Modulo per la presentazione delle osservazioni per i piani/programmi/progetti sottoposti a procedimenti di valutazione ambientale di competenza statale

Presentazione di osservazioni relative alla procedura di:

- ❑ Valutazione Ambientale Strategica (VAS) – *art.14 co.3 D.Lgs.152/2006 e s.m.i.*
- **X** Valutazione di Impatto Ambientale (VIA) – *art.24 co.3 D.Lgs.152/2006 e s.m.i.*
- ❑ Verifica di Assoggettabilità alla VIA – *art.19 co.4 D.Lgs.152/2006 e s.m.i.*

I Sottoscritti

Prof. Ing. Davide Castagnetti
Geom. Andrea Giglioli
P.A. Livio Castagnetti
P.I. Roberto Castagnetti
P.A. Lorenzo Melioli
Prof. Ing. Andrea Boni

PRESENTANO

ai sensi del D.Lgs.152/2006, le **seguenti osservazioni** al

- ❑ Piano/Programma, sotto indicato
- **X** **Progetto, sotto indicato.**

Codice procedura (ID_VIP/ID_MATTM): 6269

Razionalizzazione della rete elettrica nazionale a 132 kV nell'Area di Reggio Emilia

Stato procedura: Istruttoria tecnica CTVIA

OGGETTO DELLE OSSERVAZIONI

- ❑ Aspetti di carattere generale *(es. struttura e contenuti della documentazione, finalità, aspetti procedurali)*
- ❑ Aspetti programmatici *(coerenza tra piano/programma/progetto e gli atti di pianificazione/programmazione territoriale/settoriale)*
- **X** **Aspetti progettuali *(proposte progettuali o proposte di azioni del Piano/Programma in funzione delle probabili ricadute ambientali)***
- **X** **Aspetti ambientali *(relazioni/impatti tra il piano/programma/progetto e fattori/componenti ambientali)***
- **X** Altro *(specificare)* **Aspetti agronomici**

ASPETTI AMBIENTALI OGGETTO DELLE OSSERVAZIONI

- ❑ Atmosfera
- ❑ Ambiente idrico
- ❑ Suolo e sottosuolo
- ❑ Rumore, vibrazioni, radiazioni
- ❑ Biodiversità (vegetazione, flora, fauna, ecosistemi)
- **X** **Salute pubblica**
- **X** **Beni culturali e paesaggio**
- ❑ Monitoraggio ambientale
- ❑ Altro *(specificare)* _____

TESTO DELL' OSSERVAZIONE

- In qualità di **membri del Comitato per l'ottimizzazione del progetto del nuovo elettrodotto di Terna a Villa Sesso**, nonché **Residenti nel Comune di Reggio Emilia in prossimità tracciato delle tratte CS2 ed RE1** relative al progetto di *Razionalizzazione della Rete Elettrica Nazionale a 132 kV nell'Area di Reggio Emilia*, tratta individuata da Terna Spa in concerto con l'amministrazione comunale di Reggio E.,

  sottoponiamo alla Vostra attenzione un documento che risponde alle

  Controdeduzioni della Società Terna Rete Italia SPA, depositate in data 11/07/2022

  (MiTE-2022-0086038).

Sezione 2.1

Controdeduzione A: Concertazione e Avviso al Pubblico

Osservazione 1

Il 10 e 11 dicembre 2019 si è svolta la seconda fase del processo di confronto con il territorio attraverso **giornate informative (Terna Incontra)** dedicate alla cittadinanza per la presentazione delle fasce di fattibilità definite. Gli incontri con i cittadini dei cinque Comuni interessati dall'opera si sono svolti a Castelnovo di Sotto, Reggio Emilia e Sant'Ilario d'Enza. Durante questi incontri i tecnici Terna hanno illustrato gli interventi previsti dal progetto e risposto alle domande dei partecipanti al fine di condividere il percorso di progettazione delle opere.
In particolare, le persone intervenute hanno potuto parlare con i progettisti e chiedere spiegazioni sulle motivazioni dell'opera e la localizzazione degli interventi, sul percorso di autorizzazione e realizzazione dell'opera; hanno potuto anche lasciare osservazioni e indicare punti di attenzione.
Le indicazioni della popolazione sono state registrate e, per quanto tecnicamente fattibile, recepite, in fase di progettazione.
Ai Terna incontra hanno partecipato circa 50 cittadini alcuni dei quali ci hanno chiesto spiegazioni sul tratto di elettrodotto aereo che va da Castelnovo verso Mancasale e lasciato osservazioni. Abbiamo ricevuto anche richieste via e-mail per i tratti di elettrodotto aereo. Di questi incontri Terna ha dato pubblicità oltre che sui giornali anche con un volantinaggio porta a porta fatto con il supporto dei Comuni nelle aree di interesse del progetto e lasciando locandine nei luoghi di maggior frequentazione.
Per garantire la massima partecipazione di tutti gli interessati Terna ha anche messo a disposizione una e-mail dedicata volta a mantenere sempre attivo il canale di comunicazione con tutti gli interessati (info.emilia@terna.it); è stata inoltre creata sul sito di Terna una pagina web dedicata all'opera nella quale è disponibile la cartografia dell'intervento: https://www.terna.it/it/progetti-territorio/progetti-incontri-territorio/terna-incontra-emilia

- Siamo assolutamente certi che Terna abbia seguito l'iter previsto dalla legislazione vigente relativamente alla Concertazione ed avviso al pubblico.
- Osserviamo però che:
  - **volantinaggio porta a porta**: nessuno dei proprietari interessati dal tracciato dell'elettrodotto ha ricevuto alcun volantino
  - le giornate **Terna Incontra** si sono svolte nel centro storico del Comune di Reggio Emilia;
  - la **frazione di villa Sesso** (Comune di Reggio Emilia) pesantemente interessata dalla tratta aerea CS2 ed RE1 avrebbe meritato una presentazione dedicata del progetto, sul territorio;
  - **i comuni interessati al progetto sono 5**, la partecipazione di 50 cittadini significa mediamente **10 cittadini per ciascun comune**: un dato di questo tipo dovrebbe fare riflettere sull'efficacia della procedura di coinvolgimento della Cittadinanza.
  - **quante sono le mail** ricevute sulla casella info.emilia@terna.it dal momento della sua attivazione?
  - a prova di tutto ciò:
    - le **770 firme raccolte in un solo giorno tra i residenti della frazione di Villa Sesso, a sostegno della Mozione Popolare per l'ottimizzazione del progetto** (documentate nelle osservazioni già depositate). La raccolta firme è avvenuta dopo soli 5 giorni dall'Assemblea Pubblica in cui si è informata la cittadinanza del progetto.
    - le **55 osservazioni pervenute al Ministero**, da singoli, da aziende, dalle Associazioni Agricole.
    - **Il Consiglio Comunale del 13/12/2021 ha approvato all'unanimità la Mozione di Iniziativa popolare e due relativi Ordini del Giorno**, dimostrando **pieno sostegno politico** a quanto chiesto dalla Cittadinanza (vedere osservazione MATTM-2021-0142358 del 20/12/2021)

Osservazione 2

In data 14/02/2020 è stato fatto un incontro con **Coldiretti Reggio Emilia**, presente il Dott. Fausto Castagnetti, Responsabile Area Economica, per condividere la fascia di fattibilità dei tratti di elettrodotto aerei nell'intento di salvaguardare le produzioni tipiche come i vigneti.

Coldiretti Reggio Emilia è solo una delle Associazioni Agricole rappresentative del tessuto imprenditoriale locale.

Oltre a questa (vedere le osservazioni presentate):

- **Confagricoltura**
- **Cia Emilia Romagna**
- **Cia Reggio Emilia**
- **Associazione UGC CISL Reggio Emilia**

Vista la delicatezza del progetto in esame, **come mai l'incontro non ha coinvolto tutte le Associazioni** rappresentative degli Imprenditori Agricoli del territorio?

La riunione in Coldiretti, si è svolta alla presenza delle Aziende associate o solo dei rappresentanti dell'Associazione?

Controdeduzione B: Aspetti paesaggistici

Osservazione 3

L'impatto del progetto in esame va considerato nella sua totalità ed è stato valutato nel SIA alto e positivo, alla luce delle numerose demolizioni di linee aeree previste, alcune delle quali in ambiti urbani residenziali o che coinvolgono territori vincolati paesaggisticamente ai sensi del D. Lgs. 42/2004.
Ciò è stato confermato nel parere tecnico istruttorio (MIC prot. n.0146251 del 28-12-2021) della Direzione Generale Archeologia Belle Arti e Paesaggio del Ministero della Cultura, pervenuto nell'abito dell'istruttoria VIA.

Occorre specificare che **i nuovi tratti di linea aerea della tratta CS2 ed RE1 nel Comune di RE, vengono realizzati in zona vergine** (quindi ha scarsa rilevanza fare un mero confronto tra il numero di tralicci tolti e quelli nuovi).

Come scritto nell'elaborato Terna RU0000006B1937518 (SIA pag. 365) e riportato nelle osservazioni già inviate, **l'impatto della tratta CS2, RE1 è alto e negativo.**

E' proprio su questa problematica che si chiede di intervenire efficacemente attraverso l'ottimizzazione del progetto.

Tabella 2.17: Impatto paesaggistico dei diversi interventi previsti dal progetto in esame

Intervento	Sensibilità	Incidenza	Impatto
SI1	Alta	Molto alta	**Molto alto e positivo**
SI2	Molto bassa	Bassa	**Trascurabile**
CS1	Bassa	Media	**Basso e positivo**
CS2, RE1	Alta	Alta	**Alto e negativo**
RE2	Bassa	Molto bassa	**Trascurabile**
RE3, RE4	Media	Molto alta	**Alto e positivo**
RE5	Alta	Molto alta	**Molto alto e positivo**
RU1	Alta	Alta	**Alto e positivo**

Figura 14 – Impatto paesaggistico del progetto in esame (Tabella tratta da elaborato Terna **RU0000006B1937518**, pag. 365)

Osservazione 4

> Il bilancio complessivo della razionalizzazione è molto positivo, riducendosi i chilometri totali di elettrodotti aerei esistenti con miglioramenti in termini di:
>
> - Diminuzione della pressione delle infrastrutture elettriche sul territorio;
> - Riduzione delle aree asservite;
> - Opportunità di costruire le nuove linee in aree lontane dai centri abitati;
> - Progettazione e scelta della localizzazione delle opere condivise.

Opportunità di costruire le nuove linee in aree lontane dai centri abitati: la linea **CS2** all'interno del Comune di Reggio Emilia e la linea **RE1** attraversano centri abitati, passano nell'adiacenza di numerose abitazioni, in certi casi nel corridoio tra abitazione e capannoni.

Osservazione 5

Si ricorda che il bilancio complessivo della razionalizzazione è il seguente:

Bilancio complessivo della razionalizzazione

	In progetto	Da demolire
km linea aerea	14	30,9
n. sostegni linea aerea	54	129
km cavo interrato	24,9	1,3

e che il bilancio per il solo Comune di Reggio Emilia è ancora migliore in termini di percentuale di linee eliminate rispetto a quelle realizzate:

Come già sottolineato nelle osservazioni inviate (MATTM-2021-0142292):

In totale quindi la tratta **CS2** è lunga **12.4 km**, di cui 0.8 km in cavo interrato nel Comune di Castelnuovo Sotto.

I rimanenti **11.6 km in linea aerea** sono organizzati nel seguente modo:

CS2 – linea aerea				
Tralicci	**Comune**	**Lunghezza**	**% del totale**	**Tracciato**
da 1 a 20	Castelnuovo Sotto	6.3 km	**54%**	Lungo elettrodotto esistente
da 20 a PG1	**Reggio Emilia**	**5.3 km** (di cui 1.7 km in doppia terna)	**46%**	**Completamente nuovo**

Si osserva quindi che **la linea aerea della tratta CS2, per il 46% della sua lunghezza, percorre un tracciato completamente nuovo rispetto alla linea esistente**, andando ad **impattare una porzione di territorio** su cui andrebbero **a gravare vincoli e servitù perpetue di elettrodotto ora assenti**, con un effetto paesaggistico, ambientale, economico e sulla salute delle persone estremamente elevato e negativo.

In particolare, questa enorme criticità ricade **interamente all'interno del Comune di Reggio Emilia**.

A questo si aggiunge, sempre nel Comune di RE, la **tratta RE1**, prevista per collegare la CP Mancasale con la direttrice Villa Cadè. La tratta ha una lunghezza totale di 6.1 km ed è articolata nel seguente modo:

RE1 – aereo + cavo interrato				
Tralicci	**Comune**	**Lunghezza**	**% del totale**	**Tracciato**
da PG2 a 30 (DT)	Reggio Emilia	**1.7 km**	**28%**	**Completamente nuovo**
da 1 a 4 (ST)	Reggio Emilia	**1.6 km**	**26%**	**Completamente nuovo**
Cavo interrato	Reggio Emilia	2.8 km	**46%**	**Completamente nuovo**

Anche questa tratta è **completamente nuova**, attraversa il territorio da Nord-Est a Sud-Ovest e, per una lunghezza pari ad **3.3 km**, è **in linea aerea**, di cui 1,7 km condivisi con la tratta CS2, in doppia terna.

