Ampliando os sistemas de aeronaves não tripuladas: especificação de uma arquitetura de comunicação de dados segura e com vista à mobilidade

Daniel F. Pigatto[1], Kalinka R. L. J. C. Branco[1]

[1]Instituto de Ciências Matemáticas e de Computação – Univ. de São Paulo (USP)
São Carlos – SP – Brazil

{pigatto,kalinka}@icmc.usp.br

Abstract. *Embedded systems are computer systems that are part of a larger system providing generally monitoring and real-time control for the entire system. They provide a set of pre-defined tasks, usually dedicated to a real time application, and have special requirements. These systems are considered critical when failure events may jeopardize lives or high-value assets. Usually these systems operate with frequent information exchange between the inner parts of the vehicle or between the vehicle with ground stations or also with other vehicles. Due to the fact that they are real-time systems, this communication generally requires low latency and security mechanisms that guarantee the basic requirements of a critical scenario, such as confidentiality, integrity, authenticity and availability of communication channels. Furthermore, there is the concern about the vehicles modules/components safety (also known as "health"), which may present malfunctions, whether intentional (attempted attacks) or not, which can lead to vehicle accidents. Given this increasing need to ensure communication and operation of unmanned vehicles plus the desirable characteristic of increasing connectivity in these scenarios, this project proposes the complete specification of a data communication architecture based on safety and mobility concepts. The principal scenario of development will be the aerial, but we expect to obtain a flexible architecture which will be portable to other scenarios of unmanned vehicles, such as ground and water. The specification of this data communication architecture also contributes to the integration of new heterogeneous aircrafts in the airspace, once the requirements for the certification process are being considered.*

Resumo. *Sistemas embarcados são sistemas computacionais que fazem parte de um sistema maior provendo, geralmente, monitoramento e controle em tempo real para todo o sistema. Eles fornecem um conjunto pré-definido de tarefas, normalmente dedicados a uma aplicação em tempo real, e apresentam requisitos especiais. Estes sistemas são considerados críticos quando eventos de falha podem acarretar perdas de vidas humanas ou perdas de ativos de alto valor. Geralmente estes sistemas operam com frequente troca de informações entre as partes internas do veículo ou do veículo com estações de solo ou, ainda, com outros veículos. Por se tratar de sistemas de*

tempo real, esta comunicação em geral exige baixa latência e mecanismos de segurança que garantam os requisitos básicos de um cenário crítico, tais como confidencialidade, integridade, autenticidade e disponibilidade dos canais de comunicação. Associado a isso está a preocupação com a segurança ("saúde") dos módulos/componentes de um veículo, os quais podem apresentar falhas de funcionamento, sejam elas intencionais (tentativas de ataques) ou não, que podem levar o veículo a provocar acidentes. Tendo em vista esta necessidade crescente de se assegurar a comunicação e o funcionamento de veículos não tripulados somada à desejável característica de aumento da conectividade em cenários deste tipo, este plano de trabalho propõe a especificação completa de uma arquitetura de comunicação de dados com vista a aspectos de segurança e mobilidade. O cenário aéreo será foco do desenvolvimento deste trabalho, porém espera-se obter uma arquitetura flexível de modo que seja facilmente portável para outros cenários de veículos não tripulados, tais como o terrestre e o aquático. A especificação desta arquitetura de comunicação de dados contribuirá para a inserção de novas aeronaves heterogêneas no espaço aéreo, uma vez que os requisitos para o processo de certificação das mesmas estarão sendo contemplados.

1. Introdução

Esta seção apresenta uma revisão sobre o uso de arquiteturas de comunicação de dados em sistemas embarcados críticos como forma de facilitar o desenvolvimento de sistemas deste tipo e, no caso de aeronaves não tripuladas, facilitar sua inserção no espaço aéreo. Esta inserção depende de uma adaptação às normas estabelecidas por órgãos específicos, tais como a FAA (*Federal Aviation Administration*) dos Estados Unidos e a ANAC (Agência Nacional de Aviação Civil) do Brasil. Nos Estados Unidos, a inclusão de uma aeronave ao *National Airspace System* (NAS) deve obedecer uma série de requisitos, incluindo questões ligadas a *Sense and Avoid* (SAA), que buscam "imitar" o conhecimento e a percepção de um piloto humano em relação a anormalidades com a aeronave ou obstáculos que possam surgir em tempo de voo.

