Atenuando as Vulnerabilidades do GPS

Shankar Achanta, Steve T. Watt e Eric Sagen
Schweitzer Engineering Laboratories, Inc.

Apresentado na
Power and Energy Automation Conference
Spokane, Washington, EUA
10–12 de março de 2015

Edição original lançada em março de 2014

Traduzido para o português em fevereiro de 2017

Atenuando as Vulnerabilidades do GPS

Shankar Achanta, Steve T. Watt e Eric Sagen, *Schweitzer Engineering Laboratories, Inc.*

***Sumário*—O Sistema de Posicionamento Global (GPS) é um sistema de navegação global por satélite que é onipresente em aplicações como navegação, construção e sincronização de tempo preciso. Esta tecnologia de transmissão de sinal econômica, operada pelo Departamento de Defesa dos EUA, fornece precisão na sincronização de tempo de algumas dezenas de nanossegundos. A tecnologia GPS tornou-se parte integrante das aplicações de sistemas das concessionárias de energia para sincronização de tempo. Nos últimos anos, ameaças e vulnerabilidades foram identificadas, tais como interferências ("jamming"), explosões solares e ataques ao sinal do GPS ("GPS spoofing"), as quais podem afetar a operação correta dos sistemas de controle e proteção das concessionárias de energia.**

Este artigo fornece uma visão geral das tecnologias e sistemas baseados em tempo normalmente utilizados para fornecer tempo preciso. O artigo discute as vulnerabilidades do sistema de tempo baseado em GPS e explica como projetar sistemas de distribuição de tempo resilientes para aplicações do sistema de potência visando atenuar estas vulnerabilidades.

I. Introdução

O conceito de tempo preciso encontrou sua utilização em diversas aplicações do passado recente, e a tecnologia continua a pressionar os limites para a exatidão do tempo. Sistemas de Navegação Global por Satélite (GNSSs: "Global Navigation Satellite Systems) de diferentes países são usados para determinar precisamente uma posição exata em qualquer ponto na Terra, com uma precisão tão baixa quanto 1 milímetro, e o tempo exato, com uma precisão de nanossegundos (10^{-9}). Estes sistemas também são usados para determinar a velocidade e a direção de viagens, tornando-os muito valiosos para várias aplicações.

O Sistema de Posicionamento Global (GPS: "Global Positioning System"), operado pelos Estados Unidos, é um exemplo popular de um GNSS que passou a ser uma tecnologia usada em diversas aplicações e indústrias. Este artigo discute a tecnologia GPS juntamente com escalas de tempo e métodos de distribuição de tempo para aplicações de tempo preciso, apresentando uma visão geral resumida dessas aplicações. Este trabalho também discute algumas das vulnerabilidades encontradas pela tecnologia GPS, concluindo com técnicas para mitigação destas vulnerabilidades.

II. Escalas de Tempo

Antes de discutirmos a tecnologia GPS, vamos considerar várias escalas de tempo disponíveis atualmente.

A. Tempo Atômico Internacional (TAI)

TAI ("International Atomic Time") é um padrão de tempo atômico baseado na média do tempo ponderada mantida por mais de 200 relógios atômicos de cerca de 50 laboratórios científicos ao redor do mundo. Como ele usa a média de vários relógios atômicos, este tempo é o tempo mais preciso conhecido pela humanidade.

B. Tempo Universal (UT)

UT ("Universal Time") é definido pela rotação da Terra, que é determinada atualmente por satélites GPS que estão em órbita na Terra. Anteriormente, este tempo era derivado de observações astronômicas. UT1 é uma versão de UT que corrige o desvio polar da Terra, que é um desvio do eixo rotacional da Terra. UT e UT1 diferem por algumas dezenas de milissegundos.

C. Tempo Universal Coordenado (UTC)

UTC ("Coordinated Universal Time") foi introduzido para considerar os efeitos da rotação da Terra na determinação do tempo ("timekeeping"). UTC e TAI variam entre si por *m* segundos, onde *m* representa os segundos intercalados ("leap seconds") que podem ser incrementados ou subtraídos em 30 de junho ou 31 de dezembro de cada ano.

$$\mathrm{UTC} = \mathrm{TAI} - (10 + \mathrm{m}) \tag{1}$$

Os segundos intercalados são responsáveis por um ajuste de tempo com base na redução ou aceleração da rotação da Terra. O Serviço Internacional dos Sistemas de Referência e Rotação da Terra (IERS: "International Earth Rotation and Reference Systems Service") publica o evento de ocorrência de segundos intercalados com seis meses de antecedência.

A Fig. 1 mostra a diferença entre as escalas de tempo de TAI e UTC desde o ano de 1972. Na ocasião da elaboração deste artigo, a diferença entre TAI e UTC era de 35 segundos.

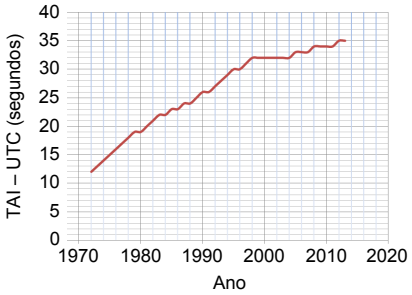

Fig. 1. Diferença de tempo entre as escalas de tempo TAI e UTC desde 1972 devida às inserções dos segundos intercalados.

D. Tempo GPS

O tempo GPS é sincronizado com o TAI. A época de referência inicial do tempo GPS é a meia-noite (UTC) de 6 de janeiro de 1980. Os segundos intercalados não são adicionados ao tempo do GPS. Portanto, a diferença entre o tempo UTC e GPS varia em incrementos de segundos cada vez que um segundo intercalado é adicionado à escala de tempo UTC.

Tempo GPS = TAI – 19 segundos (2)

E. Número da Semana GPS

O número da semana GPS é o número da semana começando a partir do tempo da época do GPS (6 de janeiro de 1980). As semanas são numeradas desde 0 e vão até 1.023 e então retornam para 0. Este ciclo da contagem ("rollover cycle") tem 1.024 semanas ou 7.168 dias, que representa aproximadamente 19,6 anos civis. É importante para os dispositivos de determinação do tempo que usam GPS (tais como receptores e relógios GPS) lidar com o ciclo de contagem do número da semana GPS para garantir que o tempo exato seja reportado.

F. Tempo Local

Tempo local é específico para o local e geralmente tem um deslocamento ("offset") em relação ao tempo UTC. Durante a comunicação entre locais geograficamente separados, é importante usar UTC e não o tempo local para evitar confusão na análise das estampas de tempo do evento.

A Fig. 2 mostra a diferença entre as escalas de tempo a partir de dezembro de 2013.

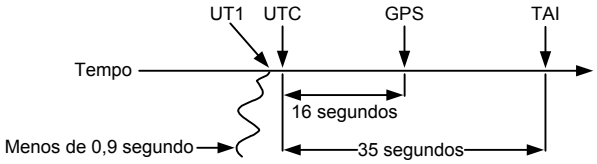

Fig. 2. Diferença entre UT1, UTC, GPS e TAI a partir de dezembro de 2013.