Controdeduzione C: Agricoltura 4.0

Osservazione 6

C Agricoltura 4.0

La precisione del servizio del GPS

La linea aerea 132kV in progetto intrinsecamente produce un campo elettrico e magnetico durante il suo normale funzionamento. Tali valori non influenzano la precisione dei rilevatori GPS posizionati all'interno degli apparati installati nei mezzi agricoli per l'agricoltura 4.0.
Pertanto le opportunità che tali tecnologie, basate sulla telemetria satellitare, mettono a disposizione non si ritiene siano bloccate e/o ostacolate nello sviluppo a causa dell'inserimento dell'infrastruttura in adiacenza dei territori agricoli interessati.
A tal proposito sono stati fatti una serie di studi scientifici che hanno dimostrato che non vi è influenza sostanziale sul funzionamento dei sistemi di rilevamento GPS nelle vicinanze di elettrodotti ad alta tensione. Si allega alla presente, per maggiori approfondimenti, lo studio "Investigating the impact of High Voltage Power Lines on GPS Signal" del Prof. Mostafa Rabah – National Research Institute of Astronomy and Geophysics – Helwan Egypt 06/2011.

Il lavoro citato nella Controdeduzione di Terna per sostanziare la tesi della non interferenza è pubblicato su una **rivista (*ZFV - Zeitschrift fur Geodasie, Geoinformation und Landmanagement*) non riconosciuta dalle banche dati internazionali di riferimento della comunità scientifica (Scopus e Web of Science)**:

ZFV - Zeitschrift fur Geodasie, Geoinformation und Landmanagement

Formerly known as: Zeitschrift fur Vermessungswesen

Scopus coverage years: from 2002 to 2018

(coverage discontinued in Scopus)

Publisher: Verlag Dr. Bernd Wiissner

ISSN: 1618-8950

Subject area: Earth and Planetary Sciences: General Earth and Planetary Sciences

Source type: Journal

Si ritiene pertanto **scarsamente attendibilile il risultato della ricerca scientifica presentato in tale pubblicazione**.

Al contrario si sottlinea come l'effetto dei campi elettromagnetici prodotti dalle linee di potenza sia un tema ancora aperto ed in corso di studio. Si riportano alcuni lavori, tratti da riviste internazionali indicizzate nelle banche dati di riferimento della comunitità scientifica. Tali articoli sono allegati in appendice.

1) J. M. Silva, Senior Member, IEEE, and B. Whitney, Member, IEEE "Evaluation of the Potential for Power Line Carrier (PLC) to Interfere With Use of the Nationwide Differential GPS Network", IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 17, NO. 2, APRIL 2002

   "***Power line carrier fields can have sufficient energy under or close to power lines to affect use of the DGPS signals.***"

2) J. M. Silva, Senior Member, IEEE, and R. G. Olsen, Fellow, IEEE "Use of Global Positioning System (GPS) Receivers Under Power-Line Conductors", IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 17, NO. 4, OCTOBER 2002

"Even if there were significant attenuation due to scattering for one satellite signal, it is unclear if this would cause a problem. This is because a GPS receiver relies on a dispersed constellation of satellites (at least four and often more). ***However, loss of lock on just one satellite could potentially affect accuracy due to an increase in dilution of position error caused by poor satellite constellation geometry****."*

"*Further work might include an* ***analysis of degraded performance due to steel lattice towers and signal scattering from bundled conductors in corona****."*

3) J.M. Silva, Senior Member, IEEE, "Evaluation of the Potential for Power Line Noise to Degrade Real Time Differential GPS Messages Broadcast at 283.5–325 kHz", IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 17, NO. 2, APRIL 2002

*"****The potential to degrade performance of DGPS receivers due to broadband corona and gap discharge noise was found for certain situations close to electric power facilities.****"*

4) V.L. Chartier, Discussion of "Evaluation of the Potential for Power-Line Noise to Degrade Real-Time Differential GPS Messages Broadcast at 283.5–325 kHz", IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 18, NO. 1, JANUARY 2003

"The ***manufacturers of digital global positioning systems (DGPS) readily admit that power-line noise can cause interference****. Therefore, they know that the use of DGPS is limited unless greater immunity is built into these instruments through hardware and/or software."*

5) W. Aziz W. A. and Low, T.Y. "Interference Effects on the Global Positioning Satellite Signals", Sensors, 2003 281-287.

*"****Electrical interference can result from electrical storms, power lines,*** *2-way radios, nearby elecmc motors, microwave towers, cellular phones, …"*

6) L.j. Fan, X.C. Pan, Z.X. Huang and X.D. Zu, "The mechanism and experimental study on the interference of high voltage lines to navigation system", Latin American Applied Research 48:175-179 (2018)

"*Through the GPS signal obtained by UAV while flying below and above the high voltage lines respectively, it finds that* ***the loss of GPS navigation date happens when the UAV flies below the lines and not when it flies over the limes****. Through the measurement and comparison of the electromagnetic wave spectrum while the electromagnetic wave traveled through the corona plasma, the shielding and interference effect of corona plasma on electromagnetic wave is observed.* ***This proves that the signal loss of UAV navigation system is because air is ionized under high voltage environment into corona plasma, which has strong shielding effect on the GPS signal sent by satellites****."*

7) A. Rettore de Araujo Zanella, E. da Silva, L.C.P. Albini, “Security challenges to smart agriculture: Current state, key issues, and future directions”, Array 8 (2020) 100048

In smart farming, the devices (sensors and actuators) and communication systems are exposed to *climatic fluctuations (sun, rain, snow), natural events (lightning, hail), engines (used in agriculture),* ***power line transmissions*** *(common in some rural regions), wandering animals, people and agricultural machinery.* ***These elements make smart farming vulnerable to problems that have not been addressed in other contexts so far.***

Controdeduzione D: Deprezzamento e servitù

Osservazione 7

D Deprezzamento dei terreni e Servitù

Le condizioni relative alla servitù di elettrodotto non attengono la presente procedura di VIA in corso.
Le istanze attinenti alla valutazione dei pregiudizi subiti dalle proprietà interessate in conseguenza della realizzazione dell'opera potranno essere esaminate nelle sedi previste dalla legge per la determinazione degli indennizzi relativi all'imposizione delle servitù e alla realizzazione delle opere.
Per le osservazioni nelle quali si lamenta che il vincolo preordinato all'imposizione in via coattiva della servitù di elettrodotto e la dichiarazione di pubblica utilità paiono portatori di potenziali danni, si rammenta che la norma di riferimento DPR 327/2001 ha valutato che in casi simili sia preminente l'interesse della collettività alla realizzazione di un'opera di interesse nazionale, considerando il danno subito dal privato compensato dall'indennizzo dovuto.

Le opere di sviluppo della rete di trasmissione nazionale, come quella oggetto delle presenti controdeduzioni, sono opere di pubblica utilità, l'apposizione del vincolo di servitù di elettrodotto ha lo scopo di garantire la sicurezza dell'opera stessa. Nelle aree asservite è consentita qualsiasi attività purché questa non metta a rischio il regolare esercizio e la manutenzione dell'elettrodotto. Sono quindi consentite le attività agricole comprese quelle relative a vigneti e frutteti e quelle a seminativi irrigui.
Sono già esistenti elettrodotti su aree agricole nello stesso territorio, dove la coltivazione avviene senza particolari limitazioni.

Generalmente la manutenzione ordinaria non arreca danni alle colture in essere. Solo in casi di manutenzione straordinaria, nel caso si dovesse creare la necessità di intervenire sulla struttura dei sostegni, qualora si dovessero creare eventuali danni alle colture questi verrebbero in ogni caso risarciti. I danni subiti dalla parte concedente per la realizzazione dell'elettrodotto sono valutati e liquidati a lavori ultimati, secondo la stima corrente. Sono valutati e liquidati, a lavori ultimati, i danni causati in occasione di riparazioni di carattere straordinario ed eccezionale o di modifiche all'elettrodotto.

Le attività agricole risultano consentite al di sotto delle linee aeree, il progetto di Terna non costituisce quindi pregiudizio alla continuazione delle attività agricole e non provoca una frammentazione dei poderi. Inoltre, la superficie sottratta dalla presenza dei sostegni è di pochi metri quadri ed è stata nella quasi totalità dei casi scelta in modo che ricadesse al di fuori di vigneti e frutteti.

Per dare piena credibilità a queste affermazioni, sarebbe necessario **documentarle con fonti oggettive ed inoppugnabili**, quali ad esempio il **testo della servitù perenne di elettrodotto** che il proprietario dell'immobile attraversato dalla linea o su cui insisterebbe un traliccio si troverebbe a firmare e **l'articolo di legge o disciplinare o regolamento regionale** che stabilisce la possibilità di ottenere autorizzazione all'impianto di NUOVI vigneti o frutteti nella fascia di rispetto della servitù di elettrodotto.

Controdeduzione E: CEM

Osservazione 8

In riferimento all'osservazione nella quale si esprime preoccupazione **per le aree di coltivazione dei vigneti e frutteti,** si specifica che, in base a quanto indicato nel D.P.C.M. 8 luglio 2003 artt. 3 e 4, i campi coltivati non sono assimilabili a luoghi adibiti a permanenza sistematica, poiché la presenza non è continuativa durante tutto l'arco dell'anno.
Ciò anche in riferimento al documento ISPRA (*Decreti 29 maggio 2008 "Approvazione delle procedure di misura e valutazione dell'induzione magnetica" e "Approvazione della metodologia di calcolo per la determinazione delle fasce di rispetto per gli elettrodotti" - Disposizioni integrative/interpretative)* dove, nella nota n. 1 a pag. 4, par 2.1 si legge: *<<Per "luogo adibito a permanenze non inferiori a quattro ore giornaliere" si intende un luogo "stabilmente attrezzato" (destinato tale negli strumenti urbanistici) per una permanenza ricorrente non inferiore a 4 ore giornaliere, mentre gli "ambienti abitativi" sono rilevabili da titolo edilizio (ciò esclude a mero titolo di esempio, salvo specifico titolo edilizio-urbanistico contrario, locali destinati a magazzino, sottoscala, stenditoio, lastrici solari non calpestabili, locali caldaia o volumi tecnici, cantine, box auto e altri ambienti comunque non soggetti a permanenza ricorrente non inferiore a 4 ore giornaliere).>>*

Al di la delle disposizioni di legge, si sottolinea come **le attività lavorative nei vigneti e frutteti vedono una presenza continuativa di durata pari ad 8 ore** nel caso di potatura, raccolta ed in particolare in caso di operazioni colturali svolte manualmente: queste attività, quando svolte nell'adiacenza del tracciato di elettrodotto aereo, comportano una esposizione rilevante per gli operatori.

In particolare, la linea **CS2 ed RE1** all'interno del Comune di RE **sorvolano vigneti e frutteti per una lunghezza di 2.2 km**, come documentato nelle osservazioni inviate.

Controdeduzione F: Mitigazioni degli impatti di cantiere

Osservazione 9

F Mitigazioni degli impatti di cantiere

Nello studio di Impatto ambientale vengono valutati gli impatti previsti anche in fase di cantiere.
I sostegni vengono messi prevalentemente ai margini dei campi, l'area di cantiere ha una dimensione limitata all'area circostante al sostegno da realizzare e ha una durata limitata nel tempo a circa un mese per ciascun sostegno. Per raggiungere l'area di cantiere si utilizzeranno le aree interpoderali in modo da arrecare meno danno possibili alle coltivazioni.
Gli approfondimenti sugli accorgimenti legati alla mitigazione dei possibili impatti del cantiere sulla componente suolo sono riportane nel paragrafo 3 dello Studio di Impatto Ambientale – Seconda parte (RU0000006B1937518).

Gli impatti di cantiere sono comunque elevati ed inevitabili, in relazione al **passaggio di mezzi** pesanti su suolo agricolo, **indipendentemente dalle condizioni climatiche ed ambientali**, con conseguente compattamento del suolo e perdita di fertilità per elevato periodo di tempo.

Controdeduzione G: Scelta del tracciato dell'elettrodotto aereo

Osservazione 10

> Nell'ambito dello SIA è stata comunque analizzata una alternativa al tracciato di progetto nel **paragrafo 2.3 Analisi delle alternative dello Studio di Impatto Ambientale** (cod. elaborato RU0000006B1937518). Questa alternativa confrontata con quella di progetto, analizzando il complesso degli impatti sulle componenti ambientali, risulta peggiorativa.

Non è chiaro **perché l'alternativa (linea gialla)** esaminata nell'elaborato RU0000006B1937518 e qui sotto riportata (Figura 2.4 a pagina 22), **sia stata valutata peggiorativa:** andrebbe a percorrere un tracciato ben al di fuori di centri abitati e per larga parte in adiacenza di un canale, evitando tutte le problematiche messe in evidenza nelle osservazioni.