Sistemas aéreos não tripulados são apenas um exemplo de sistemas embarcados críticos. Sistemas embarcados são sistemas computacionais que fazem parte de um sistema maior provendo, geralmente, monitoramento e controle em tempo real para todo o sistema [1, 2, 9, 13, 15]. Eles fornecem um conjunto pré-definido de tarefas, normalmente dedicados a uma aplicação em tempo real, e apresentam requisitos especiais. Estes sistemas são considerados críticos quando eventos de falha podem acarretar perdas de vidas humanas ou perdas de ativos de alto valor.

Além do cenário aéreo, existem os cenários terrestre e aquático, este último dividido em veículos de superfície e subaquáticos. Em todos eles, salvo algumas características particulares de cada cenário, a comunicação e a baixa tolerância a falhas são requisitos altamente desejados e, portanto, a comunicação que provê o completo gerenciamento de missões executadas por tais sistemas é um dos fatores-chave no projeto de um sistema embarcado crítico de qualquer natureza. Mesmo sistemas que executam missões de coleta de informações e não são sensíveis a tempo real, ou seja,

não necessitam do envio de informações em tempo de execução para uma estação de base ou para outros sistemas operantes nas proximidades, têm a necessidade de armazenamento adequado das informações coletadas no interior do sistema para evitar que ocorram roubos, manipulações por entidades maliciosas ou mesmo perda destas informações.

Esta proposta visa a especificação completa de uma arquitetura de comunicação de dados aplicável a sistemas embarcados críticos de qualquer natureza. Entretanto, de modo a guiar os passos da definição e do desenvolvimento da arquitetura, esta proposta será focada nos veículos aéreos não tripulados, também conhecidos como VANTs. O motivo da escolha do cenário aéreo se deve, ainda, à maior criticidade em relação aos outros cenários existentes (terrestre e aquático).

2. Trabalhos relacionados

Apesar de o fator velocidade ser considerado como elemento impactante no resultado final da comunicação, este projeto deve efetuar uma avaliação deste e de outros fatores em ambientes com e sem mobilidade. O trabalho apresentado em [12] faz uma avaliação de desempenho de protocolos de roteamento *mesh* para aplicações de agrupamento de VANTs, abordando tecnologias que visam o compartilhamento rápido e seguro de informações entre veículos e estações de base e de veículos com outros veículos que compõem o sistema aéreo não tripulado (SANT). Entretanto, a velocidade atingida por estes veículos é considerada baixa, sendo em média 1 m/s. Esta proposta visa projetar uma arquitetura que contemple aeronaves de todos os tipos e características.

Considerando o aumento significativo de aeronaves para aplicações em agricultura de precisão, segurança nacional (missões militares), monitoramento ambiental e doméstico e visando a maximização da conectividade dessas aeronaves, alguns trabalhos têm feito testes com o uso da nova versão do protocolo IP, o IPv6. O trabalho [10] propõe uma solução móvel segura baseada em IPv6 para veículos terrestres, primeiramente exigindo uma autenticação para acesso à rede e posteriormente fazendo uso do padrão NEMO (*Network Mobility*) e de uma combinação de IPsec/IKEv2 para o controle e tráfego de dados seguros. Esta proposta busca adotar o protocolo IPv6 com vista ao aproveitamento do novo padrão sugerido e de suas vantagens em relação ao IPv4 que está em fase de obsolescência, contribuindo para que a arquitetura proposta tenha vista à mobilidade [5, 11]. Ainda no contexto de IPv6 aplicado a veículos terrestres, o trabalho apresentado em [6] avalia o uso de pseudônimos em IPv6 para comunicação de aplicações de ITS (*Intelligent Transportation Systems*). O resultado final provou ser possível atingir confidencialidade e integridade, contudo não provê privacidade de localização, um requisito desejado em aplicações de ITS.

O artigo publicado em [14] detalha a arquitetura de software da plataforma de VANT conhecida como Berkeley. Ela demonstra com sucesso a navegação baseada em visão autônoma para evitar obstáculos e valida conceitos ligados ao controle para execução de missões colaborativas, ou seja, para a formação de esquadrilha de VANTs. Trata-se de uma arquitetura modular, como a maioria dos trabalhos relacionados, devido às já conhecidas vantagens no desenvolvimento de sistemas modularizados. Entretanto,

adotando a ideia de uma arquitetura mais genérica que contemple SANTs heterogêneos, esta proposta de doutorado difere do artigo citado pois objetiva-se definir e especificar parâmetros, protocolos, mecanismos e enlaces focados em SANTs de diversos tipos.

