UNIVERSIDADE FEDERAL DE SANTA MARIA

VICTOR DALLAGNOL BENTO

Criptografia de Dados GPS em uma Plataforma de Coleta de Dados

SANTA MARIA - RS

2019

RESUMO

O Sistema Brasileiro de Coleta de Dados Ambientais (SBCDA) utiliza satélites brasileiros desenvolvidos e gerenciados pelo Instituto Nacional de Pesquisas Espaciais (INPE) para realizar suas atividade. No entanto, novos aplicativos de coleta de dados (localizadores - principalmente em sistemas estrangeiros), como monitoramento de embarcações, precisam transmitir posições geográficas aplicando um algoritmo de criptografia sobre os dados. Para suprir essas necessidades, um localizador foi desenvolvido para ser usado em plataformas únicas de coleta de dados. Este localizador tem um receptor GPS que irá coletar os dados da posição geográfica e trabalhará em conjunto com um microcontrolador que aplicará sobre os dados um algoritmo de criptografia, fornecendo uma comunicação confiável e segura. Após a criptografia, os dados serão transmitidos através de um transmissor UHF para os satélites SBCDA. Estudos sobre diferentes algoritmos de codificação, com foco em sua viabilidade, eficiência e facilidade de implementação, apontaram o Advanced Encryption Standard (AES) como a melhor opção a ser adotada, sendo anunciado pelo Instituto Nacional de Padrões e Tecnologia (NIST) como um algoritmo padrão de codificação, em 2001. Sucessor do método DES (Data Encryption Standard), o AES (Rijndael) é um algoritmo baseado em permutações de bytes completos, permitindo flexibilidade ao usuário na escolha dos tamanhos da chave simétrica e dos blocos de mensagem: 128, 192, 256 bits. Os testes de cifragem foram realizados de acordo com as referências existentes, a fim de validar a implementação do algoritmo no microcontrolador.

I. INTRODUÇÃO

Com o aumento da busca por conhecimento e evolução da sociedade em relação a tecnologia, principalmente no campo da comunicação que teve um avanço exponencial, apresentando uma maior qualidade na comunicação ao mesmo tempo que apresenta um custo mais baixo para efetuá-la.

Todo esse avanço na tecnologia acarretou em uma baixa no preço de sistemas receptores de GPS, tornando-os cada vez mais baratos e ao mesmo tempo mais presentes no nosso dia a dia como por exemplo em veículos, smartphones, microcomputadores, laptops, etc.

O Instituto Nacional de Pesquisas Espaciais (INPE), através do Sistema Brasileiro de Coleta de Dados Ambientais (SBCDA), oferece a oportunidade de realizar experimentos de comunicação envolvendo diversas tecnologias de comunicação digital com ênfase em aplicações de coleta de dados ambientais utilizando um conjunto de satélites desenvolvidos e operados pelo INPE. Os serviços prestados por este sistema são relacionados à coleta de dados ambientais adquiridas pelas Plataformas de Coleta de Dados (PCD), que utilizam os satélites como meio de comunicação para transmissão dos dados até as estações de recepção. Os dados recebidos são posteriormente enviados ao Centro de Missão Coleta de Dados que faz o processamento, o armazenamento e a difusão desses dados aos seus usuários. Novas demandas de coleta de dados necessitam adquirir as posições geográficas de uma dada plataforma e ao mesmo tempo garantir a proteção dos dados contra acesso não permitido.

Com ênfase nestas necessidades foi desenvolvido um sistema de localização acoplado a uma PCD já existente, onde um localizador oferece o serviço de localização geográfica através de um receptor do Sistema de Posicionamento Global (GPS), aplicando sobre os dados de posição um algoritmo de criptografia. O método criptográfico adotado para esta aplicação foi o Advanced Encryption Standard (AES), criado por Vincent Rijmen e Joan Daemen.

