tipos de enlace de dados (e.g. satélites, comunicações aéreo-aéreo e aéreo-terrestres) [1]. Tais redes são projetadas para trabalhar com aplicações que exijam um alto nível ou baixo nível de segurança. A rede ATN oferece quatro tipos de serviços [2]: (i) sistema de tráfego aéreo (ATS); (ii) Controle operacional aéreo(AOC); (iii) Controle administrativo das linhas aéreas (AAC); e (iv) comunicação de passageiros aéreos (APC). Os serviços ATS e AOC exigem um forte nível de segurança, usados geralmente em comunicações operacionais. Já os serviços APC e AAC exigem baixos requisitos de segurança, usados geralmente em comunicações não operacionais.

Inicialmente, a indústria tem adotado o modelo OSI para comunicações aeronáuticas. Entretanto, iniciativas como o projeto NEWSKY [3] propõe a migração do modelo OSI para o modelo TCP/IP, ofertando uma nova geração de tecnologias que serão empregadas para uso aeronáutico. Embora hajam esforços na direção de uma rede de telecomunicação aeronáutica baseada na pilha atual da Internet, tal modernização ainda se

encontra em estágio inicial. Diversas aplicações serão desenvolvidas devido a aquisição deste novo padrão. Alguns trabalhos [4, 5] têm proposto alternativas para aumentar a segurança à nível de arquitetura para estas redes. Todavia, existem poucos trabalhos que lidem com aspectos relacionados a segurança das aplicações neste novo cenário aeronáutico. A arquitetura TCP não oferece a segurança adequada para o processo de autenticação, sendo que problemas como erros em canal, excessivos *handoffs*, falta de conectividade podem dificultar o uso de algoritmos de segurança. Para resolver tal problema, uma aplicação que captura uma credencial biométrica e a distribui para as estações aéreo-terrestres programadas em um plano de vôo estabelece comodidade para o usuário e aumenta o desempenho na rede.

Portanto, este artigo propõe uma arquitetura de rede projetada para suportar a autenticação biométrica em redes de telecomunicação aeronáutica que implementem serviços APC. Tal arquitetura oferece um protocolo *overlay* entre as camadas de aplicação e transporte, com agentes responsáveis na realização do processo de autenticação. Dentre os benefícios esperados, tal arquitetura propicia o desenvolvimento de inúmeras aplicações para a segurança de dados dos usuários que viajam em uma aeronave.

O trabalho é organizado da seguinte maneira: Na Seção 2 são apresentados alguns trabalhos relacionados. A Seção 3 apresenta as principais técnicas da autenticação biométrica. A Seção 4 descreve a arquitetura proposta neste trabalho, descrevendo o cenário, a pilha de protocolos e a arquitetura de agentes envolvida. A Seção 5 apresenta um estudo de caso para avaliar a arquitetura, definindo alguns exemplos de aplicações que se beneficiam da implantação desta arquitetura. A Seção 6 apresenta as considerações finais deste trabalho.

2. Trabalhos Relacionados

O projeto NEWSKY [3] foi pioneiro no desenvolvimento e análise da nova geração de tecnologias baseadas no modelo ATN/IPS que serão empregadas no cenário aeronáutico nos próximos anos. O escopo desta investigação inclui a rede aéreo-terrestre, considerando apenas os serviços que exijam um alto nível de segurança. Além do projeto NEWSKY, outros autores em [10] também propuseram arquiteturas de rede aeronáutica baseados no padrão ATN/IPS para comunicações aéreo-terrestres. Estes autores discutem problemas relacionados a mobilidade, segurança e integração em arquiteturas ATN. Autores em [10] investigam a aplicação da tecnologia Mobile IP em programas aeronáuticos e da agência espacial norte-americana, discutindo as características, capacidades e possíveis cenários de uso. Em particular, estes autores investigam a conectividade IPv4 e IPv6 entre *hosts* fixos e móveis através de *testbeds*. As questões relativas a segurança destas redes são discutidas em [4, 5].