Todos os trabalhos correlatos apresentados preocupam-se com a modularização de arquiteturas, apresentam características diferentes quanto a mobilidade e não se preocupam, na maioria das vezes, com a segurança e a "saúde" dos componentes dos veículos abordados. Em alguns casos, abordam apenas aeronaves de pequeno porte, o que representa a exclusão de grande parte das aeronaves existentes atualmente e que são empregadas para a execução de missões mais robustas. Desse modo, o projeto aqui proposto busca especificar uma arquitetura de comunicação de dados completa para sistemas de aeronaves não tripuladas heterogêneas, com vista ao aumento da mobilidade e vazão de dados trocados entre os diversos elementos constituintes do SANT. Essa arquitetura busca, ainda, o aumento da segurança dos módulos internos e externos existentes nos veículos e estações de base. Para isso, um protocolo de autenticação dos módulos de hardware é proposto e protocolos como o IPv6 deverão ser avaliados e, de acordo com os resultados, adotados para a arquitetura. Além disso, o conceito de redes sem fio 3-D deve ser incorporado ao projeto como forma de aumentar as possibilidades de troca de informações entre os elementos que compõem o SANT [10].

O uso crescente de VANTs deve fazer com que eles se tornem comuns, passando a ser comercializados de forma mais ampla. Nesse cenário, a arquitetura proposta facilitará o desenvolvimento automatizado de sistemas de VANTs, permitindo que esses veículos sejam inseridos e incorporados mais facilmente ao espaço aéreo, contribuindo para a sua disseminação. Além disso, incorporando segurança pode-se facilitar também o processo de certificação desses VANTs junto a agências responsáveis.

3. HMSB-DataCom: *Health, mobile and safety-based data communication architecture*

O primeiro passo para auxiliar na especificação de uma arquitetura de comunicação é identificar as partes de um VANT e as partes de uma estação de solo que apresentam requisitos críticos de tempo real, permitindo abordagens adequadas para cada uma destas partes de modo a garantir o funcionamento correto da aeronave como um todo. Na Figura 1 está ilustrada uma visão interna da aeronave e da estação de solo com os módulos organizados de acordo com a necessidade de baixa latência, média latência ou sem preocupações com tempo real no que tange à comunicação.

Como pode ser visto na Figura 2, a arquitetura de comunicação do VANT que é base para esta proposta possui três barramentos de comunicação: de tempo real (em vermelho) cuja latência é expressa na ordem de milissegundos e tem foco em partes da aeronave de fundamental importância para a sua operação segura (ex.: sensores básicos da aeronave); de tempo real flexível (em amarelo) cujo tempo de comunicação situa-se na ordem de algumas dezenas de milissegundos, contemplando módulos menos críticos, mas ainda assim sensíveis a tempo real (ex.: comunicação com outros veículos, que pode ser uma característica operante a baixas latências, mas ainda assim não é tão crítica quanto o piloto automático, o qual, em situações de falhas que exijam a

abortagem da missão, pode operar sem a comunicação com outros veículos ou estações de solo); e o barramento sem preocupação com tempo real (em verde) que permite o uso de serviços com tempos não-determinísticos e que não são essenciais para o funcionamento das funções básicas da aeronave. No caso da estação de solo, a organização segue a mesma ideia, porém apenas com um barramento de tempo real e outro sem preocupação com tempo real, considerando que as funções exercidas pela estação de solo deverão limitar-se ao envio de informações/comandos de altíssima criticidade à aeronave e à comunicação com outras entidades via Internet. Esta última situação pode não requerer canais de comunicação de tempo real.

Partindo da organização acima apresentada, as próximas seções abordarão a proposta geral deste projeto separada em duas partes: a primeira delas aborda questões ligadas à "saúde"[1] dos componentes e à segurança da comunicação; e a segunda aborda o forte requisito de mobilidade em SANTs.