II. AMEAÇAS E REQUISITOS DE SEGURANÇA

O Sistema Brasileiro de Coleta de Dados Ambientais é constituído pela constelação de satélites SCD-1, SCD-2 e CBERS-2B, pelas diversas redes de plataformas de coleta de dados espalhadas pelo território nacional, pelas Estações de Recepção de Cuiabá e de Alcântara, e pelo Centro de Missão Coleta de Dados (CMCD).

Os satélites funcionam como retransmissores de mensagens. Assim, as comunicações entre uma plataforma e as estações de recepção são estabelecidas através dos satélites. As plataformas podem ser fixas ou móveis, e nas aplicações de hidrologia e de meteorologia com plataformas fixas, estas são geralmente configuradas para transmitirem, a cada 200 segundos, até 32 bytes de dados úteis, correspondendo a no máximo 1 segundo de transmissão.

As funções básicas do SBDA são a de coleta de dados ambientais transmitidas por plataformas fixas ou móveis, processamento, armazenamento e disseminação de dados aos usuários. Os dados coletados devem ser de interesse científico ou de monitoramento ambiental ou de proteção ambiental.

Um problema existente é a obtenção/interceptação dos dados por terceiros, podendo assim ocorrer uma alteração ou modificação dos dados, ocasionando um resultado diferente da realidade, podendo assim mudar a qualificação do ambiente (e.x: uma empresa modifica os dados para continuar aproveitando de um pedaço de terra para o desmatamento, motivados por poder e ganância). A obtenção de dados modificados pode alterar totalmente o estudo científico sobre a área estudada, ocasionar um monitoramento ambiental errado podendo desproteger um ambiente que precisa de cuidados.

III. IMPLEMENTAÇÃO DE SEGURANÇA

Primeiramente, o processo de implementação de segurança começa com a coleta dos dados pelo PCD (Plataforma de Coleta de Dados) que pode ser dividida em 3 segmentos: recepção, processamento e transmissão. Para a aquisição dos dados o dispositivo GPS dispõe de uma antena com um amplificador de sinal interno, enviando assim, estes dados recebidos para uma unidade de processamento e criptografia de dados, onde estes são processados por um microcontrolador PIC. O receptor GPS disponibiliza diferentes protocolos para envio dos dados de posição geográfica, entre os quais foi escolhido o *NMEA-0183* devido à sua larga utilização em vários segmentos, como: comunicações industriais, equipamentos de navegação náutica, entre outros. O microcontrolador escolhido foi o PIC18F4550, que faz parte da popular família de microcontroladores série PIC18F, possui alto valor de memória RAM e Flash o que o torna ideal para para aplicações de monitoramento onde é exigido conexões com computadores de forma periódica para fazer upload, downloads de dados e atualizações de firmware.