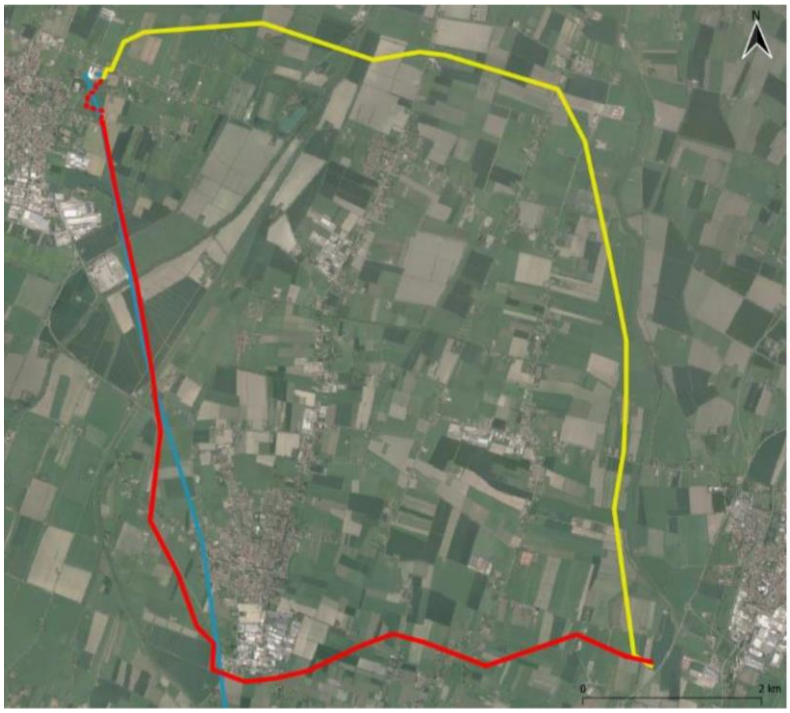
Dall'immagine sottostante, si nota infatti come **il tracciato in rosso (progetto proposto)**, per buona parte della sua estensione, si sviluppa fuori dal corridoio dell'attuale elettrodotto (linea azzurra), interferendo tra l'altro con centri abitati ed un territorio che non vede infrastrutture di questo genere, caratterizzato da agricoltura specializzata (vedere osservazioni già presentate, MATTM-2021-0142292).

Pertanto la motivazione a pagina 25:

> azzurro nella seguente figura); l'alternativa B percorre invece una porzione di territorio completamente diversa su cui andrebbero a gravare impatti ora assenti. Si sottolinea inoltre che l'alternativa B risulta posta a brevi distanze da sei aree definite come "Territori coperti da foreste e boschi (comma 1, lett.g)" mentre l'alternativa A è in prossimità di una sola di tali aree (cerchiate in rosso nella seguente figura).

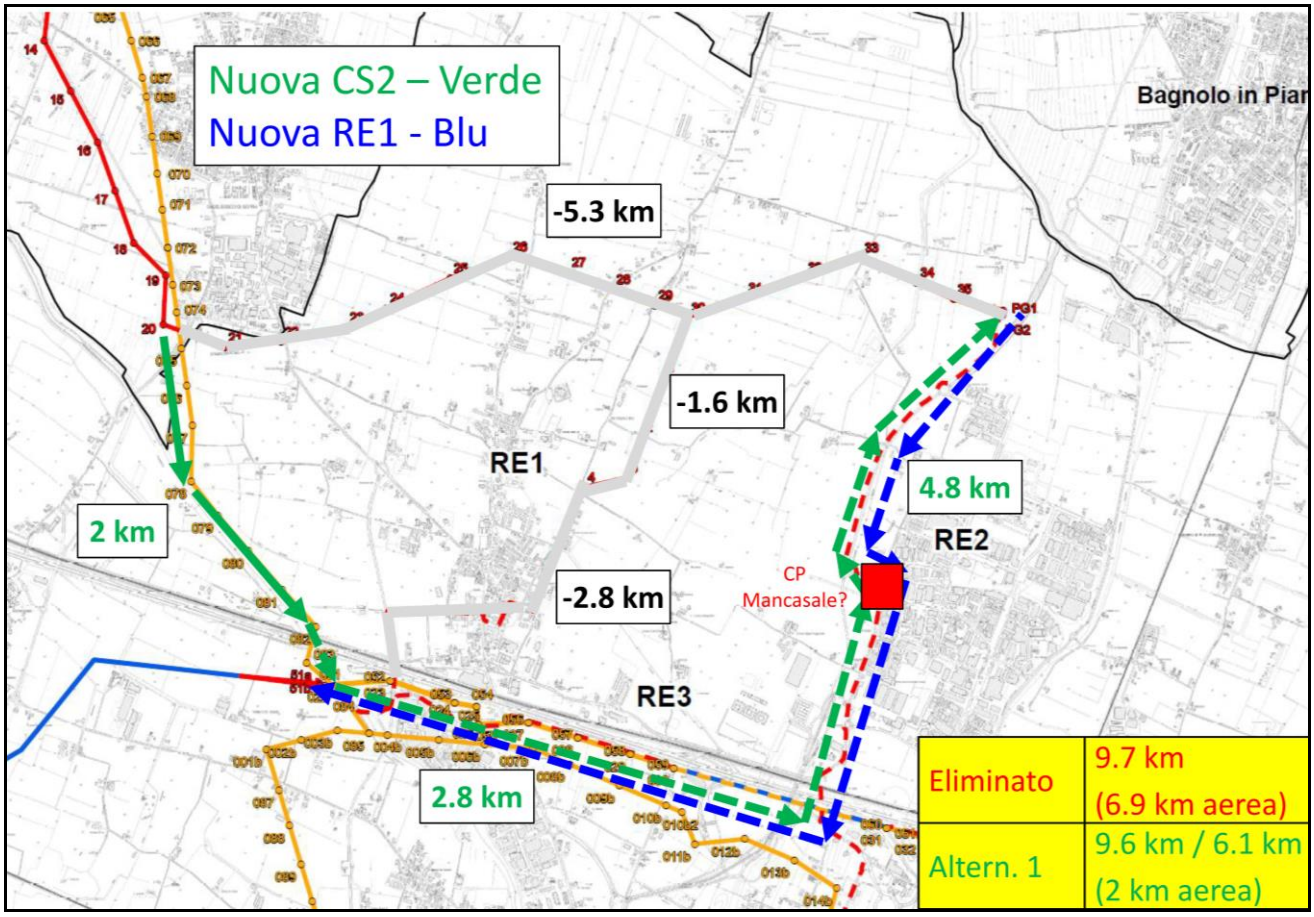
e' scarsamente giustificabile.

Inoltre, non è chiarito nello SIA **quali siano le sei aree definite come "Territori comperti da foreste e boschi"** con cui la soluzione B andrebbe ad interferire.



Si sottolinea, infine, che **la soluzione A (linea rossa) sarebbe pienamente giustificata nel caso in cui si sfruttasse per l'intera lunghezza il corridoio dell'elettrodotto esistente,** fino a raggiungere l'asse autostradale, per poi costeggiarlo in cavo interrato ed infine risalire alla CP Mancasale (Tracciato verde in figura sottostante)

Ciò **eliminerebbe ogni attraversamento in linea aerea ed in cavo interrato (CS2 ed RE1) nella frazione di Villa Sesso**, nonché renderebbe il percorso molto più rettilineo e razionale (tracciato grigio in figura sottostante). La presenza di più linee in cavo interrato che corrono parallelamente è un problema tecnico sicuramente superabile, considerando la presenza di una zona di rispetto in fregio all'asse autostradale, ed altrettanto per quanto riguarda la tangenziale lungo cui si colloca la linea RE2.



Controdeduzione H: Richiesta di alternative in cavo interrato nell'area di Villa Sesso

Osservazione 11

H Richiesta di alternative in cavo interrato nell'area di Villa Sesso

La scelta della differenziazione tecnologica è stata affrontata e ponderata scegliendo di allontanare gli elettrodotti attualmente in esercizio dalle aree più densamente urbanizzate: la contestuale presenza di elettrodotti in cavo interrato o in soluzione aerea, opportunamente distribuiti sul territorio, assicurano la migliore risposta del sistema elettrico di trasmissione nel suo complesso, in tutte le condizioni di rete, favorendo una strategia di sviluppo perseguibile ed efficace, a garanzia della continuità di alimentazione di tutti i carichi (utenti) collegati alla rete.
La connessione alla cabina primaria di Mancasale è stata prevista con tre elettrodotti che devono garantire la sicurezza e la continuità dell'alimentazione. Per tale motivo gli elettrodotti non sono stati previsti né tutti in aereo né tutti in cavo interrato, privilegiando l'adozione di differenti tracciati e differenti tecnologie, così da unire pregi e difetti delle stesse rafforzando e garantendo la resilienza di collegamento alla nuova cabina primaria.
Nella progettazione dei nuovi collegamenti è stata dunque privilegiata la tecnologia del cavo interrato nelle aree urbanizzate, assicurando l'equilibrio a garanzia dell'utilizzo delle due tecnologie.
Si sottolinea, infatti, che l'interramento dei cavi implica le seguenti problematiche:

- minore affidabilità nel tempo rispetto alle linee aeree;
- tempi più lunghi per la riparazione in caso di guasto;
- necessità di un'adeguata viabilità in fase di cantiere;
- potenziali limitazione per lo sviluppo dei sottoservizi necessari per la vivibilità del territorio;
- potenziali limitazioni in caso di guasto per la viabilità del territorio.

Per quanto riguarda la salvaguardia del paesaggio e della natura, occorre sottolineare che il bilancio complessivo della razionalizzazione è molto positivo come indicato al precedente punto **B Aspetti paesaggistici**
Qualora si ritenesse utile ai fini del miglioramento dell'impatto paesaggistico si propone di valutare la possibilità di utilizzare la tecnologia aerea con pali monostelo (tubolari).

Minore affidabilità nel tempo rispetto alle linee aeree:

- perché non vengono forniti **dati tecnici oggettivi** a supporto di questa tesi?
- secondo lo stato dell'arte attuale, **le linee in media tensione sono quasi sempre realizzate in cavo interrato**
- si sottolinea, inoltre, che **nel tratto iniziale la linea CS2 è già prevista in cavo interrato per circa 1 km**

Tempi più lunghi per la riparazione in caso di guasto:

- esistono **dati tecnici oggettivi** a supporto di questa tesi?

Perché non considerare in questo bilancio anche:

- i costi e tempi di manutenzione associati alle linee aere?
- La probabilità di guasto di una linea aerea vs in cavo interrato?

Si riporta infine quanto già espresso nella osservazione MATTM-2021-0142015 dell'ing. Tiziano Toschi in merito alla **tecnologia del cavo interrato XLPE ed alle realizzazioni già effettuate da Terna**, peraltro in territori di montagna.

Considerato che la tecnologia del cavo interrato in XLPE è matura, disponibile con costi decrescenti per la maggiore diffusione, negli ultimi progetti di razionalizzazione della rete di trasporto presentati da Terna sono previsti numerosi tratti in cavo, alcuni dei quali realizzati e altri in fase di realizzazione.

- progetto di interramento dell'elettrodotto a 220 kV, della lunghezza di 24 km, "Passo Resia – Val Venosta"
- elettrodotto a 380 kV Dolo-Camin, realizzato in cavo interrato. Originariamente previsto come elettrodotto aereo a 380kV in terna semplice, per una lunghezza complessiva di circa 15 km, a seguito dell'opposizione delle amministrazioni locali, e, appunto, in considerazione del «sistema di valori ambientali e culturali dell'Area del Brenta», Terna ha accettato di procedere al suo completo interramento.
- linea 220 kV "Polpet – Scorzè" con tecnologia con cavo interrato a 220 kV dalla Nuova stazione di Polpet sino a prima dell'attraversamento del fiume Piave";
- realizzazione della linea a 132 kV Somprade – Zuel completamente in cavo interrato" e, "per migliorare ulteriormente detto progetto, minimizzando la realizzazione di tratte di elettrodotto in aereo, [Terna] presenterà al Ministero dello Sviluppo Economico una variante nella quale la lunghezza dei nuovi raccordi in aereo saranno minimizzati
- Il progetto della Stazione Elettrica di Volpago e la razionalizzazione della rete esistente, che prevede 26 Km di nuovi collegamenti in cavo interrato e la demoli zione di 51 km di linee aeree.
- Il progetto di riassetto della rete elettrica nell'Alto bellunese, che prevede la realizzazione di un collegamento elettrico a 150 kV tra Cortina ed Auronzo di Cadore per una lunghezza di 24 Km interamente in cavo interrato, quale risultato di un lungo percorso di dialogo e collaborazione con la Regione del Veneto, con le amministrazioni comunali interessate e il territorio. Progetto realizzato in soli 13 mesi.