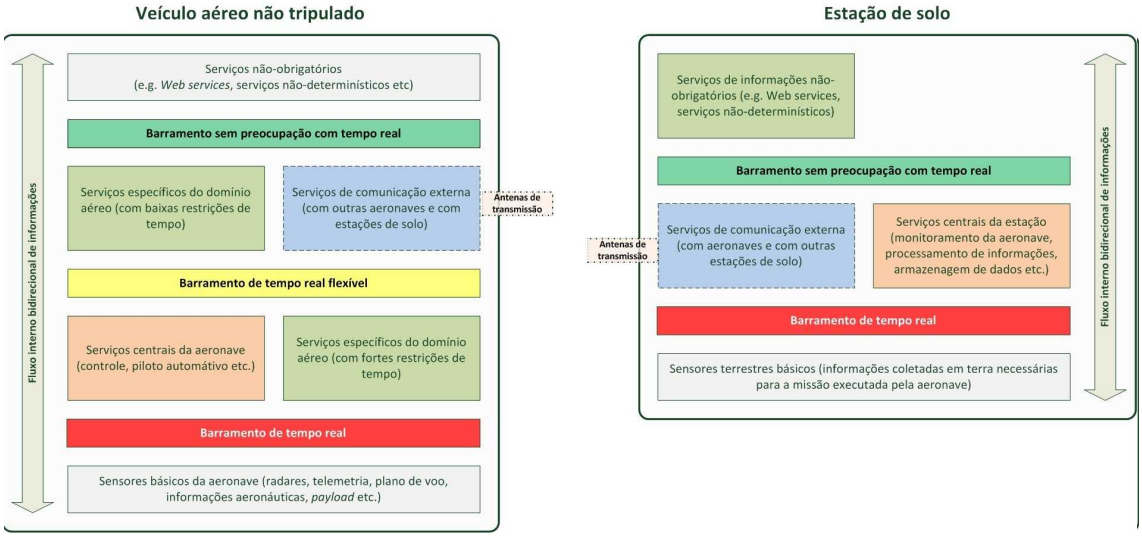

Figura 1. Partes básicas de um VANT e de uma estação de solo com os barramentos definidos de acordo com a necessidade de velocidade de comunicação.

3.1. "Saúde" e segurança dos componentes

Uma das primeiras etapas para se garantir a segurança de funcionamento de um veículo e facilitar sua inserção no espaço aéreo deve ser a redefinição de algumas políticas de uso dos componentes desse veículo. Poucas partes de uma aeronave recebem a atenção adequada que as assegure como módulos autênticos e que não tenham sido substituídos ou adulterados por terceiros. A política atual adotada pela maioria dos fabricantes de aeronaves usa um conceito de "*Accept all*" que confia em todos os componentes embarcados em uma aeronave. Esta proposta sugere a adoção da abordagem "*Deny all*", que nega a autenticidade de todos os componentes mecânicos e periféricos acoplados ao veículo até que o contrário seja provado, o que pode resultar em veículos mais seguros (*security*) contra alguns tipos de ataques.

1 "**Saúde**", neste contexto, refere-se à condição de bom funcionamento dos componentes existentes em um veículo. Um componente "saudável" é aquele cujo funcionamento não está comprometido por ações tais como a deterioração por ação do tempo ou por condições climáticas extremas e/ou por adulterações realizadas por terceiros.

A categorização de módulos é, portanto, crucial para que este novo modelo de segurança para veículos aéreos seja aplicado. Existem diversos periféricos e módulos que compõem um VANT e cada um deles exige níveis diferentes de segurança (safety), o que leva à necessidade de uma classificação de módulos de acordo com a criticidade da função exercida pelos mesmos. Esta proposta sugere a categorização em módulos primários e secundários. Nos módulos primários estão todos os componentes considerados essenciais para que a aeronave voe, tenha conhecimento de sua localização e seja capaz de efetuar um pouso emergencial com segurança, mesmo sem o cumprimento de uma missão que pudesse estar em curso. Ou seja, módulos como o piloto automático, o receptor GPS e as unidades barométrica e inercial são exemplos de módulos classificados como primários. Em contrapartida, módulos que agregam funções não-essenciais aos VANTs são classificados como módulos secundários. Quando comportamentos anormais são detectados em qualquer módulo secundário do avião, o funcionamento dos componentes primários do avião não é afetado e o módulo secundário que apresentou este comportamento anormal é desativado, além de gerar o bloqueio de todos os pacotes enviados pelo mesmo, uma vez que este comportamento pode se tratar de um ataque à segurança. Isso implica que todos os módulos primários sejam autenticados antes do voo iniciar, caso contrário a aeronave não deve efetuar o processo de decolagem. Entretanto, os módulos secundários não necessitam obrigatoriamente de uma autenticação antes da decolagem.