Agora que várias escalas de tempo foram introduzidas, vamos verificar diferentes métodos de distribuição de tempo e saídas de tempo que são geradas a partir dessas escalas de tempo para uso comercial e civil.

III. Métodos de Distribuição de Tempo

A. Métodos de Distribuição de Área Ampla

1) GNSSs

Os GNSSs usam os tempos de trânsito do sinal para determinar a localização, velocidade e tempo preciso através de receptores GNSS na Terra, os quais recebem sinais por meio de tecnologias sem fio dos satélites em órbita. Existem vários GNSSs em serviço atualmente em todo o mundo.

O GPS dos Estados Unidos é o GNSS mais conhecido. Outros incluem o sistema russo GLONASS e, num futuro próximo, o sistema chinês Compass e o sistema europeu Galileo. Todos estes sistemas transmitem os sinais de tempo com frequências da portadora ("carrier") na faixa de 1.200 a 1.800 MHz.

2) Estações de Rádio Baseadas na Terra

Antes de existirem os GNSSs, estações de rádio baseadas na terra como a WWVB e a Navegação de Longo Alcance (LORAN: "Long Range Navigation") eram populares para distribuição de tempo preciso rastreável ao UTC ("traceable to UTC"). A estação WWVB, localizada no Colorado, Estados Unidos, transmite informações de tempo rastreável ao UTC usando uma portadora de rádio em 60 kHz. Este tempo pode ser decodificado pelos receptores da WWVB da América do Norte, dependendo da proximidade dos receptores da estação WWVB. Embora a WWVB transmita sinais de tempo muito precisos em relação ao UTC, a precisão do tempo no receptor é afetada pelos atrasos de propagação do sinal e pela incerteza do cruzamento pelo zero da onda portadora. Com técnicas de processamento de sinais digitais e compensação de atrasos, precisões de até 1 milissegundo podem ser obtidas usando os sinais WWVB [1].

B. Métodos de Distribuição de Área Local

Uma vez que os sinais de tempo tenham sido recebidos através dos métodos de distribuição de área ampla, estes sinais têm de ser convertidos em um formato que possa ser facilmente processado pelos dispositivos eletrônicos inteligentes (IEDs: "Intelligent Electronic Devices") a jusante. Existem várias normas que descrevem os formatos que são usados para distribuir o tempo localmente através de uma rede. Exemplos populares incluem IRIG-B, Protocolo de Tempo de Rede (NTP: "Network Time Protocol"), e Protocolo de Precisão de Tempo (PTP: "Precision Time Protocol") baseado na IEEE 1588. Cada um desses métodos de distribuição possui suas próprias vantagens e desvantagens, e sua utilização depende do nível de precisão dos tempos das aplicações.

A Tabela I compara os métodos populares de distribuição de tempo de área local.

TABELA I
MÉTODOS DE DISTRIBUIÇÃO DE TEMPO DE ÁREA LOCAL

Método de Distribuição de Tempo	IRIG-B	NTP	PTP (IEEE 1588 e IEEE C37.238)
Camada Física	Cabo coaxial	Ethernet	Ethernet
Modelo	Mestre-escravo	Cliente-servidor	Mestre-escravo
Precisão da Sincronização	~100 ns a 1 µs	~1 a 100 ms	~100 ns a 1 µs
Compensação para Latência	Sim, usando comprimento do cabo como entrada do usuário	Sim	Sim
Intervalo de Atualização	Uma vez por segundo, pulso por segundo	Minutos	Configurável (tipicamente uma vez por segundo)
Requisitos de Hardware	Hardware especial exigido para mestre e escravo	Somente mestre	Suporte requerido para alta precisão
Custo Relativo de Implementação	Médio (cabeamento IRIG-B)	Baixo (software)	Médio a alto (cada dispositivo tem de suportar PTP para melhor precisão)

IV. Osciladores e Padrões de Césio

Os osciladores são um componente crítico e essencial para qualquer dispositivo de determinação do tempo. Esses componentes são regulados ou condicionados por uma fonte

de tempo externa (por exemplo, GPS) e mantêm o tempo no dispositivo ou instrumento local. As características destes componentes são fundamentais para obter precisão nas aplicações de tempo preciso. Esta seção descreve alguns conceitos básicos para osciladores e padrões de césio.

A. Osciladores

Qualquer dispositivo que produz sinais de saída de tempo possui um oscilador. Cada relógio é constituído por dois componentes. O primeiro componente é um dispositivo de oscilação que calcula a duração de um segundo ou o intervalo de tempo desejado. Este oscila pelas leis da física e é referido como um padrão de frequência. Exemplos disso incluem o clássico pêndulo que oscila com uma determinada frequência (mostrado na Fig. 3). O segundo componente de um relógio é um dispositivo que computa essas transições periódicas de forma cumulativa para produzir um valor resultante (geralmente digitalizado) que pode ser usado para gerar uma variedade de sinais, tais como pulsos por segundo.

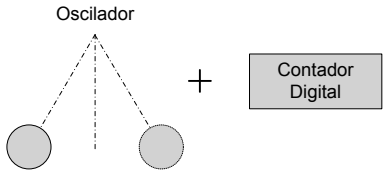

Fig. 3. Ilustração de um relógio.

Nos equipamentos eletrônicos mais modernos que têm circuitos ativos, há um oscilador de cristal. Quando certos cristais são submetidos ao estresse mecânico, eles produzem sinais elétricos através dos lados opostos do cristal. Por outro lado, quando um potencial elétrico é aplicado, estes cristais produzem vibração mecânica. Isto é conhecido como efeito piezoelétrico. O quartzo tem excelente estabilidade mecânica e imunidade suficiente para condições ambientais externas. Quando um cristal de quartzo é conectado em um circuito eletrônico de *loop* fechado, ele pode ser usado como uma fonte confiável para frequência e tempo nos dispositivos eletrônicos [1].

Para qualquer dispositivo de frequência, o número de eventos por unidade de tempo (por exemplo, oscilações) é conhecido como frequência.

$$F = 1/T \tag{3}$$

onde:

T é o período de tempo ou o tempo entre os eventos.

Algumas das características comuns inerentes aos osciladores de cristal são as seguintes:

- Envelhecimento (“Aging”) é definido como a mudança na frequência de um oscilador devido a mudanças internas, ao invés de fatores externos como temperatura e fonte de alimentação.
- Precisão (“Accuracy”) é o valor calculado ou medido da estabilidade da frequência de um oscilador. Isto define a qualidade do oscilador.
- Escorregamento/Desvio (“Drift”) é a variação da frequência com relação ao tempo em uma aplicação que usa osciladores. Isto inclui fatores internos como envelhecimento e fatores externos como temperatura e fonte de alimentação para o oscilador.
- Deslocamento (“Offset”) é a diferença entre a frequência real e a especificada para um oscilador.