Non sono solo Veneto e Alto Adige gli ambiti territoriali nei quali Terna procede all'interramento di elettrodotti esistenti o di nuova progettazione. sono previsti interramenti di elettrodotti di varia portata in gran parte delle Regioni italiane, dalla Sicilia al Piemonte, dalla Calabria al Friuli-Venezia Giulia, dal Lazio alla Liguria, dall'Abruzzo alla Lombardia.

Alla luce di quanto esposto si osserva:

Osservazione 2

In ragione **dell'art. 22 comma 3, lettera d), del Codice dell'ambiente**, il quale impone al proponente di un'opera di descrivere le alternative ragionevoli prese in considerazione al fine di vagliare l'esistenza della possibilità di adottare soluzioni progettuali che minimizzino la portata delle esternalità negative, **si ritiene carente** il progetto esposto in termini di **alternative ragionevoli** che come dimostrato esistono e sono perseguibili.

Controdeduzione: Integrazione e chiarimenti richiesti dalla Regione ER

Osservazione 12

Risposta alla richiesta n. 1 Aspetti progettuali

1. Si rimanda all'approfondimento di cui al punto **A Concertazione e Avviso al pubblico** e al punto **G Scelta del tracciato dell'elettrodotto aereo**, in cui si ricorda che il percorso del tracciato in aereo è stato condiviso con i Comuni interessati ed è stato sviluppato proprio seguendo il principio di sfruttare al massimo i corridoi esistenti.
2. Dovendo collegare la Stazione elettrica di Castelnovo di Sotto alla Cabina Primaria di Mancasale, l'elettrodotto CS2 in una prima tratta segue il precorso nord-sud già interessato dalla linea esistente di futura demolizione, ma necessariamente deve poi deviare verso est per connettersi alla CP di Mancasale.
3. Si rimanda all'approfondimento di cui al punto **H Richiesta di alternative in cavo interrato nell'area di Villa Sesso**.
4. Nello SIA sono state analizzate le alternative nel paragrafo 2.3 Analisi delle alternative dello Studio di Impatto Ambientale (cod. elaborato RU0000006B1937518). L'alternativa all'elettrodotto aereo nei tratti CS2 RE1 è stata confrontata con quella di progetto, analizzando il complesso degli impatti sulle componenti ambientali, risulta peggiorativa. Per quanto riguarda le differenze tra cavo interrato ed elettrodotto aereo si rimanda all'approfondimento di cui al punto **H Richiesta di alternative in cavo interrato nell'area di Villa Sesso**.
5. Il tracciato proposto risulta non in linea con i principi che hanno guidato la progettazione dell'opera indicati al **punto A Concertazione e Avviso al pubblico** e ai punti **G Scelta del tracciato dell'elettrodotto aereo e H Richiesta di alternative in cavo interrato nell'area di Villa Sesso.**

   Il percorso si ritiene inoltre problematico per la vicinanza al canale di bonifica, che implica una verifica puntuale della possibile deroga alle fasce di rispetto e delle potenziali limitazioni nell'esercizio e manutenzione del cavo interrato.

   Inoltre, in riferimento alla richiesta di posizionare le due linee in cavo interrato nell'area di Villa Sesso in affiancamento, si specifica che nella realizzazione di collegamenti in cavo interrato di due elettrodotti, i tracciati devono preferenzialmente essere posizionati lungo percorsi separati in modo che la manutenzione di uno non comporti la necessità di messa fuori servizio anche dell'altro. Per tale motivo i percorsi dei cavi interrati seguono generalmente tracciati nettamente separati oppure devono essere tenuti a debita distanza tra loro, tale accorgimento tecnico non sembrerebbe rispettabile nella proposta di tracciato interrato pervenuta nelle osservazioni.

1. I **corridoi esistenti vengono sfruttati solo in piccola parte**, in quanto il tracciato proposto per più di metà lunghezza va ad impattare su territorio vergine relativamente a queste infrastrutture, nonché caratterizzato dalla presenza di numerose abitazioni ed agricoltura specializzata (vedere Osservazione 5 e 10).

4. **Non è assolutamente chiaro quale alternativa è stata confrontata con quella di progetto:** l'alternativa individuata nella SIA, oppure quelle proposte nelle osservazioni?

   Non è fornita alcuna valutazione oggettiva dei costi di realizzazione e manutenzione: si ritiene assolutamente necessario un confronto delle alternative anche da questo punto di vista, adottando protocolli riconosciuti in ambito internazionale che permettano una corretta quantificazione della totalità dei costi costituiti da:

   • costi interni/industriali a carico del soggetto realizzatore dell'opera;

   • costi esterni che ricadono solo sulla comunità (patrimoniale, paesaggistico, ambientale, immobiliare, agronomico, ecc.).;

Una corretta valutazione del costo totale permetterà di individuare e ottimizzare il tracciato o la tecnologia più adeguata per realizzare l'opera prendendo in considerazione il vantaggio per il realizzatore e la minimizzazione del danno alla comunità secondo il principio di una equa ripartizione degli oneri.

5. **I principi che hanno guidato la progettazione dell'opera non considerano in misura adeguata l'impatto alto e negativo che la linea CS2 ed RE1 all'interno del Comune di RE avrebbero,** in termini di lacerazione ambientale e danno all'economia del territorio.

   Il tracciato che segue il canale di bonifica ha ricevuto parere positivo di fattibilità da parte del Consorzio di Bonifica dell'Emilia Centrale, come depositato sulla pagina MiTE del progetto in data 30/03/2022 (MiTE-2022-0040601): ciò significa che non esistono impedimenti tecnici legati alle fasce di rispetto, ne limitazioni nell'esercizio e manutenzione del cavo interrato, tutto ciò anche in relazione al fatto che il canale è in corso di tombamento.

   Il canale stesso, avendo due lati permette una naturale separazione dei cavi.

   In aggiunta a questo, **non sono state analizzate le altre due alternative proposte nelle osservazioni del Comitato** (MATTM-2021-0142292), altrettanto migliorative rispetto alla soluzione dell'attuale progetto. Le si riporta qui sotto.

<u>Alternativa 2</u>

È quella già discussa in Osservazione 10.

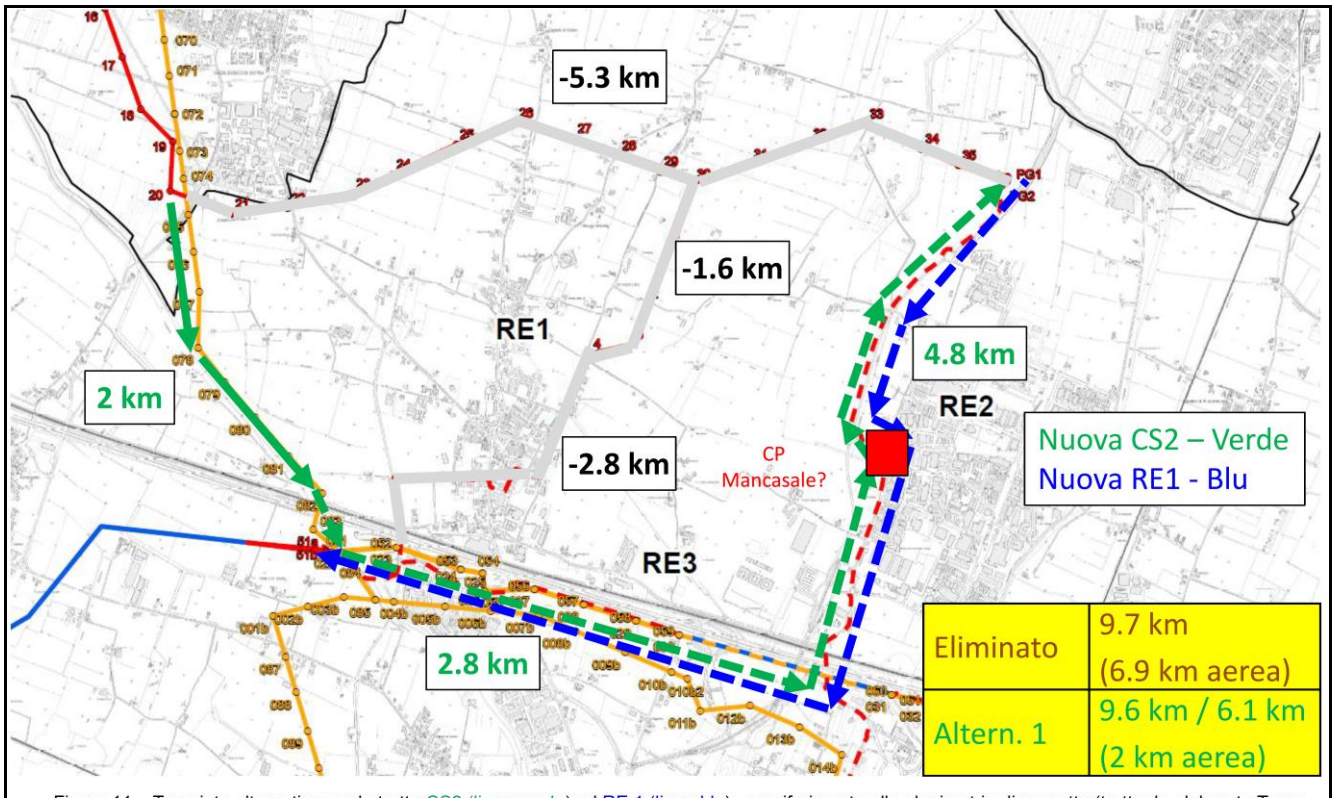
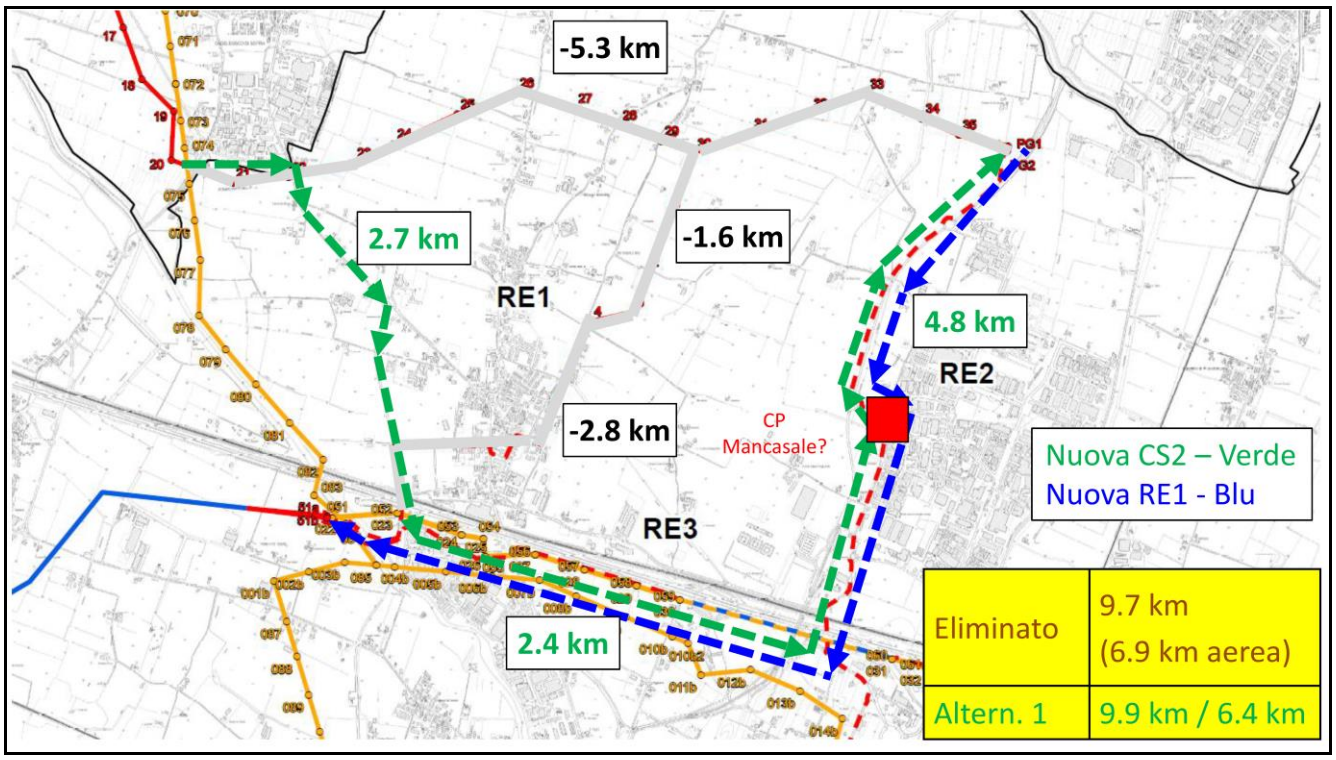


Figura 11 – Tracciato alternativo per le tratte CS2 (linea verde) ed RE 1 (linea blu), con riferimento alla planimetria di progetto (tratta da elaborato Terna DU0000006B1937737)

Alternativa 3

E' simile alla 2 ma segue il corso della statale SS3 e della tangenziale (Via Bice Bertani Davoli), in cavo interrato, per raggiungere l'asse autostradale.