Além da proteção contra ataques mal intencionados existe ainda a possibilidade de identificar anomalias provenientes do tempo de uso dos componentes. Com a ação do tempo, da pressão, de colisões e do próprio uso dos componentes da aeronave, degradações naturais podem ocorrer. Deste modo, mecanismos que identifiquem a existência de comportamentos incomuns devem auxiliar na segurança da aeronave de um modo geral, mesmo com uma consequente abortagem de uma missão por questões de integridade física da aeronave. Estes conceitos estão fortemente ligados à área de *Sense and avoid* (SAA), que, apesar de não ser parte deste projeto, será considerada como um elemento a ser incorporado à HMSB-DataCom futuramente. Essa segurança reforçada de cada módulo da aeronave auxilia na obtenção de aeronaves mais seguras e, consequentemente, mais aptas a serem inseridas no espaço aéreo.

Outro conceito associado à ideia de autenticação de módulos é a criação de perfis de usuários. Quando uma missão é acoplada à aeronave, ela deve passar por um processo de autenticação, o que atribuirá diferentes permissões de acesso aos módulos da aeronave. Este conceito é similar ao utilizado em sistemas operacionais modernos, onde um usuário do tipo administrador pode instalar e remover programas, por exemplo, sem restrições, ao contrário de um usuário do tipo visitante, que tem acesso à execução de parte dos programas instalados e não tem permissão para instalação/remoção de novos programas. No contexto de VANTs esse conceito acrescenta uma camada de segurança que permite o bloqueio de uso de determinados módulos em um nível localizado abaixo da camada de software, garantindo que módulos específicos fiquem bloqueados para determinadas classes de usuários. Essa especificação visa evitar acessos não autorizados. Mesmo que se tenha um único usuário efetivo do VANT, nenhum outro usuário (seja ele um atacante ou não) terá acesso privilegiado a informações ou módulos do VANT.

Para proteger a aeronave de ataques advindos de componentes maliciosos conectados a ela, esta proposta sugere algumas etapas que devem garantir que todos os componentes ajam como o esperado. Quando busca-se aplicar políticas mais severas de segurança dos componentes de um veículo é necessário garantir que todos eles sejam autênticos, então quando um deles apresentar uma falha ou anormalidade, os demais serão impedidos de enviar informações a ele. Além disso, estas políticas precisam ser aplicáveis mesmo em tempo de voo, considerando que mudanças climáticas, por exemplo, podem afetar o comportamento dos componentes. E mais: cada componente precisa contribuir para o aumento geral da segurança da aeronave. De modo a aplicar estes métodos e requisitos, assume-se que na inicialização do sistema da aeronave ou após mudanças de hardware, o módulo CSU (*Central Security Unit*) permanece em um estado seguro. Ele ainda será responsável por armazenar uma tabela de chaves públicas de todos os componentes do veículo, atuando de forma semelhante a uma entidade certificadora [8]. Cada módulo (ou componente) deverá armazenar um *hash* da tabela de chaves para verificar se a mesma está corrompida. Durante a inicialização do veículo, uma fase de autenticação mútua deve ocorrer com a unidade CSU. Ela verifica no banco de dados as credenciais de todos os módulos, a criticidade dos mesmos e, ainda, se existe algum tipo de restrição de acesso. Há também a possibilidade de decidir se um módulo deve ser inicializado ou não durante a etapa de verificação.

Sob o ponto de vista de segurança de comunicação, uma situação ideal seria que todos os módulos pudessem se autenticar com os demais. Porém, este método ocasionaria uma sobrecarga no sistema, uma vez que o aumento de módulos na aeronave viria a provocar um crescimento exponencial no número de mensagens trocadas. Para solucionar este problema existem os protocolos de *e-voting*, como por exemplo [4]. No caso do módulo CSU não ser autêntico, protocolos como os apresentados em [3] podem ser utilizados. Este modelo pode ainda ser expandido de acordo com as necessidades da aeronave, incluindo uma negociação mediada pela CSU para criação de um canal seguro de comunicação entre os módulos (ou parte deles). Uma representação gráfica dos processos executados durante a fase de autenticação dos módulos com a CSU pode ser vista na Figura 2.