B. Padrão de Césio

A definição oficial atual de um segundo baseia-se em um átomo de césio. O segundo é definido como a duração de 9.192.631.770 períodos de radiação correspondentes à transição entre os dois estados não perturbados de um átomo de césio. O padrão de césio é considerado o principal padrão de frequência pela sua precisão e estabilidade de longo prazo. Isto também é conhecido como um relógio atômico ou padrão atômico.

Existem outros padrões de tempo e frequência, tais como OCXOs (“Oven Controlled Crystal Oscillators”), TCXO (“Temperature Compensated Crystal Oscillators”) e os padrões de rubídio que são usados em dispositivos de determinação do tempo, dependendo dos requisitos da aplicação.

V. Sistema de Posicionamento Global

O GPS (mostrado na Fig. 4) fornece um sinal de tempo de alta precisão [1].

O GPS é um dos mais populares e bem-sucedidos GNSSs disponíveis atualmente. A tecnologia GPS teve um enorme crescimento em diversos setores de negócios desde sua criação, tornando-se uma parte essencial da infraestrutura de comunicações de dados em todo o globo. A disponibilidade gratuita desta tecnologia habilitou muitas aplicações através de uma variada faixa de indústrias, incluindo aviação, segurança pública, lazer, telecomunicações, transporte, mapeamento e topografia, finanças e concessionárias de energia.

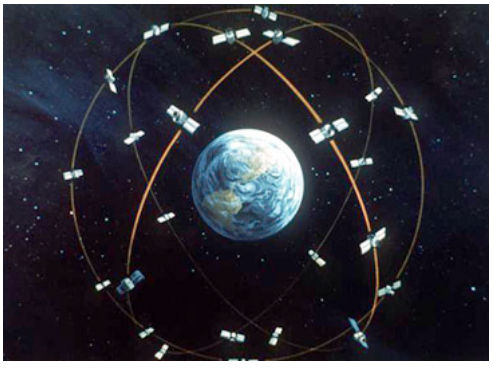

Fig. 4. O Sistema de Posicionamento Global. Esta imagem foi fornecida como cortesia do Departamento de Defesa dos EUA.

O GPS é composto por três segmentos, a saber: espacial, controle e usuário. A Fig. 5 mostra como estes três segmentos formam o sistema GPS.

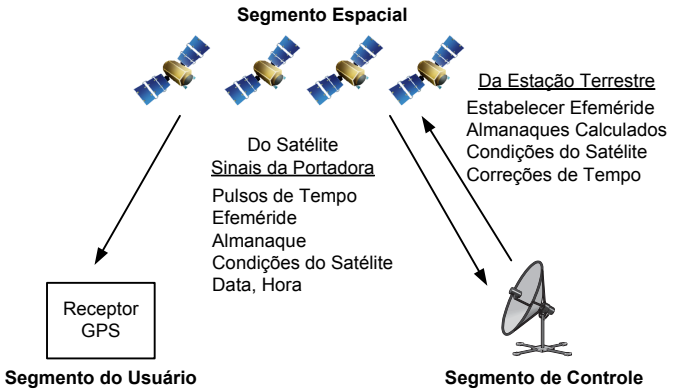

Fig. 5. Os três segmentos do GPS.

A. Segmento Espacial

O segmento espacial é composto por uma constelação de satélites orbitando a Terra, os quais transmitem sinais de rádio para os usuários. Há mais de 24 satélites disponíveis para aplicações civis. Os satélites orbitam em seis planos orbitais ao redor da Terra, duas vezes por dia, a uma altitude de cerca de 12.000 milhas. Estes planos orbitais são projetados de tal forma que há pelo menos seis satélites visíveis em qualquer parte da Terra em todos os instantes. A constelação de satélites do GPS é controlada pela Força Aérea dos EUA, que é responsável por melhorias e manutenção periódica.

Cada satélite transmite informações, conhecidas como uma mensagem de navegação, a uma taxa de 50 bits por segundo.

As mensagens de navegação dos satélites são geradas usando um processo denominado técnica de Espalhamento Espectral por Sequência Direta (DSSS: "Direct-Sequence Spread-Spectrum"). DSSS é uma técnica onde um sinal de informação ocupando uma banda de frequência estreita é combinado com um sinal de frequência mais alta para gerar um sinal que ocupa uma banda de frequência mais larga. O sinal de frequência mais alta é frequentemente um sinal digital que é gerado de forma pseudoaleatória. O sinal resultante que ocupa uma faixa de frequência mais larga é transmitido pelo canal de comunicação e é decodificado pelo receptor, combinando o sinal recebido com o mesmo sinal de alta frequência pseudoaleatório. A Fig. 6, Fig. 7 e a Fig. 8 ilustram a técnica DSSS.

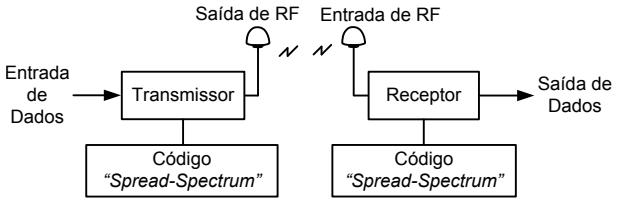

Fig. 6. A técnica DSSS.

Na Fig. 6, Entrada de Dados ("Data In") é a informação para o transmissor, que é combinada com o código de espalhamento espectral ("spread-spectrum"). O sinal resultante é transmitido através de um canal de comunicação sem fio. Na extremidade do receptor, o mesmo código de espalhamento espectral é usado para recuperar a informação enviada pelo transmissor [2].

Isto pode ser explicado no domínio da frequência, conforme mostrado na Fig. 7.

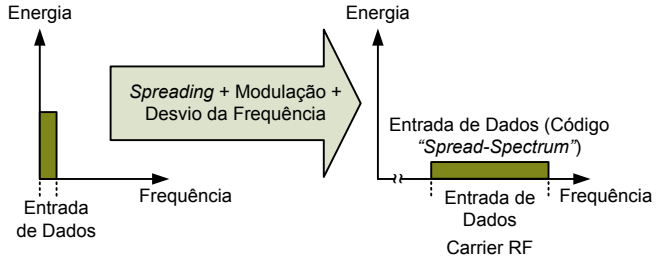

Fig. 7. Espalhamento do sinal.

No bloco de transmissão, os dados de entrada são submetidos às operações de espalhamento ("spreading") e modulação e são espalhados e deslocados (para transmissão sem fio) na frequência. Na extremidade receptora, a operação inversa ao espalhamento ("despreading") e a demodulação são executadas para extrair os dados originais, conforme mostrado na Fig. 8.

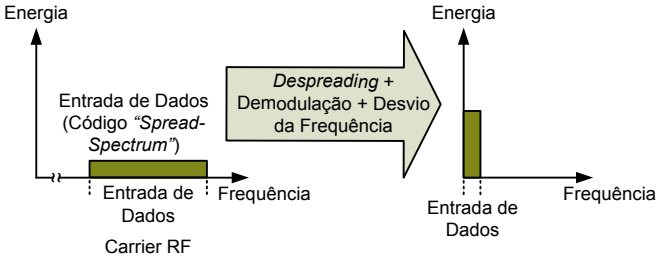

Fig. 8. Operação inversa ao espalhamento ("despreading") do sinal.