Il/La Sottoscritto/a dichiara di essere consapevole che, ai sensi dell'art. 24, comma 7 e dell'art.19 comma 13, del D.Lgs. 152/2006 e s.m.i., le presenti osservazioni e gli eventuali allegati tecnici saranno pubblicati sul Portale delle valutazioni ambientali VAS-VIA del Ministero dell'Ambiente e della Tutela del Territorio e del Mare (www.va.minambiente.it).

Tutti i campi del presente modulo devono essere debitamente compilati. In assenza di completa compilazione del modulo l'Amministrazione si riserva la facoltà di verificare se i dati forniti risultano sufficienti al fine di dare seguito alle successive azioni di competenza.

ELENCO ALLEGATI

Allegato 1 - Dati personali del soggetto che presenta l'osservazione

Allegato 2 - Copia del documento di riconoscimento in corso

Allegato 3 – Articoli scientifici

Luogo e data

Reggio Emilia, 06/08/2022

I dichiaranti

Prof. Ing. Davide Castagnetti

(Firma)

Geom. Andrea Giglioli

(Firma)

P.A. Livio Castagnetti

(Firma)

P.I. Roberto Castagnetti

(Firma)

P.A. Lorenzo Melioli

(Firma)

Prof. Ing. Andrea Boni

(Firma)

Evaluation of the Potential for Power Line Carrier (PLC) to Interfere With Use of the Nationwide Differential GPS Network

J. Michael Silva, *Senior Member, IEEE,* and Bruce Whitney, *Member, IEEE*

***Abstract*—Power line carrier (PLC) is an important technique used extensively on electric power lines for communication and telemetry. PLC uses signals in the 40–490 kHz range that couple to and propagate over power line conductors. Applications of PLC include protective relaying, telemetering, voice communications, supervisory control, etc. The new Nationwide Differential Global Positioning System (NDGPS) network uses the 283.5–325 kHz band to broadcast GPS correction messages throughout the world, and some PLC transmitters may operate in this band. Limited work has been done to either measure or model the electromagnetic fields associated with PLC operation and some of these studies demonstrate the potential for PLC fields close to power lines to degrade navigation signal receiver performance. This paper presents PLC field strength measurements, describes NDGPS signal structure, and recommends frequency separation as the best approach to mitigation for potential PLC interference to NDGPS receivers operated near to power lines.**

***Index Terms*—Communications systems, global positioning system (GPS), interference, power transmission lines.**

I. Introduction

THE electric utility industry and others make extensive use of power line carrier (PLC) for a variety of applications. The PLC transmitters are operated in a frequency range of approximately 40–490 kHz. The frequencies used for PLC include the 283.5–325 kHz broadcast band used by the new Nationwide Differential Global Positioning System (NDGPS) network. This frequency overlap has raised questions about the potential for PLC fields to affect use of the NDGPS close to power lines. Previously, some limited work was done to evaluate the potential for PLC to interfere with navigational radiobeacon systems in various low frequency bands of about 90–505 kHz. This work (often done above the ground for aircraft) demonstrated the potential for PLC fields close to power lines to degrade the performance of navigation signal receivers. Limited published data indicate that the PLC field strength close to power lines, even when the PLC is operated at only 1 W, can significantly exceed typical NDGPS broadcast signal strengths. This paper provides measurement data of PLC fields at ground level, a description of the NDGPS network, signal structure, and broadcast signal strengths, and mitigation recommendations.

Manuscript received May 2, 2001. This work was supported by EPRI under Contract WO 7319-01 and by Enertech Consultants. The EPRI project manager was F. Young.

J. M. Silva is with the Enertech Consultants, Campbell, CA 95008 USA.
B. Whitney is with the Detroit Edison Company, Detroit, MI 48226 USA.

Publisher Item Identifier S 0885-8977(02)02721-8.

TABLE I
PLC Transmitter Summary (March 1999)

PLC Frequency Range	Number of Transmitters in U.S.
10-50 kHz	1,169
50-100 kHz	5,986
100-150 kHz	8,788
150-200 kHz	8,897
200-250 kHz	2,615
250-300 kHz	989
300-350 kHz	219
350-400 kHz	95
400-450 kHz	38
450-490 kHz	20
	28,816

II. Power Line Carrier

PLC is an important technique used extensively on electric power lines for quick and reliable communication and telemetry. PLC uses low-medium frequency signals that are coupled to and propagate over power line conductors. PLC equipment has been used on electric power systems since the early 1920s [1]. Applications of PLC include protective relaying, telemetering, voice communications, supervisory control, etc., [1]–[3]. A PLC system consists of terminal assemblies (transmitters, receivers, and relays), coupling and tuning equipment, and the power line conductors between terminals. Sometimes the same PLC system is used for multiple purposes. Coupling of the radio frequency (RF) carrier is done with coupling capacitors attached to the power line conductors. Removal or blocking of the carrier signal is achieved with line traps i.e., a parallel resonant circuit tuned to offer high impedance at the carrier frequency but not to 50/60-Hz power currents [1], [3]. Many PLC systems use some form of discrete frequency shifting to transmit digital information in the 40–490 Hz frequency range [4]. Table I provides a summary of installed PLC transmitters in the United States. [5].

Power lines can have multiple PLC frequencies used for different functions or redundancy [1], [3]. PLC used in protective relaying can be operated in different modes with variable power levels depending on losses for a particular line. Based on the application, the PLC may be either ON (at low power) or OFF (no power) and switch to ON or jump to a higher power level to convey information. Sometimes a shift in frequency is also

TABLE II
PLC FIELD STRENGTH NEAR GROUND LEVEL IN DECIBEL MICROVOLTS PER METER

Appx. Distance from Conductors	230 kV-152 Hz [7]	161 kV- 200/284 kHz [10]	500 kV- 284/400 kHz [10]	230 kV- 283 kHz [6]	Computer Model [13]
10 m	85-92 dB	80-90 dB	72-75 dB	95 dB (est.)	110 dB
100 m	55-71 dB	40-62 dB	48-56 dB	60 dB (est.)	40-70 dB
1000 m	18-25 dB	26-35 dB	34-37 dB	37-41 dB	30 dB

employed. PLC generally operates at low power levels (typically 1–10 W), but some applications can reach 100 watts. Typical bandwidths, i.e., the range of frequencies over which the receiver responds and usually defined within 3 dB of the peak response, for these systems are generally less than 3.4 kHz. In some older systems bandwidths of up to 10 kHz have been used.

The PLC transmitter is often coupled to only one phase conductor of a transmission line using coupling capacitor potential devices (CCPD). In some applications the PLC signal is coupled across two phase conductors. The PLC signal propagates along the line conductors in three general modes. In the first mode, PLC current is flowing away from the transmitter on two outside conductors and returning in the center conductor. This mode has the least attenuation with distance. In the second mode, PLC current is flowing away on one outer conductor and returning on the other. This mode has greater attenuation than the previous mode and is more frequency dependent. In the last mode, PLC current is equal on all three phases with an earth return. This mode has the highest attenuation. Beyond a few kilometers from the transmitter, the PLC signal is present on all the phase conductors regardless of the form of coupling [6].

PLC signals can also be induced in the conductors of transmission and distribution lines that parallel the PLC-equipped line for long distances [7]. These other lines radiate the induced PLC signals and may cause PLC RF fields on a multiple line corridor to be higher than those from the source line alone. Distribution lines can cause up to a 20 dB field strength variation up to 200 m away. PLC signal strength away from the transmitter (longitudinally along the line) typically decreases about 0.10–0.42 dB/km depending on frequency, line geometry, conductor size, etc. [7]. Longitudinal attenuation of the PLC signal is one reason measurements may not compare for different locations along the length of a power line. Lateral measurements of PLC fields on opposite sides of a power line can differ by as much as 20–25 dB at distances of 100 m or less from the line, but tend to converge beyond about 200 m. Ambient electromagnetic noise can mask PLC fields beyond about 1–1.5 km from a power line.

The significance of PLC with respect to this paper is that the DGPS band of 283.5–325 kHz is within the range of frequencies used for PLC applications. Some work has been done to either measure or model the electromagnetic fields associated with PLC operation on an electric power line [6]–[13]. In general, this work was done to evaluate the potential for PLC to interfere with navigational radiobeacon systems in various low frequency bands of about 90–505 kHz [9], [10]. Some of these studies demonstrate the potential for PLC fields close to power lines to degrade the performance of navigation signal receivers. Limited published data indicate that the PLC field strength close to power lines, even when the PLC is operated at only one watt, can significantly exceed typical DGPS broadcast signal strengths. Table II summarizes some of the data on PLC field strength measured or modeled near power lines. Variation is due to lack of symmetry from each line side, antenna orientation, line design, etc. Most measurements were for 1-W PLC transmitters.

Fig. 1. Vehicle with spectrum analyzer, active loop antenna, and printer.

III. PLC MEASUREMENTS

This evaluation of PLC involved some practical field measurements. This included measurement of typical DGPS signal strengths and some measurements of PLC generated field strength. The field measurements used a radio frequency measurement system (broadband antenna and spectrum analyzer) and a digital GPS/DGPS unit equipped to receive and process differential corrections. In addition to this instrumentation, a portable printer and laptop computer were used to facilitate data collection. The instrumentation vehicle is shown in Fig. 1 and the primary equipment used for this study of PLC is summarized in Table III.

Measurements of PLC field strength were made near transmission lines using the HP Spectrum Analyzer and 0.6 m diameter active loop antenna system. Measurements of PLC signals vs. distance from power lines were made near ground level with this test equipment. All measurements revealed

TABLE III
SUMMARY OF INSTRUMENTATION USED IN GPS/DGPS FIELD MEASUREMENTS

Equipment	Description
Broadband Antenna	EMCO Model 6502 Active Loop Antenna. Range: 10 kHz-30 MHz. Dia. 60 cm
RF Spectrum Analyzer	Hewlett Packard Model HP8568B Spectrum Analyzer. Range: 100 Hz-1.5 GHz
Freq. Selective Voltmeter	Rycom Model 6020 Frequency Selective Levelmeter. Range: 0-1,500 kHz
Digital GPS Receiver	Trimble Navigation. 12 channel/carrier phase filtered. DGPS w/ H-field antenna

Fig. 2. Multiple line easement with double circuit 120-kV, 345-kV, and 345-kV transmission lines.

Fig. 3. PLC signal strength versus frequency displayed on the spectrum analyzer.

significant PLC signals that attenuate rapidly with increasing distance from the power line. PLC measurements are reported for a 120 kV/345 kV/345 kV multiple transmission line easement with clear access for lateral measurements (see Fig. 2). Real-time PLC signals can be displayed on the Spectrum Analyzer as presented in Fig. 3. The PLC measurements were taken at discrete locations starting about 150 m away from the 120-kV line and extending onto the easement and directly under each of the transmission lines. Representative measurement results are provided for three different PLC frequencies found at this location in Table IV (there were more than three PLC frequencies observed at this site). The measured PLC field strength for 1-W transmitters in the region near power lines can be comparable to or larger than the amplitude of DGPS signals. These measurement data compare well with previous data and modeling of Table II. PLC measurement results can vary due to distance along line from the PLC transmitters, line design, ground conductivity, and induced signals from parallel circuits.

IV. NATIONWIDE DIFFERENTIAL GPS NETWORK

The Global Positioning System (GPS) is a satellite-based radionavagation system developed by the U.S. Department of Defense to provide worldwide coverage and year-round navigation and positioning data. Many civilian and commercial GPS applications require greater dynamic positioning accuracy than provided by standard code-based GPS positioning. For example, many transportation applications such as harbor navigation, positive train control, and precision agriculture need accuracies of 5–10 m or better [14]. Fortunately, methods have been developed to augment GPS and increase accuracy for the operations of a single, autonomous GPS receiver. One method to improve accuracy involves using ground stations that compare a GPS-derived position with its known location to compute a correction that can be used to remove errors (i.e., satellite clock and orbit errors, atmospheric delay errors). This correction information can be broadcast to nearby users for real time position adjustments or stored for post-processing the raw data at some convenient time. This approach, known as Differential GPS positioning (DGPS), can significantly increase accuracy. Users with mobile GPS receivers that are equipped to receive and process these corrections in real time can enjoy significant accuracy improvements; e.g., accuracy to within $\pm$5–10 m, and in some cases in the 1–3 m range or better [14].

