Sistema de Rastreamento de Embarcações de Pesca por Satélites Brasileiros com Criptografia de Dados

André Barros Cardoso da Silva, Wilson Yamaguti e Wilton Ney do Amaral Pereira

***Resumo*—O Programa Nacional de Rastreamento de Embarcações Pesqueiras por Satélite (PREPS), sob responsabilidade da Secretaria Especial de Aqüicultura e Pesca da Presidência da República (SEAP/PR), objetiva monitorar embarcações de pesca com mais de 15m e/ou 50t de arqueação, hoje estimada em trinta mil unidades. Visando contribuir com o PREPS, este trabalho propõe um sistema de rastreamento utilizando os satélites do Sistema Brasileiro de Coleta de Dados Ambientais (SBCDA), que receberão os dados cifrados de um localizador GPS. A utilização de satélites nacionais neste segmento oferece considerável redução dos custos dos serviços de rastreamento, favorecendo assim as pequenas cooperativas de pesca.**

***Palavras-chave*—Criptografia, cifragem, AES, Rijndael, GPS, rastreamento, embarcações, pesca, satélite, SBCDA.**

***Abstract*—The National Program of Vessel Monitoring by Satellite (PREPS), under responsibility of the Special Secretary of Aquaculture and Fishing of the Brazilian Government (SEAP/PR), has for main goal monitoring fishing vessels above 15m and/or 50t gross weight, nowadays estimated in thirty thousands units. As a contribution to this program, this work presents a GPS locator with data ciphering as an application of the Brazilian Environmental Data Collection System (SBCDA). The use of national satellites for this purpose helps small fishing co-operatives by offering reduced tracking service costs.**

***Keywords*—Encryption, ciphering, AES, Rijndael, GPS, monitoring, vessel, fishing, satellite, SBCDA.**

I. Introdução

O Programa Nacional de Rastreamento de Embarcações Pesqueiras por Satélite (PREPS) foi criado em 2006 com o objetivo de modernizar o monitoramento de embarcações de pesca no Brasil através da implantação de rastreadores nas embarcações, oferecendo cobertura nacional através do uso de satélites [1]. De responsabilidade da Secretaria Especial de Aqüicultura e Pesca da Presidência da República (SEAP/PR), do Instituto Brasileiro de Meio Ambiente e dos Recursos Naturais Renováveis (IBAMA) e da Marinha do Brasil, o PREPS permite melhor fiscalizar: área de atuação das embarcações, rotas, profundidade, entre outros.

O PREPS estabelece uso obrigatório de rastreadores a toda embarcação de pesca com mais de 15m e/ou 50t de arqueação, lei vigorada desde Outubro/2008 [2]. Devido ao elevado custo oferecido por sistemas estrangeiros atuantes neste setor, o Instituto Nacional de Pesquisas Espaciais (INPE) objetiva contribuir com o PREPS oferecendo uma solução nacional mais econômica por meio do Sistema Brasileiro de Coleta de Dados Ambientais (SBCDA) – composto por satélites desenvolvidos e operados pelo INPE.

Os autores André Barros Cardoso da Silva e Wilton Ney do Amaral Pereira são da Universidade de Taubaté (UNITAU), Taubaté, SP, Brasil. O autor Wilson Yamaguti é do Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, SP, Brasil. E-mails: andrebcs@hotmail.com, wilton.pereira@uol.com.br, e yamaguti@dss.inpe.br.

II. Visão Geral do Sistema

A Fig. 1 mostra o sistema de rastreamento completo junto à embarcação de pesca com o localizador GPS acoplado:

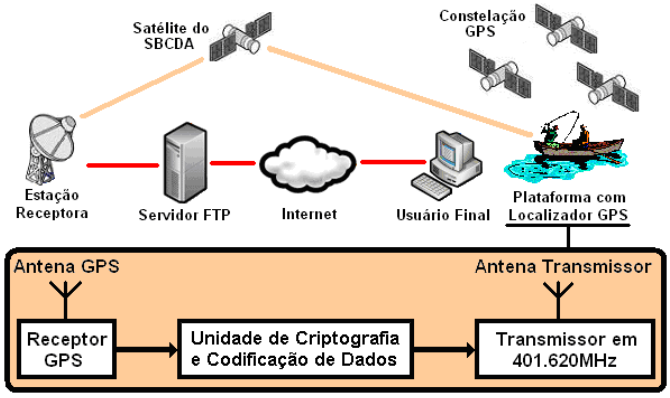

Fig. 1. Sistema de rastreamento de embarcações com o localizador GPS.