Há diversas vantagens no uso da comunicação DSSS, incluindo resistência à interferência e "jamming". Outro benefício importante é a coexistência de transmissores simultâneos compartilhando a mesma faixa de frequência e comunicando-se com múltiplos receptores. Embora todos os transmissores usem a mesma faixa de frequência e transmitam sinais simultaneamente, os receptores podem receber e recuperar os sinais de cada um dos transmissores usando os códigos de espalhamento espectral. Os satélites GPS do segmento espacial usam a mesma técnica DSSS, uma vez que eles transmitem os sinais de satélite para a Terra usando códigos exclusivos de espalhamento espectral (também conhecidos como códigos de números pseudoaleatórios [PRN: "Pseudorandom Number"]) para cada satélite. Um diagrama de blocos simplificado do satélite é mostrado na Fig. 9 [3].

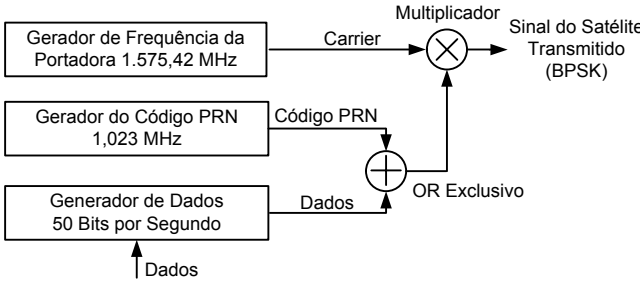

Fig. 9. Diagrama de blocos simplificado do satélite.

Cada satélite possui quatro relógios atômicos extremamente estáveis. Estes relógios são usados para gerar a radiofrequência (RF) de 1.575,42 MHz (também conhecido como um sinal L1) e um sinal de tempo para o gerador de sequência do PRN de 1,023 MHz e um sinal de 50 Hz para os dados. Os dados a 50 bits por segundo são combinados (através de uma operação OR exclusiva) com o código de espalhamento PRN (exclusivo para cada satélite) de 1,023 MHz. O sinal resultante de 1,023 MHz é modulado usando a frequência da portadora de 1.575,42 MHz para transmissões sem fio. O formato de modulação usado é o Chaveamento de Fase Binário (BPSK: "Binary Phase Shift Keying"), onde o sinal muda a fase em 180 graus cada vez que ocorre uma transição de dados de 0 para 1 ou de 1 para 0.

B. Segmento de Controle

O segmento de controle consiste de uma estação de controle mestre localizada no Colorado e várias estações de controle terrestres que se comunicam com os satélites. O segmento de controle executa o seguinte:

- Fornece os dados orbitais de todos os satélites (almanaque) para cada satélite.
- Corrige o tempo a bordo dos satélites.
- Observa e prevê o comportamento dos relógios nos satélites.
- Observa o movimento orbital dos satélites e calcula os dados da órbita para cada satélite (efeméride).
- Transmite as informações relativas às condições do satélite e erros do relógio.

C. Segmento do Usuário

O segmento do usuário compreende os dispositivos e tecnologias que recebem os sinais GPS e os utilizam para várias aplicações. Os receptores GPS precisam receber sinais GPS válidos a partir de pelo menos três satélites GPS para determinar a latitude, longitude e altitude de uma posição e receber sinais de um satélite GPS adicional para determinar o tempo. Os receptores GPS disponíveis comercialmente possuem normalmente 12 canais receptores, significando que o receptor pode rastrear simultaneamente até 12 satélites GPS. Os receptores GPS têm os mesmos códigos PRN que neles estão programados, os quais são compatíveis com os códigos da constelação de satélites GPS. Os receptores usam esses códigos para recuperar o sinal recebido e sincronizar os respectivos relógios locais com os relógios dos satélites GPS. Isso propicia a cada receptor GPS a capacidade de gerar uma referência de tempo com a mesma precisão dos relógios atômicos usados dentro de cada satélite GPS.

Há uma outra banda de frequência para os sinais GPS, conhecida como um sinal L2, que opera com uma frequência da portadora de 1.227,6 MHz. Os sinais da portadora L2 são transmitidos simultaneamente com os sinais L1 a partir dos satélites GPS com criptografia especial. A criptografia para os sinais GPS L2 é introduzida no código PRN para estes sinais. Os sinais GPS L2 são usados em aplicações militares dos Estados Unidos para fornecer posicionamento e tempo precisos. Os receptores que podem descriptografar sinais L2 precisam ser autorizados pelo Departamento de Defesa dos EUA, e esses receptores estão protegidos contra ataques ao sinal do GPS ("GPS spoofing").

Devido à enorme proliferação da tecnologia GPS, existem receptores GPS disponíveis comercialmente com um custo muito baixo. Estes receptores são receptores civis que rastreiam e decodificam os sinais L1 do GPS e não podem descriptografar os sinais L2. Estes dispositivos são muitas vezes utilizados em combinação com projetos de aplicação específica para criar um produto final que resolva o problema de um cliente. Além disso, existem receptores GPS especializados disponíveis para aplicações de tempo preciso que usam informações do satélite GPS para produzir sinais de tempo tão precisos quanto 100 nanossegundos em relação ao UTC. A Fig. 10 e a Fig. 11 mostram o desempenho do tempo de receptores GPS típicos disponíveis atualmente [4]. O Receptor B, mostrado na Fig. 11, tem um controle mais rígido (menor variação na precisão do tempo) do que o desempenho do tempo do Receptor A (mostrado na Fig. 10).

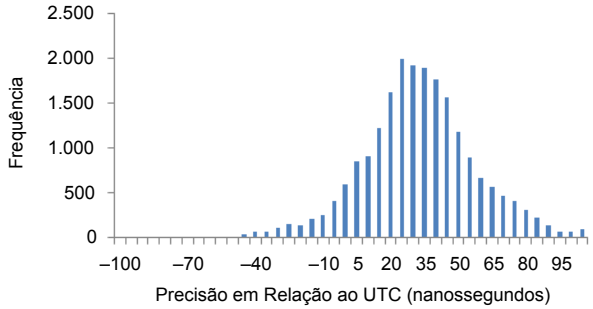

Fig. 10. Desempenho do tempo do Receptor A.

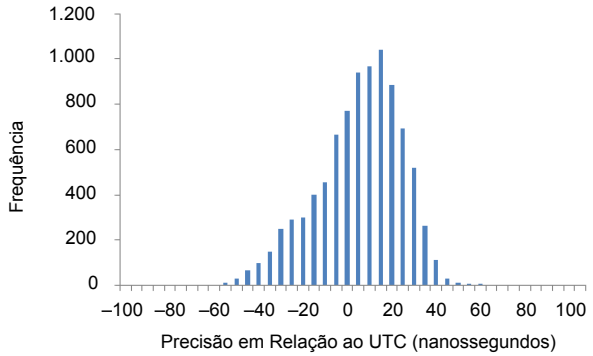

Fig. 11. Desempenho do tempo do Receptor B.