Baud rate	*4800*
Bits de dados	*8*
Paridade	-
Bits de parada	*1*
Handshake	-

Tabela 1: Configuração Serial (enlace) para o protocolo *NMEA-0183.*

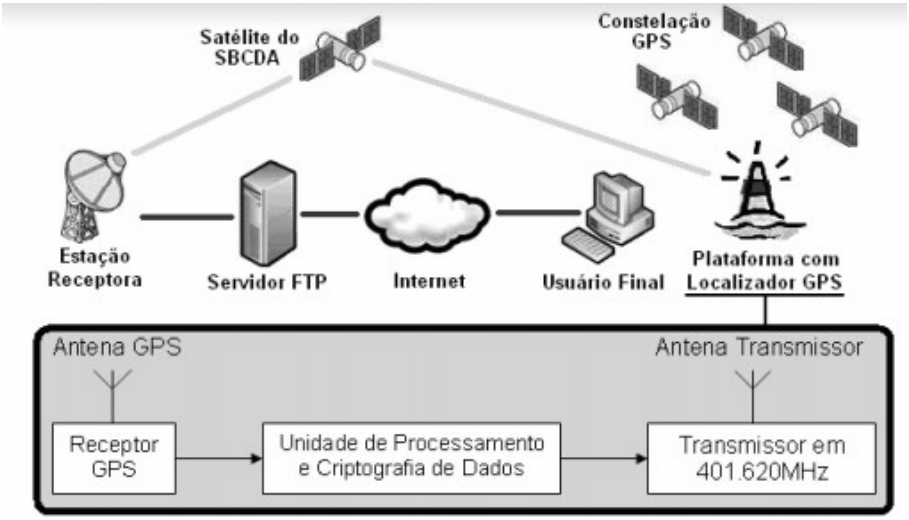

Figura 1: Sistema de rastreamento com a plataforma de coleta de dados.

O microcontrolador PIC18F4550 realiza o processamento e criptografia dos dados de posição geográfica, utilizando um programa feito em linguagem “C”. Este microcontrolador recebe a mensagem completa (estabelecida pelo protocolo NMEA-0183) armazenando somente os dados imprescindíveis para a criação do campo final da mensagem “*header 0*”. Assim, sobre este campo é aplicado o algoritmo de criptografia AES (Rijndael) que proporcionando elevada segurança sobre os dados para então serem transmitidos aos satélites do SBCDA.

Esta transmissão é feita através do transmissor ELTA HAL-2 (High Accuracy Locator 2), que possui a possibilidade de programação de seus parâmetros de transmissão, tais como: ID, frequência, potência, tamanho do campo de mensagem, etc.

Cada mensagem transmitida é estruturada de acordo com um formato padrão para transmissão de dados de localização. O formato “header 0”, utilizado em aplicações cuja precisão da posição geográfica é da ordem de 0.001°. Este formato provê a cada pacote uma posição absoluta e três posições relativas, estabelecendo um campo final de 160 bits. A posição absoluta de cada mensagem refere-se a última posição na qual foi realizada a aquisição de dados pelo receptor GPS. As posições relativas são juntamente transmitidas com a absoluta com o intuito de oferecer um “histórico” da posição ao usuário, posto que nem sempre os satélites do SBCDA serão visíveis pela PCD, podendo ocasionar períodos

sem recepção de dados. Deste modo, as posições relativas devem sempre ser referidas a posição absoluta, contendo somente a variação entre as coordenadas latitude e longitude (deltas), e o tempo de atraso entre cada transmissão (delays).

O formato do campo final da mensagem é mostrado abaixo, através das Tabelas 1 e 2:

Header	CRC	Longitude	Latitude	Horas	Minutos	Segundos
4 bits	8 bits	19 bits	18 bits	5 bits	6 bits	4 bits

Tabela 1: Primeira posição fixa (absoluta).

∆Latitude	∆Longitude	Delay	Time Index
13 bits	13 bits	4 bits	2 bits

Tabela 2: Segunda, terceira e quarta posições fixas (relativas).

Para a análise do projeto em questão foram utilizados algumas convenções:

- Longitude absoluta: 0 (0°) a 360000 (360°);
- Latitude absoluta: 0 (90°S) a 180000 (90°N);
- Horas e minutos: 0 a 23 horas e 0 a 59 minutos;
- Longitude e latitude relativas: Variação de 0 (-4°) a 8000 (+4°);
- Delay: 0 a 15 minutos;
- Time index: Adota-se como “00” (binário), indicando que o tempo real da aquisição é o contido na mensagem.
- Header: Campo que identifica o formato da mensagem. Para este caso deve ser igual à zero (formato “header 0”).
- CRC (Cyclic Redundancy Check): é calculado para cada mensagem transmitida de acordo com o polinômio “X7+X+1”, e é utilizado como um mecanismo de verificação de erros na mensagem recebida.
- Período: É um parâmetro configurável pelo usuário para aquisição de posição geográfica.