3. Autenticação Biométrica

Identificação pessoal é o processo de associar um indivíduo particular a uma identidade. Tal identificação pode ser tanto na forma de verificação (autenticação), o qual autentica uma identidade exigida, ou reconhecimento (identificação), que determina a identidade de uma pessoa através da consulta de um banco de dados de pessoas conhecidas no sistema. Para identificar automaticamente uma pessoa, usa-se algo que ela possua em mãos (abordagem baseada em tokens), ou usa-se algo que ela saiba (abordagem baseada em conhecimento), ou usa-se alguma característica fisiológica ou comportamental (abordagem

baseada em biometria). A abordagem biométrica tem se destacado devido a sua capacidade de identificar, com maior probabilidade, a pessoa correta para autorização de acesso e recursos em um determinado sistema. As outras abordagens possuem uma capacidade inferior de identificar corretamente um usuário, pois os tokens podem ser perdidos, roubados, esquecidos, ou deixados em algum lugar. Além disso, um PIN pode ser esquecido ou pego por um impostor, falhando em distinguir entre uma pessoa autorizada e um impostor.

O processo de identificação em um sistema biométrico é dividido em duas etapas: (i) captura de uma característica biométrica através de um sensor e armazenada em um banco de dados para futuras comparações (conhecida como etapa de cadastramento das credenciais biométricas); (ii) processo de comparação em tempo real de ambas as credencias (etapa de comparação). Na fase de cadastramento, a característica biométrica é escaneada por um sensor biométrico para adquirir a representação digital da característica. Depois, a representação digital é processada por um extrator de características para gerar uma representação expressiva e compacta (*template*). Este *template* pode ser armazenado ou em um banco de dados central ou em um cartão magnético (local). Na fase de reconhecimento, o leitor biométrico captura a característica do indivíduo e converte-o a um formato digital. Depois, processa-se essa captura pelo extrator de características para produzir a mesma representação como o *template*. Por último, a representação resultante é passada ao extrator de característica que compara-o novamente com o *template* para estabelecer a identidade do indivíduo [6].

Para a escolha adequada de uma determinada característica biométrica, deve-se levar em conta os seguintes fatores: universalidade, distinção, permanência, coletabilidade, desempenho, aceitabilidade e circumvenção [7].

3.1. Métodos de Autenticação Biométrica

Existem vários métodos para a captura de uma característica biométrica. Tais métodos se diferenciam através dos fatores de escolha citados na Seção 3. Estes métodos são: Reconhecimento de Face, Termograma Facial, Geometria das Mãos, Reconhecimento por Íris, Assinatura Humana, Fala Humana, Reconhecimento por Retina, Veias da Palma da Mão e Impressão Digital [7, 8].

A identificação biométrica por reconhecimento da face humana é uma das mais comuns características utilizadas para identificação pessoal. Tal identificação é baseada na localização e na forma de atributos como olhos, nariz, lábios, sobrancelhas, queixo e seus relacionamentos espaciais. Tal identificação é adotada por aplicações que funcionam em ambientes controlados ou fundos com imagem distorcida (e.g. identificação de presos e criminosos). Este modo de identificação requer iluminação especial, sendo de difícil reconhecimento caso a captura da imagem não tenha sido obtida pelo ângulo original da imagem.

O sistema de vasos sanguíneos existentes no lado interno da face permite a identificação de um indivíduo através de assinaturas faciais, devido a passagem de calor através do tecido facial. Por isso, um termograma facial identifica assinaturas faciais através dessa passagem, utilizando câmeras infra-vermelhas que capturam minúcias deste sistema. Tal método de identificação identifica unicamente uma característica do indivíduo e não é vulnerável a quaisquer tipos de disfarces. A estrutura vascular é mais rica em informação, fornecendo minúcias mesmo em ambientes com pouca iluminação.

O problema principal desta técnica é que é suscetível a mudanças de temperatura, estado emocional do indivíduo e ângulo da imagem obtida.