VI. Aplicações de Tempo Preciso em Sistemas de Potência

As concessionárias de energia elétrica necessitam de tempo preciso para entrega e controle eficiente das redes de transmissão e distribuição de energia elétrica. As concessionárias de energia contam com relógios sincronizados por GPS para sincronizar os dispositivos de subestações, centros de controle e circuitos de alimentadores da distribuição. Ter o tempo preciso disponível em toda a rede de energia permite que as concessionárias efetuem um melhor controle e monitoramento do sistema de potência com tempos de resposta mais rápidos, visando gerenciar de forma eficaz as perturbações e, consequentemente, evitar *blackouts* no sistema.

As subseções seguintes discutem algumas das aplicações das concessionárias de energia para o tempo preciso.

A. Registro de Perturbações

Quando ocorrem faltas no sistema de potência, é importante alinhar os dados registrados por diversos IEDs para efetuar uma análise pós-evento, a qual inclui a descoberta da causa raiz que provocou a falta, bem como a avaliação da gravidade e duração da falta. Normalmente, uma precisão de 1 milissegundo é adequada para este tipo de caracterização. A sincronização de tempo foi perdida durante o *blackout* de 2003 no Nordeste da América do Norte, levando vários meses para que os engenheiros das concessionárias sincronizassem os relatórios dos eventos e determinassem a causa principal do *blackout*. Os relatórios de eventos com estampas de tempo precisas simplificam enormemente a tarefa de uma análise básica da interrupção, bem como de uma análise em larga escala da perturbação e do *blackout*. A proposta mais recente da NERC ("North American Electric Reliability Corporation") exige que os eventos tenham uma estampa de tempo com precisão de um quarto de ciclo (aproximadamente 4 milissegundos em 60 Hz) [5].

Embora este requisito de precisão pareça ser muito fácil de obter, uma vez que as precisões dos relógios baseados na recepção de GPS estão no intervalo de nanossegundo, todos os fatores de erro têm que ser considerados, incluindo o tempo de ativação das entradas do sinal de tempo e a frequência de amostragem dos IEDs utilizando os sinais do tempo.

B. Relatórios do Registrador Sequencial de Eventos (SER)

Um relatório do Registrador Sequencial de Eventos (SER: "Sequential Events Recorder") fornece uma lista cronológica das mudanças de estado que ocorreram no IED durante a sua operação. Esses estados podem ser o fechamento ou abertura de um contato de saída de teleproteção, alarmes, ou estado lógico dos elementos da lógica interna. Uma análise desses eventos pode ser muito útil para solucionar os problemas de operação do IED e monitorar as mudanças de estado. Um requisito típico para precisão da sincronização do tempo para esta aplicação é 1 milissegundo.

Os registradores de evento e relés digitais produzem relatórios do SER ou da Sequência de Eventos (SOE: "Sequence of Events"), os quais fornecem uma lista cronológica de quando os dispositivos monitorados mudaram de estado. Mudanças de estado podem ser abertura ou fechamento, ativação ou desativação, ligar ou desligar, e assim por diante. Os pontos de monitoramento do dispositivo podem incluir contatos de estado do disjuntor, contatos de saída do relé de proteção e da teleproteção e, nos IEDs modernos, os estados lógicos dos elementos da lógica interna.

C. Localização de Faltas no Sistema de Potência

A localização de faltas através de ondas viajantes usa o tempo de chegada das Ondas Viajantes (TWs: "Traveling Waves") que são geradas quando ocorrem faltas nas linhas de transmissão. As TWs trafegam em direção a ambas as extremidades da linha de transmissão, e alcançam as extremidades em momentos diferentes de acordo com a localização da falta. Para localizar as faltas com precisão utilizando a TW, é importante ter uma referência de tempo precisa em cada extremidade da linha e trocar esta informação entre as duas extremidades através de um canal de comunicação confiável. Como a TW trafega com a velocidade da luz, pequenos erros na sincronização de tempo podem conduzir a grandes erros na determinação da localização da falta. Por exemplo, um erro de 2 microssegundos pode criar uma incerteza de 600 metros na localização da falta. Felizmente, existem várias técnicas de distribuição de tempo, incluindo GPS, que fornecem precisões de submicrossegundo.

Existem dispositivos de comunicações digitais projetados para infraestrutura crítica que distribuem o tempo ao longo de uma rede de área ampla (WAN: "Wide-Area Network") independentemente do GPS. Técnicas de distribuição de tempo terrestre também podem ser utilizadas para este propósito, as quais têm uma vantagem sobre o GPS, considerando que são menos susceptíveis a *spoofing* ou *jamming*. A Fig. 12 mostra um exemplo típico de um sistema de localização de falta por ondas viajantes, o qual inclui dois relés que trocam informações do tempo de chegada através de um canal de 64 kbps usando um multiplexador. Embora os receptores GPS sejam mostrados em cada um dos relés na Fig. 12, as técnicas de distribuição de tempo terrestre também podem ser utilizadas para sincronização de tempo preciso [6].

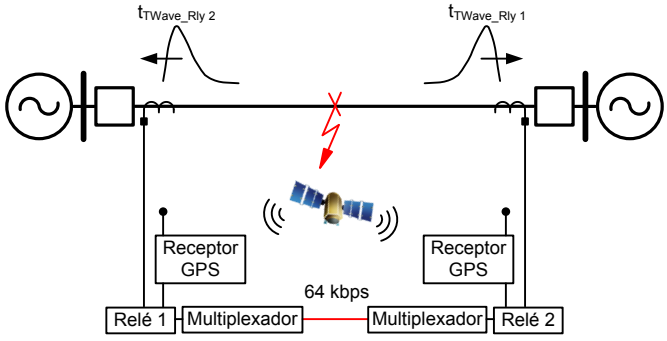

Fig. 12. Sistema de localização de faltas através de ondas viajantes.

D. Medições dos Sistemas de Potência Usando Sincrofasores Padrão IEEE C37.118.1-2011

Sincrofasores consistem de grandezas analógicas e digitais de vários dispositivos do sistema de potência com uma estampa de tempo precisa associada. Estas grandezas são coletadas e alinhadas no tempo a partir de vários IEDs do

sistema de potência. Uma referência de tempo comum para todos estes dados coletados ao longo de uma área ampla tem sido tradicionalmente usada para análise pós-evento. Recentemente, novas tecnologias permitiram que os sincrofasores sejam processados em tempo real, abrindo caminho para várias aplicações, tais como proteção e controle de área ampla em tempo real, dados de medição e valores medidos amostrados.