The NDGPS differential corrections are broadcast at frequent intervals in the band allocated for maritime radionavigation beacons: 283.5–325 kHz (in many other countries this band is described as 285–325 kHz). The DGPS messages are modulated onto the low-medium frequency carrier wave by minimum shift keying (MSK). At present, the selected transmission rates for the NDGPS signals are 100 and 200 bits per second. These data transmission rates are low, but are more immune to message loss caused by Gaussian noise and therefore achieve higher message throughput under impulse noise conditions[15]. The 99% power containment bandwidth of the MSK modulated DGPS signal is equal to 1.17 times the transmission rate, and the half power

TABLE IV
PLC FIELD STRENGTH (IN DECIBEL MICROVOLTS PER METER) MEASUREMENTS ACROSS 120/345/345 KV EASEMENT

Location	PLC @ 203.605 kHz	PLC @ 205.095 kHz	PLC @ 207.100 kHz
~150 m South- 120 kV	61.2 dB	57.0 dB	53.1 dB
30 m South- 120 kV	71.4 dB	70.2 dB	64.9 dB
120 kV CL	72.0 dB	77.3 dB	76.1 dB
120/345 kV	81.8 dB	89.8 dB	83.9 dB
So. 345 kV CL	95.8 dB	91.6 dB	91.0 dB
Midway- 345/345 kV	90.6 dB	78.4 dB	88.5 dB
No. 345 kV CL	86.1 dB	83.1 dB	76.3 dB
30 m North- 345 kV	64.4 dB	62.3 dB	60.7 dB
100 m North	55.8 dB	52.5 dB	57.0 dB

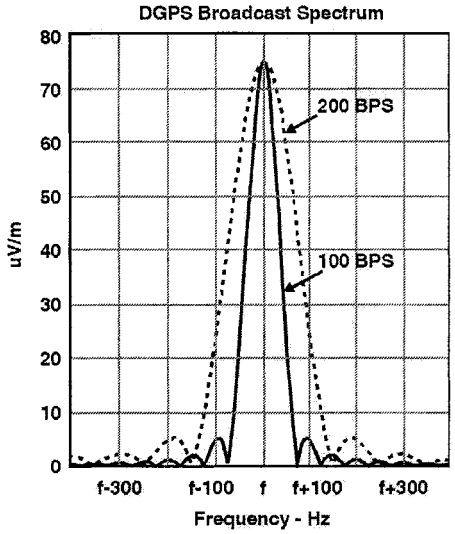


Fig. 4. DGPS broadcast spectrum at center frequency (transmission rates: 100 and 200 b/s).

bandwidth is given by 0.59 times the transmission rate [16]. This means that the DGPS broadcast information is contained in a relatively small bandwidth as shown in the conceptual sketch of Fig. 4 (i.e., 117 or 234 Hz wide). The very narrow DGPS signal bandwidth can be an important consideration when concern arises about possible interference due to other radio signals at a nearby frequency.

During normal operations the USCG specified minimum field strength for coverage of the DGPS broadcast signal is usually 75 μV/m, or 37.5 dB referenced to 1 mV/m [16]. Terrain and atmospheric conditions can significantly affect the "advertised" coverage range [17]. In any event, the specified minimum coverages are provided primarily as a guideline for radiobeacon selection purposes. Adequate reception and decoding of the DGPS correction message is possible at signal field strengths below the specified "minimum" signal strength, depending on factors such as the level and nature of local noise sources, multipath, receiver design, receiver antenna type and placement. At present, 34 countries have installed DGPS radiobeacon networks and more are considering adoption of this standard. Electric utilities should become familiar with NDGPS plans, operational characteristics, and assets within their service territory.

TABLE V
PLC TRANSMITTERS INSTALLED AS OF MARCH 1999

Frequency Range	Number (percent)
10-490 kHz (All PLC transmitters)	28,816 (100%)
283-325 kHz (DGPS Band)	425 (1.5%)

V. DISCUSSION

In the region close to power lines the PLC signal (when present, even at 1 W) is strong enough to potentially affect DGPS receiver performance if it is close to the DGPS signal frequency. There has previously been reported interference to aeronautical and maritime nondirectional beacons due to radiated emissions of HVDC converter stations or connected ac or dc transmission lines [18]. The potential for interference will depend on the emissions within the beacon band and the SNR. At present only a small fraction of PLC transmitters operate at frequencies within the DGPS band. Table V summarizes the portion of PLC transmitters in the DGPS band [5].

The simple solution to potential DGPS problems with PLC is frequency separation. The DGPS signal is contained within a very narrow bandwidth about the center frequency: 99% power containment is within a 117–234 Hz bandwidth. The PLC bandwidth is variable but could be on the order of 300–2 200 Hz [3]. Only a relatively small fraction of existing PLC transmitters are in the DGPS band and their frequencies could be changed to provide adequate frequency separation between PLC and DGPS signals. For new PLC transmitters, engineers should determine DGPS beacon coverage in their area and avoid these regional DGPS frequencies in the anticipated location for the new PLC system. The authors did not learn of any reported instances of PLC–DGPS interference. However, most DGPS stations were not inland and this situation is rapidly changing with the advent of the NDGPS network.

VI. Conclusions

The future of GPS is bright and applications will grow as GPS accuracy is improved with augmentations such as the Nationwide Differential GPS initiative. This paper reports on an evaluation of the possibility for PLC fields to affect DGPS receivers near power lines. The following conclusions were reached.

- The use of GPS will increase and applications will diversify as more accuracy is offered at no cost by the new Nationwide DGPS network. This network is comprised of low-medium frequency radio stations that continuously broadcast differential corrections in a standard format. The NDGPS network is presently expanding across the United States. It is already in wide use and should be fully operational in all 50 states within about two years. These NDGPS stations operate at frequencies presently utilized by some PLC transmitters.
- The NDGPS goals include strengthened national security, integration of GPS into nonmilitary applications, encouraging private sector investment in GPS, and promotion of safety and efficiency in transportation and other activities. It is anticipated that many people will rely on the enhanced positioning accuracy provided by the NDGPS network. Electric utilities should become familiar with NDGPS plans, operational characteristics, and assets within (or near) their service teritory.
- Power line carrier fields can have sufficient energy under or close to power lines to affect use of the DGPS signals. However, for some implementations, PLC signals are not always on and few PLC transmitters operate in the DGPS band. Only about 1.5% of PLC transmitters are in the 283.5–325 kHz DGPS band. Since DGPS signals have small bandwidth the simple solution is frequency separation.

Acknowledgment

The authors relied on advice and assistance from engineers in the GPS community and from electric utilities. Most noteworthy was the guidance on GPS by A. Lange (Trimble Navigation) and the assistance on PLC by R. Mueller (Detroit Edison Company). This work greatly benefited from their contributions. Additional assistance in the form of telephone discussions, e-mail, and technical papers was provided by R. Olsen (Washington State University) and J. Radice (U.S. Coast Guard).

References

[1] "Power-line carrier application," in *Electrical Transmission and Distribution Reference Book*, 4th ed: Westinghouse Electric Corp., 1964, ch. 12.
[2] *Applied Protective Relaying*: Westinghouse Electric Corp., Relay-Instrum. Div., 1976.
[3] *IEEE Guide for Power-Line Carrier Applications*, IEEE Stand. 643-1980, 1981.
[4] *Transmission Line Reference Book—345 kV and Above*, 2nd ed., Elect. Power Res. Inst.
[5] *Summary of Power Line Transmitters as of March*: United Telecom Council, 1999.
[6] D. E. Jones, "Power line carrier radiation from high voltage lines," *Ontario Hydro Res. Quart.*, 3rd Quart. 1965.
[7] R. C. Madge and G. K. Hatanaka, "Power line carrier emissions from transmission lines," *IEEE Trans. Power Delivery*, vol. 7, Oct. 1992.
[8] R. Moore, "Powerline carrier (PLC) interference tests," U.S. Dept. Trans., DOT/FAA/CT-TN84/19, 1984.
[9] "Assessment of Potential Interference From Power-Line-Carrier Systems to Loran-C Aeronautical Receivers," U.S. Dept. Commerce, NTIA TM-88-133, 1988.
[10] "Power Line Carrier Radiation and the Low-Frequency Aeronautical Radio Compass," FAA, Rep. FAA-RD-80-31, 1980.
[11] M. D'Amore and M. S. Sarto, "Electromagnetic field radiated from broadband signal transmission on power line carrier channels," *IEEE Trans. Power Delivery*, vol. 12, Apr. 1997.
[12] M. S. Sarto, "Electromagnetic interference from carrier channels on finite-length power lines above a lossy ground in a wide frequency range," *IEEE Trans. Power Delivery*, vol. 13, Apr. 1998.
[13] F. D. Pullen, "The calculated electromagnetic fields surrounding carrier-bearing power line conductors," *IEEE Trans. Power App. Syst.*, vol. PAS-94, Mar./Apr. 1975.
[14] P. Enge and P. Misra, "Scanning the special issue/technology on global positioning system," *Proc. IEEE*, vol. 87, Jan. 1999.
[15] B. W. Parkinson and J. J. Spilker, Eds., *Global Positioning System: Theory and Applications*: Progress in Astronautics and Aeronautics, 1996, vol. 163, 164.
[16] *Broadcast Standard for the USCG DGPS Navigation Service*, COMDTINST M16577.1, Apr. 1993.
[17] P. K. Enge *et al.*, "Coverage of DGPS/radiobeacons," *Navigat.*, vol. 39, no. 4, 1992–1993.
[18] N. A. Patterson, "Carrier frequency interference from HVDC systems," *IEEE Trans. Power App. Syst.*, vol. PAS-104, pp. 3255–3261, Nov. 1985.

J. Michael Silva (M'76–SM'84) received the B.S. degree from the University of Alabama, Tuscaloosa, in 1971 and the M.S. degree from Auburn University, Auburn, AL, in 1976, both in engineering.

He has been actively involved in electric power research for most of his 30-year professional career. He has worked for the Southern Company, the Electric Power Research Institute, GAI, and founded Enertech Consultants, Campbell, CA, in 1982, where he serves as President. He has directed pioneering efforts in instrumentation for personal exposure measurements and software for electromagnetic field modeling. He is presently leading a team that has developed a personal GPS logger for scientific and medical research applications using state-of-the-art GPS technology.

Mr. Silva is a member of the Institute of Navigation and is a registered professional engineer in seven states and the Territory of Guam.

Bruce Whitney (M'73) received the B.S.E.E. degree with honors from the University of Michigan (UM), Ann Arbor.

He a listed inventor at the United States Patent Office and has authored papers on radio noise, EMF, and power-line carrier systems. He has 30 years of engineering experience with The Detroit Edison Company, Detroit, MI, including design, project management, and software development, as well as implementation of innovative problem solutions. He has experience with data collection over extra high-voltage insulation barriers, UHF telemetering, fiber-optics, digital and analog electronic systems, power supply design, lightning detection and tracking technology, RF energy exposure safety, EHV transmission line design, and environmental effects. He is currently responsible for RF safety and EMF issue management.

Mr. Whitney is a Registered Professional Engineer in the State of Michigan. He was elected President of Etta Kappa Nu, B.E. Chapter, while attending UM.

Use of Global Positioning System (GPS) Receivers Under Power-Line Conductors

J. Michael Silva, *Senior Member, IEEE,* and Robert G. Olsen, *Fellow, IEEE*

***Abstract*—The use of global positioning system (GPS) technology continues to grow and recent accuracy augmentations will generate ever more innovative applications. The issue of GPS use under or near electric power lines has been raised since some GPS documents have vague warnings about such use. First, GPS and the satellite microwave signals used to determine position, velocity, and time are described. Then, the potential effects of electromagnetic interference and/or signal scattering from overhead conductors are evaluated analytically and with some practical measurements under transmission lines. This work demonstrates that it is unlikely that power line conductors will interfere with use of the GPS satellite signals.**

***Index Terms*—Conductors, electromagnetic interference, electromagnetic reflection, global positioning system, GPS, interference, noise, power transmission lines, scattering.**

I. Introduction

THE global positioning system (GPS) enables unique capabilities, and the benefits are substantial. This satellite-based radionavigation system has many new civilian applications for the position, velocity, and time information it can provide. As GPS use expands, it becomes more important to evaluate any potential sources of interference. One issue that is sometimes raised is the potential for degraded performance of GPS receivers when they are used near electric power facilities. Of specific interest is the use of the GPS satellite-based microwave signals under or near power line conductors. At the surface of the earth the satellite microwave signals are weak and any reduction of signal intensity due to scattering by conductors or noise due to corona and/or gap discharges could degrade receiver performance or cause loss of signal lock.

II. GPS

The GPS is a satellite-based radionavigation system developed by the U.S. Department of Defense to provide worldwide coverage and year-round navigation and positioning data primarily for the U.S. military [1]. Since the only equipment required by the user is a receiver/processor, the cost to the user of the system can be relatively small. For this reason, the personal and commercial market for GPS-based equipment, applications, and services has grown exponentially and has moved ahead of military use. GPS use is expanding internationally and there is discussion of a competing GPS constellation of satellites and infrastructure funded and operated by the European Community [2].

At present, 28 GPS satellites are in place [3], consisting of six orbital planes of four satellites each and four active on-orbit spares. On any given day, the number of operating satellites is variable and could drop to 24 before additional replacements are added. Each satellite, at an altitude of about 20 000 km, is moving at about 4 km/s and completes an orbit of the earth in approximately 12 h.