Uma das principais características almejadas para a arquitetura proposta no tocante à mobilidade é a criação de uma arquitetura distribuída, ou seja, que aborde os diversos elementos (aeronaves, estações de solo, veículos de suporte, redes de sensores terrestres etc.) que compõem um SANT e o estabelecimento de todos os tipos de comunicação possíveis neste tipo de cenário. O conceito de redes sem fio 3-D deverá ser considerado na definição da arquitetura. Estas redes consideram a fusão do mundo digital com o mundo físico permitindo a troca de informações entre indivíduos e objetos, de dados com serviços entre outros. Por exemplo, em um cenário militar moderno, as redes sem fio 3-D podem ser utilizadas para conectar aeronaves, tropas e frotas permitindo uma maior troca de dados entre eles e garantindo a segurança de informações sigilosas que possam vir a ser trocadas. Este novo paradigma introduzido pelas redes sem fio 3-D vai ao encontro das necessidades de cenários onde VANTs são aplicados [10].

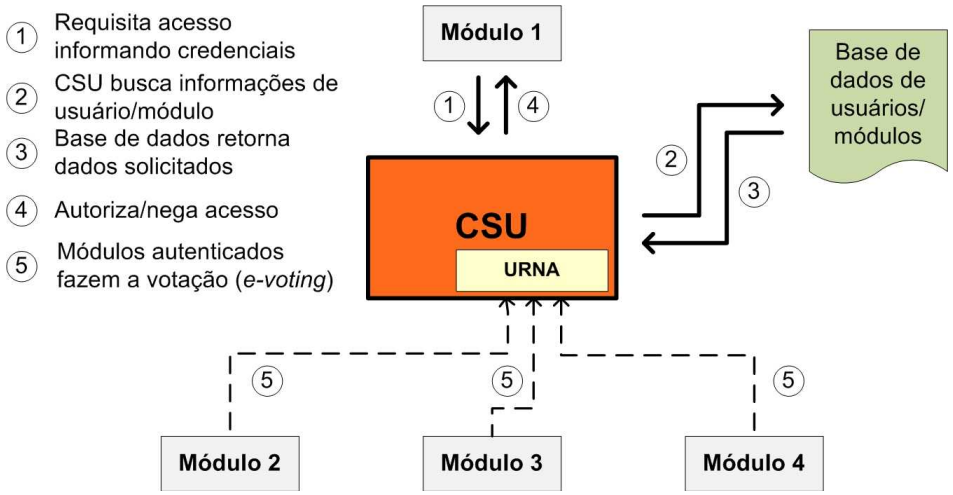

Figura 2. Fase de autenticação de módulos com a CSU

Além do abandono do protocolo IPv4 para dar lugar ao IPv6 que por si só é mais seguro, questões que podem comprometer a segurança de uma aeronave (ou de veículos em geral) devem ser consideradas e abordadas na proposta de uma arquitetura de comunicação para que sua validade e contribuição sejam efetivas. A proposta apresentada neste projeto visa incluir algumas etapas de verificação da autenticidade dos módulos existentes em um VANT e permitir a ampliação de recursos e funcionalidades conforme a necessidade do cenário e da aplicação, o que consiste em uma proposta inovadora.

A etapa de validação da arquitetura deve fazer uso, inicialmente, do ambiente proposto em um projeto de mestrado em desenvolvimento. Este projeto tem por objetivo primário a construção e/ou extensão de um projeto *open source* de uma ferramenta capaz de realizar experimentos de redes móveis com nós georreferenciados. Suas funcionalidades permitirão a experimentação dos protocolos mais recentes de comunicação sem fio, inclusive com endereçamento IPv6, rotas com múltiplos pontos de acesso e trocas de ponto de acesso (*handover*). Após estes testes de bancada, testes práticos poderão ser executados juntamente com o desenvolvimento e validação dos demais projetos em desenvolvimento no grupo e que já foram citados anteriormente, uma vez que o andamento das propostas deverá ser paralelo, havendo interação constante entre os pesquisadores envolvidos para obter produtos finais integrados.