Um dos principais requisitos para os sincrofasores é a sincronização de tempo preciso dos dispositivos que estão amostrando as grandezas analógicas e digitais em todo o sistema de potência. A norma IEEE C37.118.1 para sincrofasores define este requisito como sendo inferior a 1 microssegundo. Observe que um erro no tempo de 1 microssegundo corresponde a um erro de fase de 0,022 grau para um sistema de 60 Hz e 0,018 grau para um sistema de 50 Hz. A norma de sincrofasores exige um vetor com erro total (TVE: "Total Vector Error") menor que 1%. Isto corresponde a um erro máximo do tempo de ± 26 microssegundos para um sistema de 60 Hz e ± 31 microssegundos para um sistema de 50 Hz. No entanto, o TVE é uma somatória dos erros de sincronização de tempo, conversão da instrumentação e erros de processamento da medição fasorial. Esta precisão inferior a 1 microssegundo pode ser obtida com fontes de tempo como GPS e métodos de distribuição como IRIG-B ou PTP.

E. Valores Medidos Amostrados

O barramento de processo envolve a transferência em alta velocidade das medições de tensão e corrente instantâneas em tempo real utilizando uma rede Ethernet. Isto é baseado na norma IEC 61850-9-2 e outras normas internacionais relacionadas. A tecnologia do barramento de processo promete fornecer perfeitamente as medições de transformadores de instrumentos inteligentes para uma grande variedade de dispositivos de proteção e controle localizados na mesma rede. Como as entradas do barramento de processo são amostradas com taxas elevadas (tipicamente 4 a 16 kHz) usando digitalizadores independentes distribuídos através da subestação, a sincronização de tempo torna-se crítica para todas as aplicações que exigem dados de múltiplos locais (por exemplo, proteção diferencial de barras).

Como a sincronização de tempo preciso das medições do barramento de processo é tão importante quanto as próprias grandezas de medição, um mecanismo tem de ser implementado para lidar com a inicialização do sistema, falhas de componentes da rede, desligamentos associados à manutenção, e outros eventos que possam afetar a entrega de dados e a sincronização de tempo. De forma similar aos sincrofasores, a precisão do tempo para os valores medidos amostrados é inferior a 1 microssegundo.

VII. VULNERABILIDADES DO GPS

O GPS depende da comunicação de satélites distantes 12.000 milhas da Terra e tem uma potência do sinal recebido de –127,5 DBm, ou $178 \cdot 10^{-18}$ watts. Considerando estes fatos, o GPS é extremamente confiável, mas tem algumas vulnerabilidades. Existem vários tipos que precisam ser considerados.

A. Explosões Solares

Uma vulnerabilidade é a interferência atmosférica, causada principalmente por explosões solares. As explosões solares consistem no aumento súbito do brilho na superfície do sol devido a uma grande liberação de energia (até $6 \cdot 10^{25}$ joules). Os raios-X e a radiação ultravioleta (UV) emitidos por explosões solares podem afetar a ionosfera, que é uma camada de 53 a 370 milhas acima da Terra. As grandes erupções solares que podem afetar o sinal GPS ocorrem aleatoriamente, mas acontecem, em média, uma a duas vezes por ano. Elas tendem a se concentrar no final de cada ciclo solar de 11 anos. As labaredas solares podem durar de poucos segundos a uma hora e podem impedir temporariamente um receptor GPS de receber um sinal.

B. GPS Jamming

Os receptores GPS também podem ser bloqueados por interferência ("jamming"), que é o ruído na faixa de frequência 1,57542 GHz usada para GPS civil. Os dispositivos de GPS *jamming* são ilegais nos Estados Unidos, mas podem ser comprados internacionalmente por menos de 100 dólares. Se um dispositivo de GPS *jamming* estiver perto de um receptor GPS, ele impede que o receptor mantenha o GPS fixo (GPS *lock)*.

C. Falhas de Antena

As falhas de antena são uma das maiores contribuintes para falhas nos sistemas de tempo GPS. Qualquer relógio que utilize um sinal de GPS requer uma antena de GPS que precisa ser instalada ao ar livre para uma melhor recepção. Isto significa que as antenas selecionadas para estes sistemas de tempo crítico precisam ser à prova de intempéries e têm de ser capazes de suportar condições ambientais adversas. Em áreas propensas a descargas atmosféricas, os sistemas de tempo muitas vezes sofrem danos na antena devido a quedas de raios. Embora seja importante escolher a antena correta para uma operação confiável dos sistemas de tempo, existem soluções como sistemas de tempo redundantes disponíveis atualmente para mitigar esses tipos de falhas.

D. Erros de Multicaminho

Erros de multicaminho também podem impedir que um receptor GPS obtenha informações precisas do GPS. Os erros de multicaminho vêm de um relógio GPS recebendo um sinal que tenha refletido em um objeto, tal como um edifício ou montanha. Devido ao atraso adicional do sinal refletido, a informação do GPS será imprecisa. A maioria dos receptores GPS é sofisticada o suficiente para ignorar os sinais de multicaminho se receberem um sinal de caminho direto, pois usam o sinal que chegou primeiro. Contudo, se o caminho direto de uma antena GPS estiver bloqueado, o dispositivo está sujeito a um erro de multicaminho.

E. GPS Spoofing

Como os sinais de GPS para uso civil não são criptografados, é possível para um atacante imitar, manipular e reproduzir um sinal L1 do GPS. *Spoofing* ocorre quando um atacante gera intencionalmente sinais que imitam de forma muito similar os sinais do GPS e os transmitem com uma potência ligeiramente superior. Quando isto é feito, um receptor GPS civil pode ser fixado ("locked") no sinal adulterado ("spoofed"), ficando susceptível a mudanças intencionais nas informações de tempo e posicionamento do GPS criadas pelo intruso.

Com explosões solares ou *jamming*, um relógio GPS detecta a perda do sinal GPS e normalmente comuta para uma fonte de tempo baseada em oscilador ("holdover"). Com erros de multicaminho, um relógio GPS não sabe que está recebendo um sinal refletido, por isso pode continuar a operar com informações de tempo ligeiramente atrasadas. Além disso, com erros de multicaminho, como o caminho direto está bloqueado, pode haver uma indicação pelo relógio de uma perda do sinal GPS.

Spoofing parece ser a vulnerabilidade mais importante a ser considerada. Quando adulterado ("spoofed"), um relógio GPS continua a operar, assumindo um sinal de GPS em condições adequadas. No entanto, este sinal pode ter sido manipulado de forma significativa, produzindo informações de tempo incorretas para a informação do evento. É importante considerar todos os tipos de vulnerabilidades do GPS e atenuar o risco associado com base na aplicação de tempo preciso e sua criticidade.

VIII. Técnicas de Mitigação

Nas subseções seguintes, apresentamos algumas abordagens e ideias para mitigar as vulnerabilidades do GPS.

A. Relógios GPS Redundantes com Distribuição de Tempo

Esta abordagem usa múltiplos relógios GPS cujos receptores são separados por uma certa distância. Cada relógio GPS recebe simultaneamente sinais GPS e produz saídas de tempo independentemente dos outros. Estes sinais de tempo são comparados através de um sistema que monitora a integridade dos mesmos. Exemplos incluem o monitoramento da perda de sinal para as saídas IRIG B de múltiplos relógios ou o monitoramento dos bits de qualidade de tempo em um código de tempo IRIG-B. Quando há uma falha da antena devido a fatores como a queda de raios, o tempo GPS pode ainda ser mantido usando a referência do relógio de um receptor GPS alternativo. Atualmente, existem sistemas de seleção IRIG-B de baixo custo disponíveis, os quais selecionam de forma confiável a melhor fonte IRIG-B com base nos sinais de perda de tempo ou qualidade do tempo. Estes sistemas também fornecem recursos adicionais, tais como compensação de atraso para que a precisão das saídas de tempo seja preservada, uma vez que o sinal passa por vários dispositivos antes de alcançar os IEDs a jusante. Esta abordagem minimiza GPS *jamming* e *spoofing* se os relógios GPS mostrados na Fig. 13 estiverem separados geograficamente por uma distância suficiente.

