# Criptografia de Dados GPS em uma Plataforma de Coleta de Dados (PCD)

## Segurança de Redes

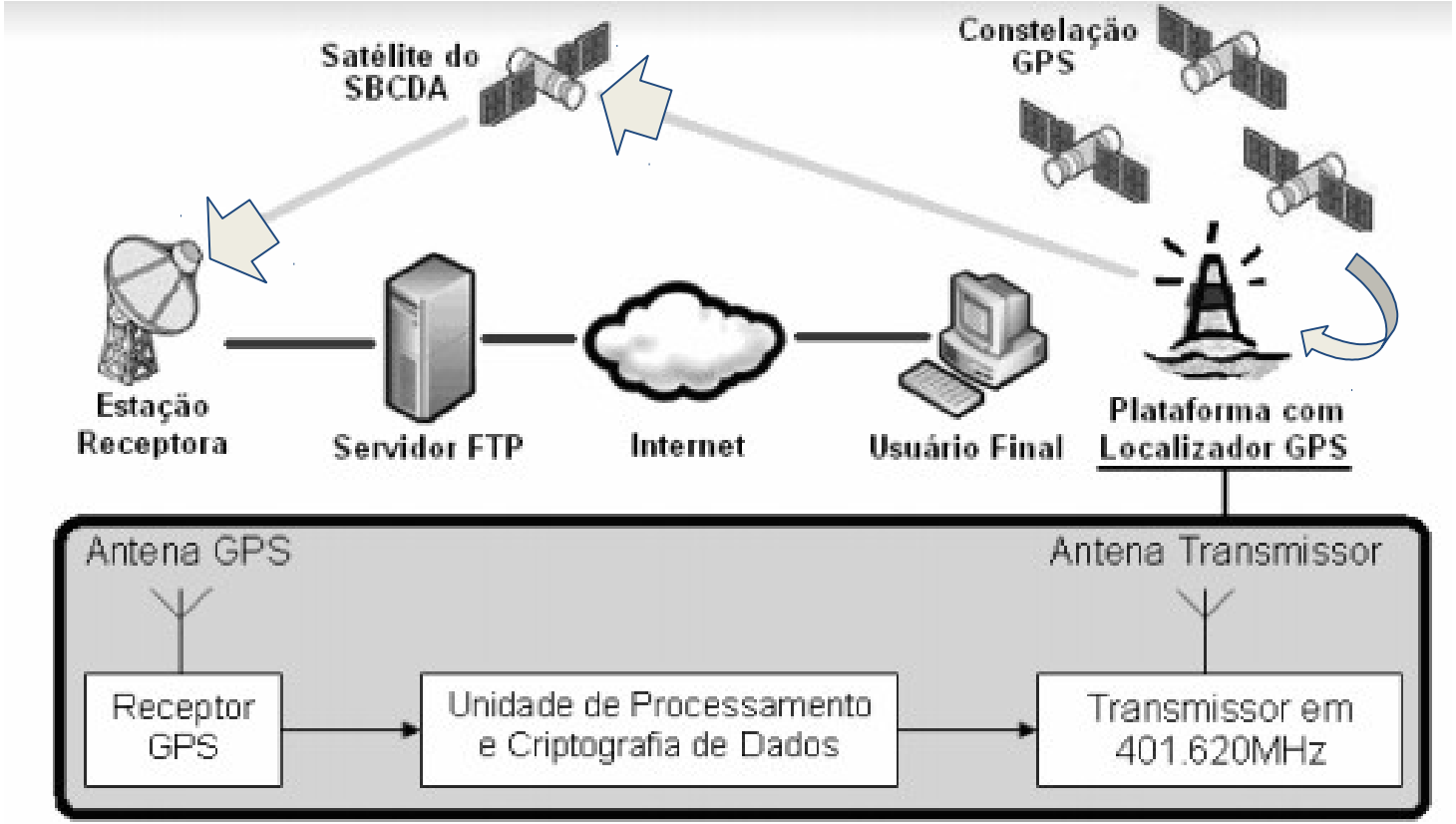
# Introdução

O Instituto Nacional de Pesquisas Espaciais (*INPE*) desenvolve satélites que em conjunto com o Sistema Brasileiro de Coleta de Dados Ambientais (*SBCDA*) são utilizados para comunicação com ênfase em aplicações de coletas de dados ambientais.

Os satélites *(INPE + SBCDA)* são utilizados pelas Plataformas de Coleta de Dados (*PCD*) como meio de comunicação para transmissão dos dados até as estações de recepção. Estes dados recebidos são posteriormente enviados ao Centro de Missão Coleta de Dados que processa, o armazena e a difunde 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.


Satélite do SBCDA
Constelação GPS
Estação Receptora
Servidor FTP
Internet
Usuário Final
Plataforma com Localizador GPS
Antena GPS
Antena Transmissor
Receptor GPS
Unidade de Processamento e Criptografia de Dados
Transmissor em 401.620MHz

# Ameaças e Requisitos de Segurança

Os dados coletados pelos satélites (*INPE + SBCDA*) devem ser de interesse científico ou de monitoramento ambiental ou de proteção ambiental.

Um possível problema seria 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.

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.

Outro exemplo seria uma empresa que modifica os dados para continuar aproveitando de um pedaço de terra para o desmatamento, ou para obtenção de recursos. Empresas motivadas por poder e ganância.

# Implementação de Segurança

A implementação da segurança segue os seguintes passos:

1. Coleta dos dados pelo *PCD* (Plataforma de Coleta de Dados).
2. Os dados são capturados com o auxílio do dispositivo GPS que envia os mesmos para uma unidade de processamento e criptografia de dados, onde estes são processados por um microcontrolador *PIC*.
3. O GPS utiliza o protocolo *NMEA-0183* e o microcontrolador escolhido foi o *PIC18F4550*.

O PIC18F4550 realiza o processamento e criptografia dos dados de posição geográfica (linguagem C). O *PIC* recebe a mensagem completa (estabelecida pelo protocolo *NMEA-0183*) armazenando somente os dados necessários para a criação do campo final da mensagem *“header 0”*. Aplicando sobre este campo o algoritmo de criptografia *AES* (Rijndael) para então transmitir os dados aos satélites do *SBCDA*. O formato *“header 0”* provê a cada pacote uma posição absoluta (Última posição na qual foi realizada a aquisição de dados pelo receptor *GPS*) e três posições relativas, estabelecendo um campo final de 160 bits.

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

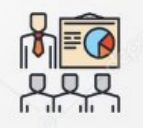
| Δ Latitude | Δ Longitude | Delay | Time Index |
|---|---|---|---|
| 13 bits | 13 bits | 4 bits | 2 bits |

As posições relativas são juntamente transmitidas com a absoluta com o intuito de oferecer um “histórico” da posição ao usuário, porque 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).

# Discussão Crítica

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.

O 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



| 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] |

| 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] |

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*.

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.


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*.

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”.

# Obrigado!

Contato:
(54) 99176-3745
Victor Dallagnol Bento
victor.bento@ecomp.ufsm.br