GPS satellites are equipped with highly accurate atomic clocks that keep time to within 3 ns. This precision in time measurement is at the heart of the GPS system function. Precise determination of the transit time for a radio wave to travel from a GPS satellite with a known position in space to the user's receiver on earth is the basis for all GPS applications. The distance, or range is obtained by multiplying the apparent transit time by the speed of light. The phrase "apparent transit time" is used because this time and the ranges derived from it will include propagation errors and other potential errors, including dilution of position errors related to satellite constelation geometry at time of use. In general, position and velocity information are determined by trilateration, which uses the ranges or distances to compute a three-dimensional (3-D) position (a process called ranging). For 3-D navigation, the GPS receiver requires range information from at least four satellites; the fourth satellite is needed to adjust for receiver clock errors. The position is given as latitude, longitude, and elevation, usually with respect to a reference ellipsoid model of the earth, such as the World Geodetic System [4], [5].

III. GPS Satellite Signal Description

Each GPS satellite broadcasts very weak, uniquely identifiable signals, using spread spectrum technology [1], [2]. At present, each satellite transmits its carrier signals on two different radio frequencies in the L-Band of the frequency spectrum: Link 1 (L1) at 1575.42 MHz and Link 2 (L2) at 1227.60 MHz; each has a bandwidth of 20.46 MHz [1]. The carrier waves are modulated with pseudo-random noise (PRN) codes for each satellite [6]. GPS transmits two types of PRN codes with significantly different structures: Coarse Acquisition (C/A code) and Precise or Protected (P-code). The C/A code is a sequence of 1,023 bi-phase modulations of the carrier signal. Each period for a possible binary phase reversal is called a chip. Since the C/A code is repeated 1000 times/s, the chip rate is 1.023 MHz. The P-code has a very large sequence of chips so that a complete sequence takes 267 days to complete [1]. The chip rate of the P-code is 10.23 MHz, significantly higher than that of the C/A code.

Manuscript received January 29, 2001. This paper was supported by EPRI under Contract WO 7319–01 and by Enertech Consultants.

J. M. Silva is with Enertech Consultants, Campbell, CA 95008 USA (e-mail: msilva@enertech.net).

R. G. Olsen is with Washington State University, Pullman, WA 99164 USA.

Digital Object Identifier 10.1109/TPWRD.2002.803791

The GPS carrier signal power density at the surface of the earth is far below the received noise density as shown in Fig. 1. In fact, the signal normally cannot be detected by a spectrum analyzer. The noise spectral density at a matched receiver (N_{receiver}) is computed as the product of Boltzman's constant (k) and the "equivalent noise temperature" (T_{eq}) in °K. This temperature is apportioned to various sources of noise such as circuit and transmission line thermal noise. Thus

$$T_{eq} = \sum_i T_i \tag{1}$$

where T_i is the equivalent temperature of the ith noise source. Above 300 MHz, most noise is generated by sources internal to the receiving system [7]. However, some noise is generated external to the receiver and is accounted for by a portion of the equivalent noise temperature called the "antenna noise temperature." Of special interest in this paper is the contribution to the antenna noise temperature from power line corona electromagnetic interference (EMI).

The C/A and P-codes are to used to determine the transit time of the radio wave as it travels from the satellite to the receiver. The user's GPS receiver does this by internally generating an exact replica of the satellite's PRN code at the same instant the satellite generates and transmits its code sequence and uses this code to extract the signal from background noise in a process called correlation. In this process, the receiver essentially offsets the internal replica code in time with respect to the (propagation delayed) code received from the satellite and integrates over the signal's duration until the signal is extracted from the noise. The amount of offset needed to do this is used to determine the time lag or transit time of the signal.

Another signal, the navigation message, is also modulated onto the L-band carriers. This message contains data on satellite ephemerides (orbital location), system time, on-board clock behavior, status messages, and C/A to P-code handover information. In the future, GPS modernization may include more satellites, additional frequencies, a more robust civilian code, a new military code, and stronger signals- depending on government funding and policy decisions.

IV. GPS Receiver Performance Criteria

The GPS signal must have sufficient strength to be detected by a correlation receiver. One measure used to quantify this strength is the carrier to noise ratio (C/N_0) defined as the signal power of the unmodulated GPS carrier available to a matched receiver divided by the noise power spectral density in the same receiver [8]. It is useful to relate C/N_0 to the measure of signal quality for the receiver used in this study. For this receiver, an "amplitude measurement unit" (AMU) is used to estimate relative signal strength of the satellite and is related to C/N_0 by [9]

$$\frac{C}{N_0} = 20\log_{10}(AMU) + 27 \text{ dB-Hz} \tag{2}$$

Since an AMU is a measure of signal strength, this relationship holds only if the noise is a constant. This is reasonable if the dominant source of noise is internal to the receiver. If however, external noise is important, AMU cannot be directly related to C/N_0. It has been reported by the manufacturer that minimum acceptable carrier signal strength for the receiver used in this study may range from 2 – 6 AMU [10]. Assuming that the dominant source of noise is internal, this corresponds to carrier to noise ratios per unit bandwidth of from 33 to 43 dB-Hz.

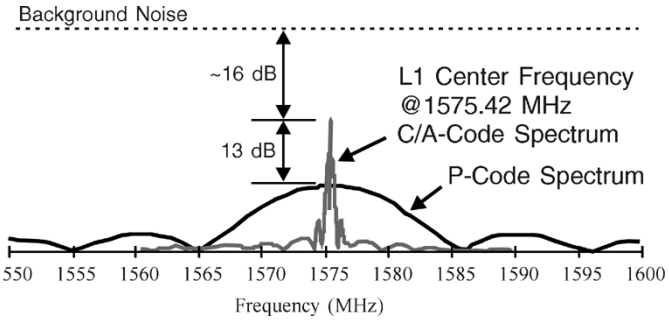


Fig. 1. Conceptual diagram of GPS signal spectrum.

It is possible that a power line can interfere with the performance of a GPS receiver in one of two ways. First, if the receiver noise due to EMI from the power line is comparable to or greater than the equivalent thermal noise, then the performance may be degraded. Second, if the electromagnetic scattering of the signal from overhead conductors is significant, then the received signal may be reduced and receiver performance degraded.

Each of these possibilities will be considered in turn. Following this, the results of experiments to study the performance of a GPS receiver near a power line will be reported.

V. Power Line EMI

This section is to evaluate the possibility that EMI from power transmission lines will interfere with the operation of GPS receivers. Two mechanisms by which this might occur are 1) corona along the length of the transmission line conductors and 2) spark discharges on the transmission line hardware [11], [12].

A. Corona Noise

EMI from power line conductors is important only on transmission lines for which the 50/60-Hz conductor surface electric fields are large enough to cause corona (i.e., local ionization of the air) [11]. The corona caused by these large electric fields at the conductor surface induces impulsive currents on the transmission line. These induced currents, in turn, cause wide band electric and magnetic "noise" fields that fill the entire frequency spectrum from below 100 kHz to approximately 1000 MHz, although they are usually too small to be measured above 10 – 20 MHz [12], [13]. Weather has a large influence on corona noise. In fact, the noise level can be 15–25 dB higher during foul weather. Another factor that affects corona is altitude. The usual rule of thumb is that corona noise increases approximately 1 dB/300 m of altitude above sea level [14].

It is commonly stated that electromagnetic interference from transmission line corona is only a problem when the following three conditions are satisfied.

1) The transmission line voltage is above 230 kV.
2) The frequency of interest is less than 30 MHz.
3) The distance between the transmission line and the receiver is small (i.e., less than a few hundred feet).

Since the second condition is not satisfied for microwave frequency GPS receivers, it could be expected that there will not be a problem. However, the signal strength from a GPS satellite is so small that a more complete investigation is warranted. Here, a noise calculation using a typical 500-kV transmission line will be made to evaluate the possibility for degraded performance. The computer program used for the calculation will be WBNOISE that was developed for the EPRI and described in [15].

The following (worst case) assumptions will be made for this calculation.

1) The receiving antenna will be assumed to be directly under the power line.
2) The polarization of the "noise" field will be assumed to be matched to that of the receiving antenna. Thus, no polarization loss of the noise will occur.
3) Average stable foul weather conditions (i.e., practical worst case) will be assumed.

Since WBNOISE calculates noise only up to 30 MHz, the noise cannot be directly calculated at this frequency. Rather, the calculation will be made at 10 MHz and then scaled to 1575 MHz using a conservative model for the corona noise spectrum [16].

The 500-kV transmission line geometry of [15] was studied, and it was assumed that the receiving antenna was 1 m above the ground. The average stable foul weather (i.e., practical worst case) noise in a 9-kHz bandwidth receiver with a CISPR Quasi-Peak detector in dB relative to 1 μV/m was obtained and is shown in Fig. 4 of [15]. The largest value of "average stable foul weather" noise in a CISPR standard quasipeak receiver at 10 MHz was 40 dB (μV/m). To apply these data to the problem considered here, it is necessary to do the following.

1) Convert from a CISPR receiver to one with an RMS detector and bandwidth appropriate for calculation of the carrier to noise ratio.
2) Convert the noise frequency from 10 to 1575 MHz.
3) Calculate the incident noise power density in a 1-Hz bandwidth at the antenna.
4) Calculate the incident power density at the receiver from the GPS satellite carrier.
5) Calculate C/N_0 to determine if it is acceptable.

For frequencies below 30 MHz, the noise in a receiver with 9-kHz bandwidth and RMS detector can be obtained by subtracting 8 dB from the noise in a CISPR receiver [13].

The noise in a 1-Hz bandwidth (since C/N_0 is reported per unit bandwidth in decibel-Hertz) can be obtained by adding $10\text{Log}_{10}(1/9000) = -39.5$ dB (i.e., the received noise power is proportional to bandwidth) [16]. The noise at a frequency of 1575 MHz can be computed by adding $10\text{Log}_{10}(10/1575) = -22.0$ dB (i.e., using Fig. 4 of [16], it is conservatively assumed that the spectrum drops off as $1/(f)^{1/2}$ in the frequency range from 10 to 2000 MHz). Finally, the effective electric field noise level at 1575 MHz (assuming a receiver with an RMS detector and after correcting to a bandwidth of 1 Hz) is

$$E_{\text{effective}} = -29.5 \text{ dB-Hz } \mu\text{V/m}. \quad (3)$$

This is read as "the effective (i.e., RMS) electric field in decibels with respect to 1 μV/m within a 1-Hz bandwidth (BW)."

Since the power density of a plane wave in free space is $P = E^2/\eta_0$ (where $\eta_0 = 120\pi\ \Omega$ is the impedance of free space), the effective electric field can be converted into an incident noise power density dB-Hz ($\mu\text{W/m}^2$) by subtracting $60 + 10\text{Log}(\eta_0)$ dB to yield

$$N_{\text{incident}} = -115.3 \text{ dB-Hz } \mu\text{W/m}^2. \quad (4)$$

Again, this is read as "the effective (i.e., RMS) incident noise power density at 1575 MHz in decibels with respect to 1 $\mu\text{W/m}^2$ within a 1-Hz bandwidth."

GPS transmitters are located in satellites approximately 20 000 km above the earth's surface. The transmitter output for the civilian signal is about 25 W and the antenna gain is 13 dB_i, yielding an effective radiated power of approximately 500 W. [1]. Since the gain of the receiving antenna is not known and the noise is assumed to be from a source external to the receiver, the carrier-to-noise ratio will be determined from a comparison of incident fields. It will thus be (conservatively) estimated here that the receiving antenna responds identically to the GPS signal and to the noise.

The incident power density at the earth's surface of a carrier signal from a transmitter that feeds a directional antenna is

$$C_{\text{incident}} = [P_t(\text{dBw}) + G_t(\text{dB}_i) - 10\log_{10}(4\pi d^2) + 60] \text{ dB } \mu\text{W/m}^2 \quad (5)$$

where P_t is the transmitter power delivered to the antenna, G_t is the antenna gain relative to an isotropic antenna, and d is the distance between the satellite and the receiver in meters. For this case

$$C_{\text{incident}} = -70.0 \text{ dB } \mu\text{W/m}^2 \text{ or about } 6\,\mu\text{V/m} \quad (6)$$

Thus, the carrier-to-noise ratio $C/N_{0,}$ for the incident field is 45.3 dB-Hz. This is above the minimum specified by the manufacturer of the receiver used in this study (i.e., 43 dB). Given the number of conservative assumptions used in this calculation (e.g., 500–kV transmission line, spectral decay of $1/(f)^{1/2}$, noise polarization matched to the GPS antenna, etc.), it is unlikely that the transmission line corona noise could degrade operation of the GPS receiver. Nevertheless, since the C/N_0 ratio is close to the minimum, it was decided that an experiment was necessary to determine whether there was any interference of a transmission line with the operation of the GPS receiver. This experiment will be reported later.

B. Spark or Gap Discharge Noise

Spark discharges generally occur between parts of hardware on a power line that are physically close but at different voltages [11], [12]. If the voltage becomes high enough, a spark occurs across the gap. Due to the nature of this discharge, the electric and magnetic noise fields from these sparks tend to dominate those from corona at frequencies above 10 – 20 MHz [12] and can be detected at frequencies above 1000 MHz. As with corona, weather has a large influence on gap discharges. However, the effect is opposite. In fact, gap discharges generally occur only during dry weather; wet conditions tend to equalize voltages between different parts of the hardware and hence suppress them.