IV. DISCUSSÃO CRÍTICA

Para se iniciar um processo de criptografia, primeiramente deve-se escolher uma chave "forte" para o sistema. Tanto a chave quanto os blocos de mensagem podem assumir três tamanhos: 16 bytes, 24 bytes e 32 bytes, sendo que número de iterações de transformação da mensagem é variável em função dos tamanhos da chave e mensagem, como mostra a **Tabela 3:**

Chave	**Mensagem**		
	16 bytes	24 bytes	32 bytes
16 bytes	10	12	10
24 bytes	12	12	14
32 bytes	14	14	14

Tabela 3: Número de iterações do AES (Rijndael).

No projeto foi utilizada uma chave de 16 bytes junta a blocos de mensagens também de 16 bytes. Logo, serão necessárias 10 iterações de transformação da mensagem. A chave e cada bloco da mensagem devem ser constituídos matricialmente, como mostra a **Figura 2** e **Figura 3**:

Bloco [0]	Bloco [4]	Bloco [8]	Bloco [12]
Bloco [1]	Bloco [5]	Bloco [9]	Bloco [13]
Bloco [2]	Bloco [6]	Bloco [10]	Bloco [14]
Bloco [3]	Bloco [7]	Bloco [11]	Bloco [15]

Figura 2: Matriz dos blocos da mensagem.

Chave [0]	Chave [4]	Chave [8]	Chave [12]
Chave [1]	Chave [5]	Chave [9]	Chave [13]
Chave [2]	Chave [6]	Chave [10]	Chave [14]
Chave [3]	Chave [7]	Chave [11]	Chave [15]

Figura 3: Matriz de chaves secretas derivadas.

Cada campo Bloco[n] representa um byte da mensagem a ser

criptografada, e cada campo Chave[n] representa um byte que é uma chave derivada da chave secreta de criptografia e em cada iteração, não se usa a chave original de criptografia, mas sim uma série de chaves derivada da mesma. Essa derivação usa um algoritmo chamado Rijndael Key Schedule. Com a chave devidamente escolhida, dá-se início ao processo de criptografia que é indicado pelos diagramas em blocos de todo o processo criptográfico que estão indicados pela **Figura 4.**

Figura 4: Diagramas em blocos dos processos de criptografia (esq.) e descriptografia (dir.).

O texto e a chave escolhidas foram disponibilizados pelo Rijndael Simulator, onde são demonstradas as dez iterações necessárias para a cifragem de um texto puro, foi possível validar o desenvolvimento completo do algoritmo.

Seguem a mensagem e a chave secreta utilizadas na validação do algoritmo:

• Texto Puro: 0x3243F6A8885A308D313198A2E0370734h (128 bits).

• Chave Secreta: 0x2B7E151628AED2A6ABF7158809CF4F3Ch (128 bits).