O localizador GPS, também responsável pela cifragem e codificação dos dados de posição geográfica, pode ser dividido em três blocos principais:

i) Recepção: composto basicamente por um receptor GPS Trimble *Lassen iQ,* que realiza a aquisição dos dados de posição geográfica encaminhando-os a unidade de processamento e criptografia de dados, via protocolo NMEA-0183.

ii) Processamento: os dados enviados pelo receptor GPS são processados por um microcontrolador PIC24FJ64GA002 (Microchip), que montará um pacote de 160 bits com base no formato de mensagem "*Header 0*" - formato utilizado em aplicações cuja precisão da posição geográfica é da ordem de 0.001°, sendo composto por uma posição absoluta (64 bits) e três posições relativas (32 bits cada). Sobre este campo de mensagem é aplicado o algoritmo de criptografia AES (Rijndael), e, subsequentemente ocorre a codificação dos dados para detecção e correção de erros na recepção.

iii) Transmissão: os dados codificados são transmitidos aos satélites do SBCDA através do transmissor UHF ELTA

HAL-2 (*High Accuracy Locator*), cujos parâmetros de transmissão são completamente programáveis pelo usuário: *ID*, potência, freqüência, campo de dados, etc.

No SBCDA, os satélites funcionam como retransmissores de mensagens. Os dados são coletados pelas Estações Terrenas de Cuiabá (MT) e Alcântara (MA), processados e armazenados pelo Centro de Missão de Coleta de Dados (CMCD), e então difundidos aos usuários através da Internet, via servidor FTP [3]. Por fim, o módulo de decodificação e decifragem AES (Rijndael) converte as mensagens processadas pelo CMCD à sua forma original, para então serem disponibilizadas ao usuário.

III. Desenvolvimento e Resultados Parciais

A. Baliza do SBCDA

A baliza é basicamente o hardware que protege o localizador GPS das mais variadas condições climáticas existentes em alto mar, sendo também responsável pela integridade física e funcional das baterias, antenas, etc. A Fig. 2 mostra o arranjo prático de uma baliza do sistema Argos, desenvolvida pelo grupo francês Martec serpe-iesm [4]:

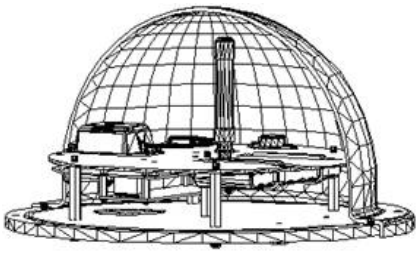

Fig. 2. Baliza do sistema Argos para rastreamento de embarcações.

A construção da baliza do SBCDA está prevista para as próximas etapas de projeto, e deve levar em consideração a antena helicoidal quadrifilar Synergetics *QFH 14A-N*, as baterias de chumbo-ácida e o localizador GPS – componentes que determinarão suas dimensões e peso (previsto até 15kg).

A baliza deve oferecer funcionalidades ao usuário, como: criptografia de dados (algoritmo descrito a seguir), diferentes pacotes de mensagem que variam de acordo com a necessidade do usuário, botão de emergência para localização instantânea da embarcação, entre outras.