4. Conclusão

O principal resultado esperado com a realização deste trabalho é a obtenção da especificação completa de uma arquitetura de comunicação de dados que leve em consideração aspectos de segurança e de mobilidade, dois requisitos cada vez mais desejados no âmbito dos sistemas embarcados críticos. O foco de desenvolvimento está nos veículos aéreos não tripulados, porém espera-se obter uma arquitetura aplicável também a outros cenários, como o terrestre e o aquático. Desse modo, busca-se facilitar o processo de certificação desses veículos para que se tornem aptos a operar no espaço aéreo, em rodovias ou no meio aquático e que, consequentemente, sejam mais explorados comercialmente.

Trabalhando com um desenvolvimento fortemente conectado a outros trabalhos em desenvolvimento, almeja-se chegar ao final do projeto com uma arquitetura validada na prática e que contemple e sirva de suporte a trabalhos futuros tanto dentro do grupo de pesquisa no qual o projeto será desenvolvido, quanto em outros grupos de pesquisa e empresas nacionais e internacionais.

References

[1] BERGER, A. S. Embedded systems design: An introduction to processes, tools, and techniques. Lawrence, KS, USA: CMP Books, 2002.

[2] DOUGLASS, B. P. Real time uml: Advances in the uml for real-time systems (3rd edition). Redwood City, CA, USA: Addison Wesley Longman Publishing Co., Inc., 2004.

[3] Hiroaki Kikuchi, Junji Nakazato. Modint: A Compact Modular Arithmetic Java Class Library for Cellular Phones, and its Application to Secure Electronic Voting. Security and Protection in Information Processing Systems, p. 177-192, 2004.

[4] Horng-Twu Liaw, A secure electronic voting protocol for general elections, Computers & Security, Volume 23, Issue 2, March 2004, Pages 107-119, ISSN 0167-4048.

[5] IPv6.br | Portal sobre IPv6 do NIC.br. Disponível em: <http://ipv6.br/> Acesso em: 16 Fev 2013.

[6] Jong-Hyouk Lee, J M Bonnin, Fernando Pereniguez Garcia, Antonio F Skarmeta Gomez. Use of Pseudonyms in IPv6 ITS Communication: Performance Degradation and Exposure New Identity with Security Protocols, International Workshop on IPv6-Based Vehicular Networks, IEEE Intelligent Vehicles Symposium 2012 (IV'2012), June 2012.

[7] Jose Santa. Continuous IPv6 Communications in a Vehicular Networking Stack for Current and Future ITS Services. In 2012 IEEE Intelligent Vehicles Symposium Workshops, 2012.

[8] KUROSE, J. F.; ROSS , K. W. Computer networking: A top-down approach. 5 ed. Addison Wesley, 2009.

[9] LAVAGNO, L.; MARTIN, G.; SELIC, B. Uml for real: Design of embedded real-time systems. Norwell, MA, USA: Kluwer Academic Publishers, 2003.

[10] Li, P.; Pan, M.; Fang, Y. Capacity Bounds of Three-Dimensional Wireless Ad Hoc Networks, Networking, IEEE/ACM Transactions on, vol.20, no.4, pp.1304-1315, Aug. 2012.

[11] Narayan, S.; Kolahi, S.S.; Sunarto, Y.; Nguyen, D.; Mani, P. Performance comparison of IPv4 and IPv6 on various windows operating systems, Computer and Information Technology, 2008. ICCIT 2008. 11th International Conference on , vol., no., pp.663-668, 24-27 Dec. 2008.

[12] Pojda, J.; Wolff, A.; Sbeiti, M.; Wietfeld, C. Performance analysis of mesh routing protocols for UAV swarming applications, Wireless Communication Systems

(ISWCS), 2011 8th International Symposium on , vol., no., pp.317-321, 6-9 Nov. 2011.

[13] RAVI, S.; RAGHUNATHAN, A.; KOCHER, P.; HATTANGADY, S. Security in embedded systems: Design challenges. ACM Transactions on Embedded Computing Systems, v. 3, n. 3, p. 461–491, 2004.

[14] Tisdale, J.; Ryan, A.; Zennaro, M.; Xiao Xiao; Caveney, D.; Rathinam, S.; Hedrick, J.K.; Sengupta, R.; , "The software architecture of the Berkeley UAV Platform," Computer Aided Control System Design, 2006 IEEE International Conference on Control Applications, 2006 IEEE International Symposium on Intelligent Control, 2006 IEEE , vol., no., pp.1420-1425, 4-6 Oct. 2006.

[15] WOLF, M. Computers as components: Principles of embedded computing system design. Burlington, MA, USA: Morgan Kaufmann Publishers, 2012.