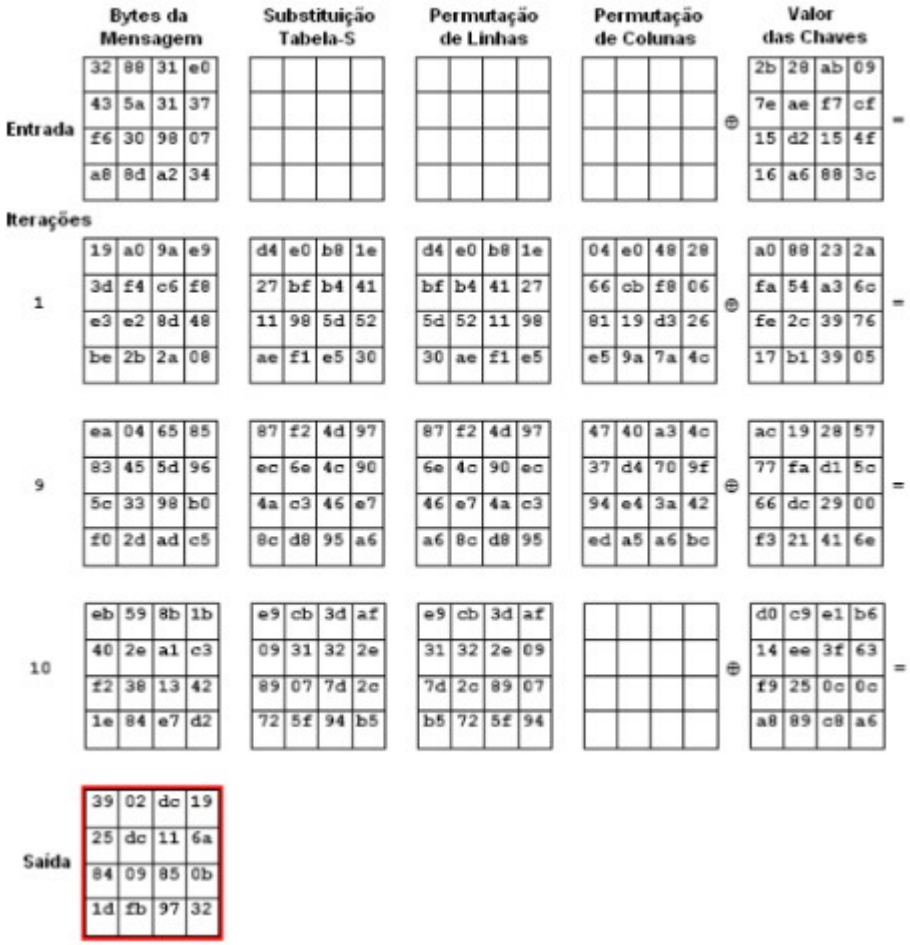

Figura 5: Matrizes com os dados do teste de cifragem.

O método criptográfico AES (Rijndael) calcula a cada iteração uma nova chave, que será utilizada na iteração seguinte. Cada uma das dez iterações utiliza uma chave diferente, cujo cálculo é baseado na chave anterior. Na última iteração não é executada a rotina “Permutação de Colunas”, também verificada no diagrama em blocos previamente mostrado. A matriz de saída já contém a mensagem criptografada: “3925841D02DC09FBDC118597196A0B32h” (128 bits).