A técnica de identificação biométrica pelo uso da geometria das mãos humanas consiste em considerar a forma da mão, alturas e tamanhos dos dedos como característica biométrica. A técnica é simples, de fácil uso e bom custo-benefício. Fatores como umidade e pele úmida não influenciam na eficácia desta técnica. Todavia, a mesma possui baixa capacidade discriminativa. Outro problema é que a geometria da mão muda ao longo da vida, oferecendo uma baixa permanência da característica biométrica. Outros fatores como o uso de jóias e artrites podem dificultar a identificação.

A técnica de identificação biométrica pelo uso da íris é uma das técnicas mais eficazes, devido a sua longa permanência (a textura visual da íris estabiliza durante os dois primeiros anos de vida) e sua unicidade. Além disso, a característica biométrica é mais fácil de capturar do que a técnica de reconhecimento por retina. Dentre as suas vantagens, destacam-se a sua segurança, visto que é difícil cirurgicamente danificar a sua textura e a facilidade em detectar íris superficiais (fraudulentas).

A assinatura é o método mais tradicional de reconhecer a autenticidade de um indivíduo. Cada indivíduo possui um estilo único de assinatura, sendo que duas assinaturas deste mesmo indivíduo são geralmente idênticas. As variações dependem do seu estado físico e emocional. Existem 2 modos de identificação: Estática e dinâmica. O primeiro utiliza apenas características geométricas de uma assinatura. O segundo adota as características do primeiro e acrescenta fatores como aceleração, velocidade, pressão e trajetórias da assinatura.

A fala humana pode ser utilizada para identificação biométrica. O som característico de cada indivíduo é formado por diferenças na fala devido a fatores como forma ou tamanho invariante do trato vocal, boca, cavidades nasais e lábios. A verificação pode ser feita pelo uso de um texto (o individuo deve ler o texto e a comparação entre o texto falado e o armazenado em uma base de dados será realizado) ou independente de texto (o que oferece maior proteção contra fraudes). A aceitabilidade por parte dos usuários é excelente. Fatores como ruídos, estado físico e emocional do indivíduo pode influenciar em um baixo desempenho da técnica. Geralmente, tal técnica é adotada em aplicações com baixos requisitos de segurança devido a alta variabilidade existente na voz.

A técnica de identificação biométrica pelo reconhecimento retinal se caracteriza pelo uso de informações capturadas das veias que se situam abaixo da superfície retinal em um olho. O dispositivo de captura biométrica projeta um feixe com baixa intensidade visual em um olho para capturar uma imagem da retina. Portanto, o indivíduo deve se aproximar do dispositivo e direcionar a sua visão para um determinado ponto no campo visual. O problema desta técnica é que é intrusiva e de alto custo. Dentre as suas vantagens, a técnica oferece uma característica única em cada indivíduo e é estável.

A técnica de identificação biométrica pelo padrão das veias de uma palma da mão consiste na identificação de minúcias devido a absorção da luz em determinados comprimentos de onda que uma hemoglobina reduzida possui em relação a hemoglobina oxigenada [8]. Ou seja, emite-se uma luz em direção a uma palma da mão, sendo que uma luz com um determinado comprimento de onda será refletido. Uma vez que há absorção de luz pela hemoglobina reduzida, a luz refletida será identificada por uma câmera de

infravermelho, formando a imagem das veias da palma da mão. Dentre as suas vantagens, o método se apresenta como não invasivo, higiênico e único. Além disso, é uma técnica de difícil fraude e possui capacidade de detecção de vida sem precisar de dispositivos adicionais.

A técnica de identificação biométrica por impressão digital é a mais popular dentre as técnicas. O método consiste em capturar minúcias do padrão de cristas e sulcos na superfície de um dedo. As minúcias detectadas são transformadas em um vetor de características, sendo uma lista de localizações e outros atributos (orientação da curva, por exemplo). Posteriormente, compara-se a identificação biométrica com *templates* armazenados em uma base de dados. A técnica possui baixo custo de implementação. Dentre as desvantagens, as impressões digitais de uma parte da população podem ser inadequadas devido a questões genéticas, envelhecimento, ambientais e ocupacionais.