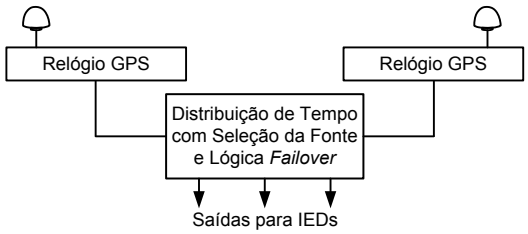

Fig. 13. Dispositivo de distribuição de tempo com seleção da fonte.

B. Fontes de Tempo Redundantes com Seleção da Fonte

Conforme discutido anteriormente, os sistemas de tempo GPS são rastreáveis ao UTC e fornecem o tempo exato com precisão da ordem de dezenas de nanossegundos. Existem vários formatos de distribuição de tempo disponíveis para uso, incluindo IRIG-B, NTP e PTP. Um esquema simples envolve sinais de tempo de múltiplas fontes, os quais são comparados uns com os outros para eliminar os valores atípicos. A Fig. 14 mostra um exemplo de um dispositivo que recebe sinais de tempo provenientes do GPS, IRIG-B, PTP e NTP.

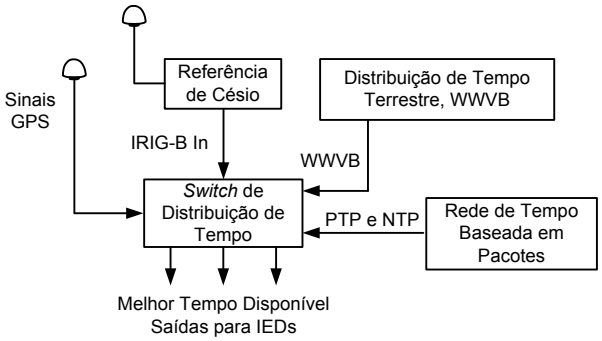

Fig. 14. *Switch* de distribuição de tempo.

O *switch* de distribuição de tempo mostrado na Fig. 14 recebe sinais de tempo provenientes de diversas fontes, todas rastreáveis à escala de tempo UTC. Este dispositivo também tem capacidade de receber sinais GPS. As entradas deste *switch* têm de ser cuidadosamente selecionadas de forma que tenham a maior diversidade. O *switch* de distribuição de tempo compara todas as entradas de tempo que chegam, monitorando vários atributos dos sinais de tempo por meio de esquemas de ponderação e técnicas de média para determinar o melhor tempo. Ele fornece este melhor tempo para os IEDs a jusante. Os algoritmos para implementação dos esquemas de ponderação e média estão fora do escopo deste artigo.

Este método não apenas reduz as interrupções de GPS locais devido a falhas de antena, *jamming* e *spoofing*, como também fornece disponibilidade do sinal de tempo sem perdas para os IEDs a jusante no caso destas falhas.

C. Distribuição de Tempo Através de WANs

Os sistemas de Rede Óptica Síncrona (SONET: "Synchronous Optical Network") são sistemas de Multiplexação por Divisão de Tempo (TDM: "Time-Division Multiplexing") que utilizam a sincronização de frequência em toda a rede para o transporte de comunicações com uma alta taxa de dados. Alguns multiplexadores SONET também são capazes de utilizar a sincronização de frequência da rede para distribuir o tempo através da rede e gerar uma referência de

tempo local, tal como IRIG-B em cada nó. Os multiplexadores SONET podem utilizar múltiplos relógios GPS ou referências de tempo em vários nós. Dependendo do tamanho da rede, cada referência de tempo pode ser separada através de uma ampla área geográfica. Estes sistemas SONET são projetados e configurados de forma que cada nó tenha seu próprio tempo local (a partir de uma antena GPS local, por exemplo) e sinais de tempo provenientes de dois nós adjacentes. O nó seleciona o melhor tempo disponível com base na comparação de pelo menos três sinais de tempo disponíveis. Isso atenua várias vulnerabilidades do GPS, incluindo falhas de antena em um único nó ou GPS *jamming* ou *spoofing* em um único nó. Esta distribuição do tempo baseada em SONET fornece uma forte camada de segurança contra um ataque malicioso ao GPS. Os nós distribuem o melhor tempo com base em todas as entradas de tempo recebidas para os dispositivos a jusante. A Fig. 15 mostra uma típica rede em anel de comunicações SONET.

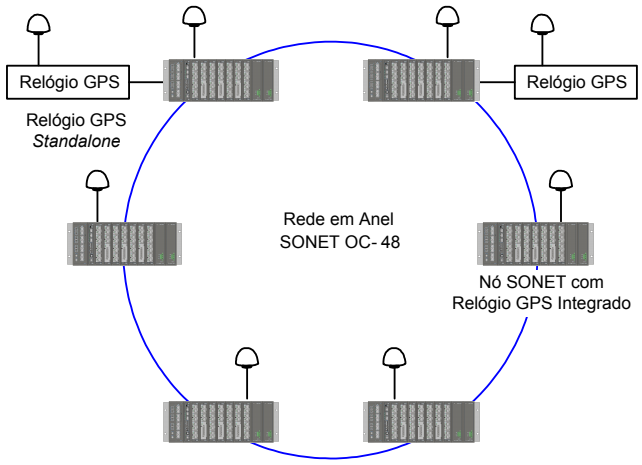

Fig. 15. Rede em anel SONET típica.

Em caso de falha total do GPS devido a eventos como explosões solares, um oscilador local de alta precisão pode permitir que a rede SONET mantenha uma precisão de tempo relativo de menos de 1 microssegundo e gere referências de tempo local para os IEDs a jusante. O diagrama da Fig. 15 mostra que alguns nós SONET podem ser configurados para ter um relógio GPS incorporado ou obter o tempo a partir de um relógio GPS separado e independente. A vantagem no uso de relógios GPS independentes é que eles vêm com opções como osciladores baseados em césio que têm uma precisão muito elevada ("holdover") no caso de perda do sinal GPS [7].

D. Referência de Césio e Caracterização do Oscilador Local

Quando os relógios do GPS recebem sinais de GPS usando os receptores de GPS embutidos nos mesmos, o receptor GPS produz um pulso de tempo que é muito preciso (dezenas de nanossegundos) em relação ao UTC. Os osciladores locais destes relógios GPS (por exemplo, TCXO e OCXO) são condicionados por esses sinais de tempo GPS. Estes osciladores combinados com alguma lógica produzem sinais de saída de tempo como IRIG-B, NTP ou PTP.