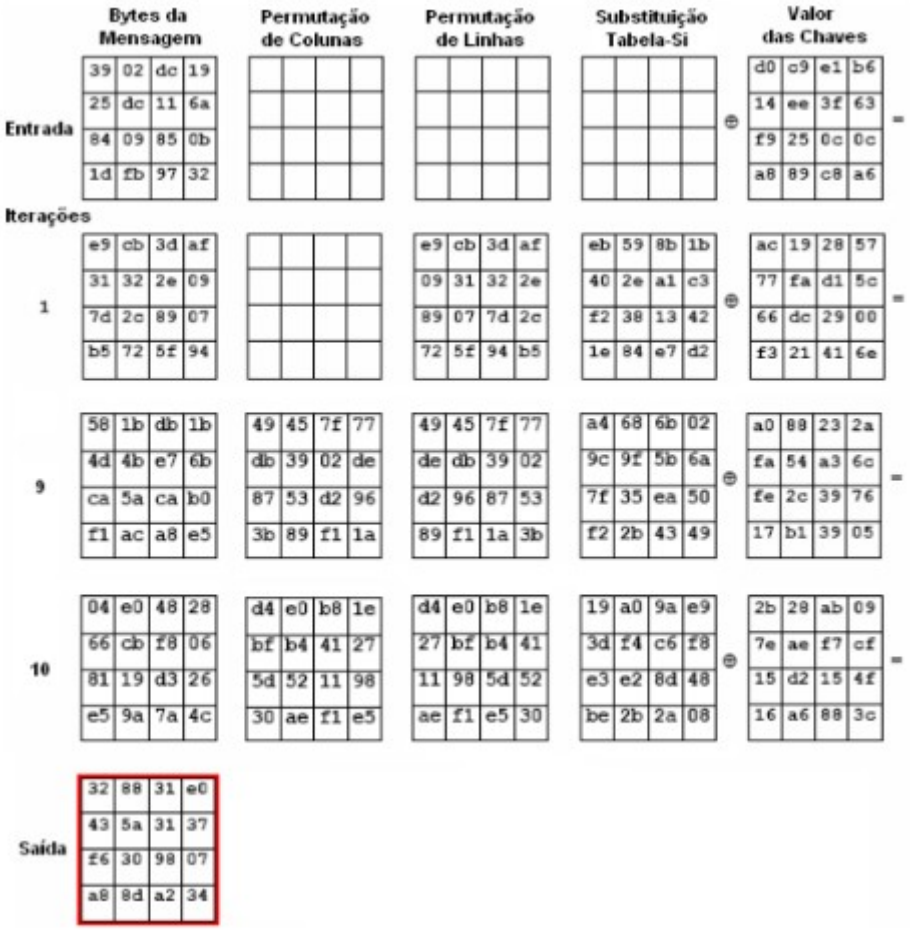

Figura 6: Matrizes com os dados do teste de decifragem.

No processo de decifragem do algoritmo AES (Rijndael) a chave inicial é a última chave calculada no processo de cifragem. Assim, nota-se na última iteração a recuperação do texto puro, e da chave propriamente dita. A rotina “Permutação de Colunas” não é executada na primeira iteração do processo de decifragem, também verificada no diagrama em blocos previamente mostrado. A matriz de saída contém então a mensagem em sua forma original, recuperando o texto puro: “3925841D02DC09FBDC118597196A0B32h” (128 bits).

V. CONCLUSÃO

Com este trabalho final podemos concluir que os estudos realizados na disciplina de Segurança de Rede serviram para a ampliação do conhecimento na área de Sistemas de Telecomunicações. O conhecimento teórico das ferramentas de criptografia, protocolos de segurança de rede, segurança de sistemas e segurança de redes sem fio foram muito importantes para findar muitas teorias vistas no curso de Engenharia de Computação e para expandir nosso conhecimento para um conteúdo muito importante que tende a crescer muito com as evoluções tecnológicas.

Ademais, este trabalho tem como base principal um artigo desenvolvido pelo INPE, servindo apenas para mostrar e dar uma ideia do uso da criptografia em sistema de posicionamento global (GPS), uma utilização real de uma ferramenta de criptografia com fim extremamente importante para a ciência. A desvantagem dos algoritmos de chave simétrica é a exigência de uma única chave secreta compartilhada, com uma cópia em cada extremidade. As chaves estão sujeitas à descoberta potencial por um adversário criptográfico, por isso necessitam ser mudadas frequentemente e mantidas seguras durante a distribuição e no serviço. Essa exigência de escolher, distribuir e armazenar chaves sem erro e sem perda, é conhecida como “gerenciamento de chave”.

Os algoritmos de chave simétrica não podem ser usados para finalidades de autenticação. Para finalidades de autenticação, geralmente são usadas funções de hash, por exemplo MD5.

BIBLIOGRAFIA

[1] **GPS (Sistema de Posicionamento Global)**, https://www.infoescola.com/cartografia/gps-sistema-de-posicionamento-global

[2] **Sistema de Posicionamento Global**, https://pt.wikipedia.org/wiki/Sistema_de_posicionamento_global

[3] **Sistema Brasileiro de Coleta de Dados Ambientais: Status e planos futuros,** http://marte.sid.inpe.br/attachment.cgi/dpi.inpe.br/sbsr@80/2008/11.17.21.20.46/doc/1633-1640.pdf

[4] **Técnica de Criptografia com Dados Geodésicos**, http://tede2.pucrs.br/tede2/handle/tede/2990

[5] **Localizador GPS com criptografia de dados,** http://marte.sid.inpe.br/col/dpi.inpe.br/sbsr%4080/2008/11.17.14.36/doc/1617-1624.pdf

[5] **Rijndael Inspector,** http://www.formaestudio.com/rijndaelinspector/