4. Arquitetura para Autenticação Biométrica em Redes Aeronáuticas

A rede utiliza o conceito de conexões segmentadas (i.e. *split connections* [9]). O usuário envia um pacote pela rede interna do avião até o roteador móvel (localizado na aeronave), responsável pelo acesso ao canal de comunicação aeronáutico. Este roteador deve enviar o pacote para a estação aéreo-terrestre cujo enlace esteja ativo. O agente intermediário irá encerrar esta conexão TCP e iniciar uma nova conexão utilizando outra socket até o *host* destino. A arquitetura de agentes é descrita na Figura 3 e a interação dos protocolos é ilustrada na Figura 2.

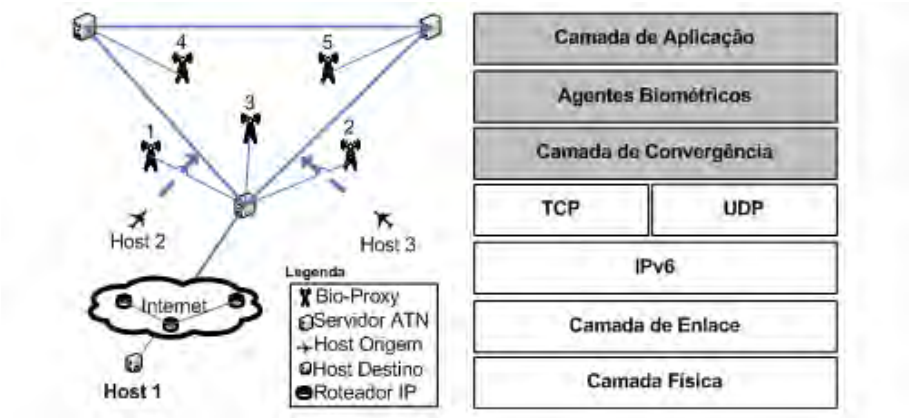

Figura 1. Descrição do cenário aeronáutico e protocolos da arquitetura proposta

4.1. Pilha de Protocolos

A pilha de protocolos é caracterizada pela presença de uma camada *overlay* entre a camada de aplicação e a camada de transporte da pilha TCP/IP, disponibilizando agentes de *software* que realizarão funções de gerenciamento de identidades biométricas. Além dessa camada, deve haver uma camada intermediária (conhecida como adaptador da camada de convergência) responsável pela comunicação entre os protocolos de transporte e a camada *overlay*. A Figura 1(b) ilustra os protocolos e as camadas envolvidas. Os agentes são divididos em quatro tipos: (i) Agente Cliente; (ii) Agente de Captação Biométrica; (iii) Agente Gerenciador; e (iv) Agente Bio-proxy.

O Agente cliente é instalado nas máquinas dos usuários do sistema. Tal agente é responsável pela comunicação com os agentes bio-proxies. Este agente envia informações sobre o o seu estado atual na rede, como a associação a uma nova rede. Tal informação será armazenada pelo agente bio-proxy desta nova rede, permitindo que o agente bio-proxy controle os dados biométricos trafegados durante o período de conectividade entre a aeronave e a estação aéreo-terrestre. Além disso, tal agente verifica se a aplicação atual do cliente necessita de dados biométricos, e envia requisições de permissão do uso de um identificador biométrico por um agente bio-proxy, caso seja necessário.

O Agente de Captação Biométrica é instalado em máquinas específicas nos aeroportos. Tal agente realiza a leitura biométrica através de tecnologias biométricas (leitura de impressões digitais, retina, face, veias da mão, etc) e envia tais credenciais biométricas para o agente gerenciador.