B. Algoritmo de Criptografia AES

Criado por Vincent Rijmen e Joan Daemen, o Advanced Encryption Standard (AES) é um algoritmo baseado em permutações de bytes completos que permite flexibilidade na escolha dos tamanhos da chave simétrica e dos blocos de mensagem: 128, 192, 256 bits [5]. Visto como um dos métodos mais seguros da atualidade, o AES não possui chaves "fracas" em sua concepção. Para o caso particular deste projeto, as mensagens e a chave de criptografia são manipuladas em blocos de 128 bits. A verificação deste algoritmo criptográfico foi realizada com base no arquivo público nº197 – anúncio de aprovação do AES [6].

Os diagramas em blocos dos processos de cifragem e decifragem são mostrados na Fig. 3. Descrições mais aprofundadas sobre os mesmos podem ser encontradas nas referências bibliográficas utilizadas [5]-[8].

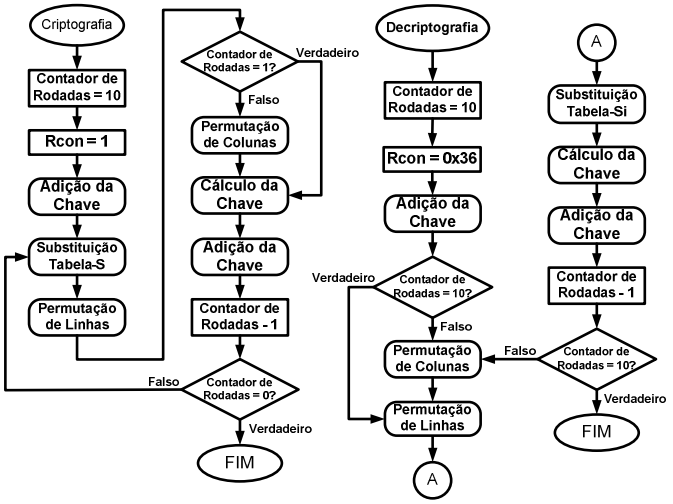

Fig. 3. Diagramas em blocos da cifragem e decifragem, respectivamente [7].

IV. Conclusões

O localizador GPS pode ser verificado por meio de simulações, onde foram obtidos dados de posição geográfica com precisão melhor que 150m. A criptografia é um recurso de aplicação potencial da baliza, capaz de oferecer ao usuário segurança nos dados transmitidos por suas embarcações. A verificação do algoritmo criptográfico AES (Rijndael) pode ser realizada através das mensagens recebidas, sendo estas corretamente decifradas. A construção da baliza será realizada de acordo com as dimensões dos módulos internos, possibilitando os primeiros testes em condições reais.

Às etapas finais deseja-se aprofundar em novos estudos criptográficos a fim de se obter criptografia em blocos menores de mensagem. O estudo, projeto e implementação do algoritmo de codificação / decodificação (p. ex. *Turbo Code*) é a meta de outro trabalho já em andamento.

Referências

[1] SEAP. Instrução normativa interministerial nº2. SEAP, 2006. 37p.

[2] SEAP. Instrução normativa nº22. SEAP, 2007. 3p.

[3] YAMAGUTI,W. et al. O Sistema Brasileiro de Coleta de Dados Ambientais:Estado atual, demandas e estudos de propostas de continuidade da Missão de Coleta de Dados. INPE, 2006.

[4] GROUPE MARTEC ANGLAIS. Disponível em: <http://en.martec.fr>. Acesso em: 31 Maio 2005.

[5] DAEMEN, Joan; RIJMEN, Vincent. The Design of Rijndael: AES – The Advanced Encryption Standard. 1. ed. New York: Springer-Verlag, 2002. 255p.

[6] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 197,1., 2001. Announcing the Advanced Encryption Standard (AES)... NIST, 2001. 52 p.

[7] FLOWERS, David. Data Encryption Routines for the PIC18. Disponível em: <http://ww1.microchip.com/downloads/en/AppNotes/00953a.pdf>. Application Note 953. Acesso em: 14 Jan. 2005.

[8] XIV SIMPÓSIO BRASILEIRO DE SENSORIAMENTO REMOTO – INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS/ Anais, SILVA, A. et al. Localizador GPS com criptografia de dados. Natal, p. 1617-1624, abr. 2009.