Quando os sinais GPS começam a ser desviados ("drift") devido à perda dos sinais de satélite ou à manipulação do sinal, uma abordagem para minimizar o desvio consiste em usar a caracterização do oscilador local para detectar o desvio nos sinais GPS. Como o comportamento do oscilador local pode ser caracterizado e compreendido, o envelhecimento, precisão, desvio/escorregamento (*drift*) e deslocamento (*offset*) destes osciladores podem ser usados para verificar se os sinais do GPS estão sendo comprometidos.

Nesta abordagem, o oscilador local computa o número de contagens (com base na frequência do oscilador) entre cada período de pulsos de tempo produzidos pelo receptor GPS. A acumulação desta contagem por um longo período permite a detecção de quaisquer manipulações dos sinais de tempo GPS.

Os limites para detecção destas manipulações são dependentes da tecnologia dos osciladores utilizados nestes dispositivos. Os algoritmos para efetuar esta implementação estão fora do escopo deste artigo.

E. Receptores GNSS Multiconstelação

Além do GPS, existem várias outros GNSSs que estão sendo desenvolvidos para fornecer informações como localização, tempo e velocidade para uso em várias aplicações. Estão incluídos o sistema russo GLONASS e, no futuro, o sistema chinês Compass e o sistema europeu Galileo. Existem receptores disponíveis atualmente que podem rastrear simultaneamente esses GNSSs e extrair independentemente sinais de tempo. Uma abordagem consiste em comparar os sinais de tempo recebidos por vários receptores por meio do rastreamento de diferentes GNSSs. Esta abordagem valida os sinais de tempo fornecidos por um GNSS com outro. Como estes sistemas possuem diferenças na frequência da portadora, codificação do sinal, e assim por diante, esta comparação fornece uma camada adicional de segurança contra vulnerabilidades como *jamming* e *spoofing*.

IX. Conclusão

Os GNSSs têm fornecido tempo de alta precisão e confiável por várias décadas. O GPS é o mais popular de todos os GNSSs disponíveis atualmente, tendo sofrido recentemente algumas ameaças intencionais de *jamming* e *spoofing*. Além disso, este sistema pode sofrer interferências devidas a causas naturais, tais como erupções solares e falhas no sistema de antena devido a raios. Em aplicações que dependem de GPS, tais como sincrofasores, valores medidos amostrados e localização de faltas através de ondas viajantes, é muito importante entender e lidar com essas vulnerabilidades. Este artigo descreve a tecnologia atrás da operação do GPS e fornece vários métodos para atenuar as vulnerabilidades e obter um maior grau de confiabilidade para aplicações de tempo crítico em sistemas de potência. A Tabela II resume as vulnerabilidades e as técnicas de mitigação.

TABELA II
SUMÁRIO DAS TÉCNICAS DE MITIGAÇÃO

Vulnerabilidade	Efeito	Mitigação (cf. explicado na Seção VIII)
Explosões solares	Perda do sinal	Oscilador Holdover (Subseção D), fontes de tempo redundantes com seleção da fonte (Subseção B)
GPS *Jamming*	Perda do sinal	Oscilador Holdover (Subseção D), fontes de tempo redundantes com seleção da fonte (Subseção B)
Falhas da antena	Perda do sinal	Redundância de relógio (Subseção A), oscilador Holdover (Subseção D), fontes de tempo redundantes com seleção da fonte (Subseção B)
Efeitos de multicaminho	Manipulação do sinal	Fontes de tempo redundantes com seleção da fonte (Subseção B), verificação do sinal multiconstelação (Subseção E), caracterização do oscilador local (Subseção D)
GPS *Spoofing*	Manipulação do sinal	Fontes de tempo redundantes com seleção da fonte (Subseção B), verificação do sinal multiconstelação (Subseção E), caracterização do oscilador local (Subseção D), distribuição do tempo sobre WANs (Subseção C)

X. REFERÊNCIAS

[1] E. O. Schweitzer, III, D. Whitehead, S. Achanta, and V. Skendzic, "Implementing Robust Time Solutions for Modern Power Systems," proceedings of the 14th Annual Western Power Delivery Automation Conference, Spokane, WA, March 2012.

[2] S. Achanta, B. MacLeod, E. Sagen, and H. Loehner, "Apply Radios to Improve the Operation of Electrical Protection," proceedings of the 37th Annual Western Protective Relay Conference, Spokane, WA, October 2010.

[3] Maxim Integrated, "An Introduction to Spread-Spectrum Communications," February 2003. Available: http://www.maxim-ic.com.

[4] Global Positioning System Standard Position Service Performance Standard, October 2001. Available: http://www.navcen.uscg.gov/pdf/gps/geninfo/2001SPSPerformanceStandardFINAL.pdf.

[5] North American Electric Reliability Council, "Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?" July 2004. Available: http://www.nerc.com.

[6] S. Marx, B. Johnson, A. Guzmán, V. Skendzic, and M. Mynam, "Traveling Wave Fault Location in Protective Relays: Design, Testing, and Results," proceedings of the 16th Annual Georgia Tech Fault and Disturbance Analysis Conference, Atlanta, GA, May 2013.

[7] K. Fodero, C. Huntley, and D. Whitehead, "Secure, Wide-Area Time Synchronization," proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2010.

XI. BIOGRAFIAS

Shankar V. Achanta recebeu seu MS em engenharia elétrica da Arizona State University em 2002. Ele ingressou na Schweitzer Engineering Laboratories, Inc. (SEL) em 2002 como engenheiro de hardware, desenvolvendo dispositivos de eletrônica de potência para comunicação, circuitos de aquisição de dados e fontes de alimentação chaveadas. Shankar recebeu uma patente para um gerador de código de tempo com autocalibração durante sua permanência na SEL, e é inventor de diversas patentes que estão pendentes na área de sincronização de tempo preciso e comunicações sem fio. Atualmente, ele ocupa a posição de gerente de pesquisa e desenvolvimento do grupo de tempo preciso e comunicações sem fio da SEL.

Steve T. Watt recebeu seu B.S. em engenharia mecânica do Virginia Polytechnic Institute and State University. Ele trabalhou na indústria de tecnologia da informação por mais de 20 anos na Hewlett Packard antes de ingressar na Schweitzer Engineering Laboratories, Inc. (SEL) em 2012. Steve é atualmente o gerente de produtos para produtos de tempo preciso no grupo de tempo e comunicações da SEL.

Eric Sagen recebeu seu BS em engenharia elétrica da Washington State University em 1997. Ele ingressou na General Electric na Pensilvânia como engenheiro de produtos. Em 1999, ele foi contratado pela Schweitzer Engineering Laboratories, Inc. como engenheiro de produtos de distribuição. Logo após, foi promovido para engenheiro líder de produtos de distribuição. Eric foi transferido para o grupo de tempo e comunicação em 2006 e é atualmente o engenheiro de produtos líder. Ele é certificado em Washington como Engineer in Training (EIT)

20140205 • TP6644-01