O Agente Gerenciador é responsável pelo uso do plano de vôo para enviar as credenciais para as respectivas estações aéreo-terrestres. Além disso, o mesmo armazena temporariamente tais credenciais, enviados pelo agente de captação biométrica. A medida que a aeronave vai mudando de estação, as credenciais armazenadas em estações anteriores vão sendo apagadas da memória (*buffer*) destas estações. Devido a velocidade de uma aeronave permanecer na maior parte do tempo constante (aproximando a um modelo matemático de movimento uniforme), o agente pode estimar o tempo de duração que a aeronave permanecerá em cada estação existente no plano de vôo. Portanto, o agente pode recalcular caso o plano de vôo sofra alterações devido a tempestades ou outros fenômenos não previstos no vôo.

O Agente bio-proxy é o agente que armazena as credenciais biométricas quando um plano de vôo está sendo realizado. É o agente que se situa nas estações aéreo-terrestres, fazendo o intermédio entre o canal aeronáutico e a rede aeronáutica terrestre. É responsável pela comunicação entre os agentes de mesma natureza. O mesmo se comunica com a aplicação, enviando IDs para o destino quando exigidos.

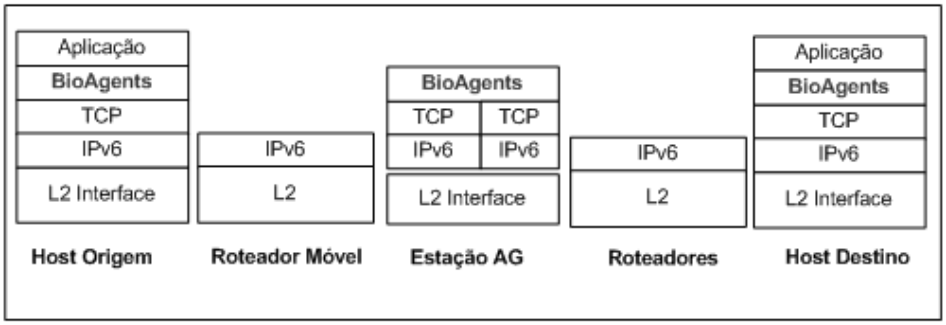

Figura 2. Interação dos Protocolos na Arquitetura Proposta.

O cenário adotado neste trabalho é caracterizado como segue: Em primeiro lugar, cada aeronave possui uma rota definida em um plano de vôo elaborado antes da sua decolagem de um determinado aeroporto. O piloto deve segui-lo corretamente, para que não hajam imprevistos (acidentes). As estações aéreo-terrestres são definidas por áreas, sendo cada área controlada por um servidor ATN. Estes servidores estão conectados en-

tre si através de enlaces ponto a ponto. Observe que, para redes aeronáuticas maiores, a topologia estrela é sugerida. Em cada rota aeronáutica, a aeronave passará por X estações conhecidas. Um dos servidores atua como gateway, disponibilizando acesso a Internet para toda a rede.

Figura 3. Arquitetura de Agentes de Software do Protocolo Overlay.

5. Estudo de Caso

Antes de viajar, o usuário deve se autenticar em um aeroporto. Sua credencial biométrica será enviada para as estações aéreo-terrestres que se comunicarão com a aeronave durante a rota definida em um plano de vôo. Tal informação será armazenada e controlada por agentes intermediários conhecidos como bio-proxies. O usuário não precisará mais se autenticar nas aplicações que exigem autenticação, pois o envio da credencial assim como o seu aceite ou rejeite será negociado pelos agentes intermediários. Caso a identificação seja rejeitada, o agente intermediário repetirá a autenticação até um número de tentativas definido em um parâmetro. Caso ainda haja a falha, o agente intermediário comunicará e passará a função de autenticação para a camada de aplicação do usuário.

5.1. Cenários de Aplicação

A autenticação através de nós intermediários auxilia na viabilidade de diversos tipos de aplicação. Dentre as mais significativas, destacam-se:

- *Acesso a instituições Financeiras:* Sites com serviços financeiros tais como bancos, operadoras de cartão de crédito e cooperativas podem se beneficiar da arquitetura proposta neste trabalho. O usuário não precisaria se autenticar nestes sites a cada nova estação aéreo-terrestre, o que implicaria em redução de fluxo de dados na rede e um atraso menor na comunicação entre hosts.
- *Acesso a sites privados:* Devido ao elevado crescimento do comércio eletrônico nos últimos anos, o usuário poderia efetuar suas compras sem se preocupar com o processo de autenticação, visto que o mesmo estaria temporariamente acessível em cada estação aéreo-terrestre.
- *Acesso a documentos compartilhados:* Sites que compartilham documentos podem utilizar as identidades biométricas sem precisar exigir uma nova captura de identidade cada vez que a aeronave mudar de estação aéreo-terrestre.
- *Jogos para Passageiros:* Aplicações como jogos eletrônicos podem utilizar as identidades biométricas capturadas pelos agentes bio-proxies para permitir a sua

continuidade. Ou seja, os usuários podem jogar entre passageiros de outras aeronaves sem precisar autenticar sua identidade nas estações.

- *Acesso a Intranets:* Empresas podem disponibilizar acesso as suas intranets através do uso das identidades biométricas capturadas nos agentes bio-proxies.

6. Considerações Finais

Este artigo propôs uma arquitetura de rede aeronáutica para oferecer serviços relacionados a segurança biométrica. Para tal, desenvolveu-se uma arquitetura de agentes de *software* que realiza o intermédio entre a aplicação do cliente e o servidor de autenticação biométrica. As estações aéreo-terrestres são responsáveis por este intermédio, armazenando a identidade biométrica durante o vôo de uma aeronave convencional que siga um determinado plano de vôo. O agente captura as informações do plano de vôo, e distribui entre os agentes da rota estimada. Como vantagens de obtenção desta arquitetura, o usuário não se preocupa durante o vôo em realizar autenticações biométricas, sendo o agente intermediário responsável por tal atividade. Como atividade futura, pretende-se realizar simulações com simuladores de eventos discretos que investiguem o desempenho desta arquitetura em cenários aeronáuticos.

Referências

[1] Feighery, P. and Hanson, T. and Lehman, T. and Mondrus, A. and Scott, D. and Signore, T. and Smith, R. and Uhl, G., *The Aeronautical Telecommunications Network (ATN) testbed*, Digital Avionics Systems Conference, 15th Edição, 1996.

[2] Jahn, A. and Holzbock, M. and Muller, J. and Kebel, R. and de Sanctis, M. and Rogoyski, A. and Trachtman, E. and Franzrahe, O. and Werner, M. and Hu, F., *Evolution of aeronautical communications for personal and multimedia services*, IEEE Communications Magazine, vol. 41, no. 7, pp. 36-43, 2003.

[3] Schnell, M. and Scalise, S., *NEWSKY Concept for NEtWorking the SKY for Civil Aeronautical Communications*, vol. 22, no 5. IEEE Aerospace and Electronic Systems Magazine, 2007.

[4] Stephens, B., *Security architecture for aeronautical networks*, The 23rd Digital Avionics Systems Conference, 2004.

[5] Ehammer, M. and Graupl, T. and Rokitansky, C.H. and Brikey, T., *Security consideration for IP based aeronautical networks*, 27th Digital Avionics Systems Conference, 2008.

[6] Pankanti, S.; Bolle, R.M.; Jain, A., *Biometrics: The Future of Identification*, IEEE Computer, 2000.

[7] Jain, A., Hong, L., Pankanti, S., *Biometric Identification*. ACM Communications, vol. 43, no. 2, 2000.

[8] Fonseca, J., Zanini, A., *Autenticação Biométrica pelas veias da palma da mão*, Instituto Tecnológico de Aeronáutica, 2009.

[9] Pucha, H. and Hu, Y.C., *Overlay TCP: Ending end-to-end transport for higher throughput*, Poster in ACM SIGCOMM, 2005.

[10] Brooks, D. and Wilkins, R. and Hoder, D. and InfraStruct, I.G. and LLC, W.C. *Mobile IP communications for aeronautical applications*, The 23rd Digital Avionics Systems Conference, DASC, 2004.