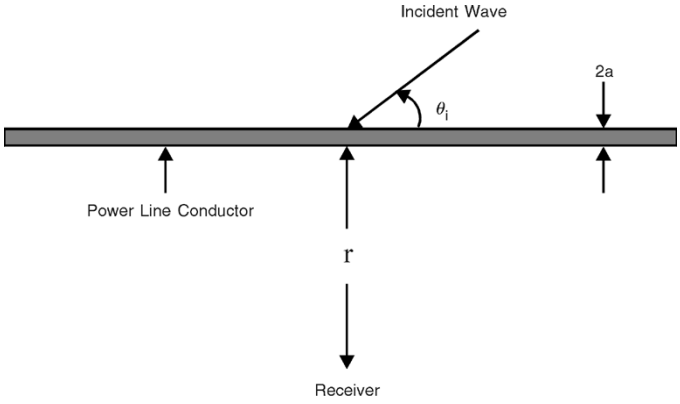


Fig. 2. Conceptual diagram of GPS carrier wave incident on single conductor.

Spark discharge fields are generally not calculated because the discharges tend to be intermittent, models are crude and only limited measured data are available [16]. Rather, if there is a problem, the source of the discharge is located and repaired [17]. GPS receivers are typically operated near ground level at some distance from spark gap sources. As a final comment, it can be said that gap sources often occur on low voltage distribution lines. Thus, they are more likely to be found on the distribution lines than on transmission lines because the former are more numerous [12]. Later, results of GPS measurements near spark discharges will be reported.

VI. GPS Microwave Signal Scattering

A possible concern for use of GPS equipment under or very close to power lines is whether an incident GPS satellite signal can be significantly scattered by a power line with a resulting adverse effect on the received signal. This possibility is considered next.

A number of simplifying assumptions will be made in the calculations presented here. First, it will be assumed that there are no towers either near the receiver or on a direct line between the satellite and receiver. Although towers are expected to be strong scatterers, they are too complex to be included in the simple model considered here. It is more appropriate that they be examined experimentally in a separate study. Given this, towers have been eliminated from the model. Second, the transmission line conductors are assumed to be horizontal, and each phase is assumed to consist of only a single conductor. Third, phase conductors are far enough apart that they can be analyzed separately. Finally, reflection from the earth will be neglected. While this effect can be important, its inclusion would not change the conclusions of this report and the additional mathematics may obscure the argument. Despite these assumptions, the simple model analyzed here leads to reasonable conclusions about whether power line conductors can interfere with GPS signals.

Consider the single conductor shown in Fig. 2. Here, a GPS signal is assumed incident upon a single power line conductor at an angle θ_i, as shown. Since the signal is circularly polarized, it can be decomposed into two plane waves: one polarized parallel to and the other perpendicular to the conductor. It is shown in [18] that for a parallel polarized incident wave, the ratio of scattered to incident field (component along the direction of the conductor) for scattering from a cylindrical conductor model of a power line conductor is

$$\left|\frac{E_z^s}{E_z^i}\right| = \frac{\sqrt{\pi}}{\sqrt{2}\ln\left(0.2885ka\sin(\theta_i)\right)\sqrt{kr\sin(\theta_i)}} \qquad ka \ll 1, \theta_i \neq 0 \quad (7)$$

where $k = (2\pi f)/3.0\times 10^8$, f is the frequency in Hertz, a is the radius of the cylindrical conductor, and r is the distance between the conductor and the receiver in meters. It is also shown in [18] that the perpendicular polarized incident wave is scattered much less than the parallel one. Thus, if scattering of the parallel polarized wave is small enough, it is not necessary to consider the perpendicular polarized component.

For an assumed 1.27-cm conductor radius, $r = 10$ m, $\theta_i = \pi/2$ and $\lambda = 19$ cm (at 1575.42 MHz), (7) yields a ratio of scattered field/incident field of 0.032 or about a 3.2% reduction in the field for normal orientation. Only for grazing angles of incidence (i.e., values of θ_i near zero) does the scattered field increase markedly from this result. In this case, however, the calculation becones much more complex [19]. Given the very small scattered field from a single conductor, it is clear that a three-phase line with single conductors will also not significantly affect the GPS signal. It appears then that power line conductors have little effect on the signal and that a GPS receiver/antenna can be used under power lines without bundled conductors. Based on measurements to be reported later, it is believed that this conclusion can also be applied to transmission lines with bundled conductors. It should be noted that even if there were significant attenuation due to scattering for one satellite signal it is unclear if this would cause a problem for a GPS user. This is because a GPS receiver relies on a dispersed constellation of satellites (at least four and often more). However, loss of lock on just one satellite could cause a poorer (less accurate) position solution due to an increase in dilution of position caused by poor satellite constellation geometry. Bundled conductors in heavy corona may merit further analysis to confirm that receiver performance is not degraded by reducing the number of satellites available to the receiver.

VII. GPS Signal Measurements Under 345-kV Lines

A series of measurements to evaluate GPS signal reception quality under power lines was performed in both fair and foul weather across the easements of two different double circuit, twin-subconductor, 345-kV transmission lines. These measurements were performed with a Trimble GPS receiver and a circularly polarized cross-dipole antenna system. The purpose of the measurements was to evaluate whether the GPS satellite signal incident on metallic conductors can be significantly scattered and adversely affect the signal received and/or whether power line EMI can degrade receiver performance.

At one location (Site #1 in Fig. 3), measurements were performed along a traverse under a double circuit 345 kV transmission line. The satellite constellation geometry that existed during the fair weather measurements at the site is shown in Fig. 4. Measurements along a traverse were also made at another

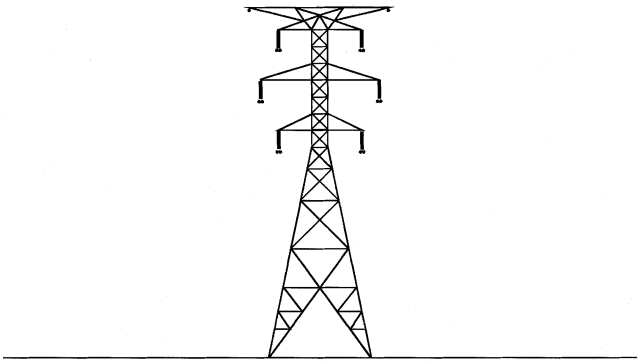


Fig. 3. Sketch of 345-kV transmission line at site # 1.

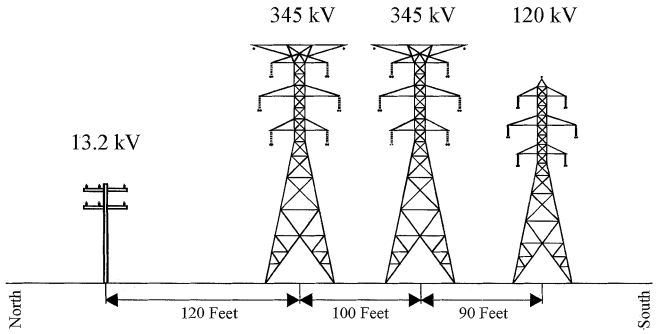


Fig. 5. Sketch of transmission line configurations at site # 2.

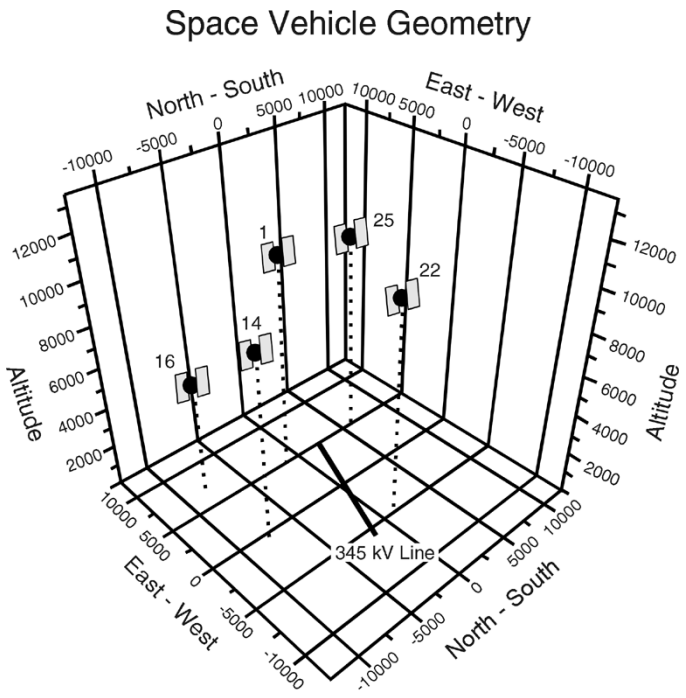


Fig. 4. GPS satellite constellation geometry at site # 1 during measurements.

location (Site #2 in Fig. 5) within an easement that included two double-circuit 345-kV lines and a double-circuit 120-kV line.

For all of these measurements, several satellites were visible to evaluate reception quality but not all are included in the presentation of results. More specifically, data from satellites with an elevation above the horizon of less than about 20° is not given because it is more subject to multipath errors and shielding by nearby objects such as trees. The impact of these factors changes as orientation to the receiver changes when the easement was traversed during measurements. This situation could result in a change in reception quality that is not associated with conductor scattering of the GPS carrier wave.

According to the results of Section V, the only condition under which corona noise might cause a problem is during foul weather since in this case corona noise is 15–25 dB higher than in fair weather. In order, then, to isolate the possible effect of scattering from power line conductors, the first measurements were conducted in fair weather along the traverses described above. The signal amplitude in AMU for GPS carrier L1 was logged for each satellite in view at one-second intervals while driving across the 345-kV easements and directly under the transmission lines. This quantity was output by the GPS receiver in the standard NMEA format and then converted to C/N_0 using (2) and the assumption that the noise is constant and entirely internal to the receiving system [9], [20]. The measured value of C/N_0 was then used to evaluate changes in reception quality as the easement was traversed. The results reveal no practical change in each satellite's C/N_0 even when directly under the 345-kV transmission lines (see Figs. 6 and 7). Thus, it does not apppear that scattering from power line conductors leads to any significant change in signal strength. This result is consistent with the earlier discussion of this subject: the conductors are small compared to a carrier signal wavelength and the receiver antenna is generally located at ground level some tens of wavelengths away.

Note that no satellite signal measurements were made inside a steel lattice tower within the area enclosed by the steel structure members and legs. However, it is anticipated that this could cause a shielding problem because of the large metallic members near a line between the satellite and the user.

The possible effect of corona noise was evaluated by repeating the measurements described above in foul weather conditions. Since the signal amplitude available from the receiver is not a measurement of noise, it cannot be used to evaluate noise level. Instead, noise was indirectly measured by noting the number of satellites on which the receiver was locked as a function of position along the traverse. It was hypothesized that excessive corona noise would cause loss of lock on at least some satellite signals. For Sites #1 and #2, the receiver maintained lock on eight and nine satellites, respectively, over the entire traverse. Thus, no degradation in receiver performance can be attributed to EMI from corona.

VIII. Other Sources of Electrical Interference

There are many nonpower system sources of potential interference that can create noise within the GPS satellite signal bandwidth. Out-of-band emissions by radio, TV, communications, and radar transmitters can cause an electromagnetic interference problem. Other potential EMI sources include gasoline engine ignition systems, TV and computer monitors, electric motors, fluorescent lights, ac–dc converters, alternators, and generators and switching power supplies. The broadband noise of a gap discharge source can extend above 1 GHz and is cited by GPS receiver manufacturers as a potential interference

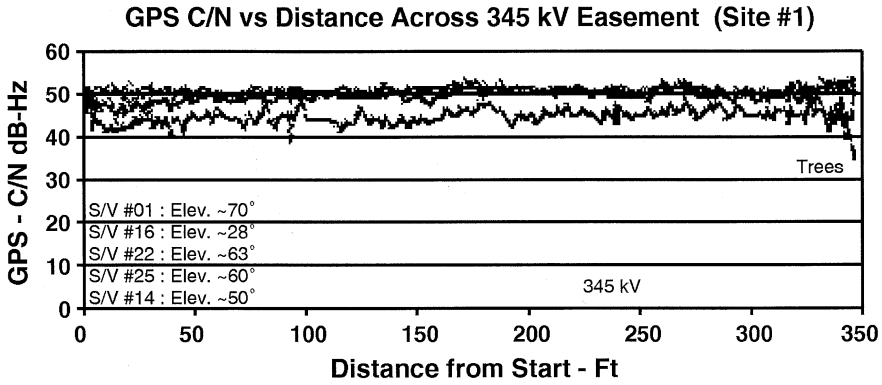


Fig. 6. Plot of GPS satellite C/N ratio versus distance across site #1 345-kV easement.

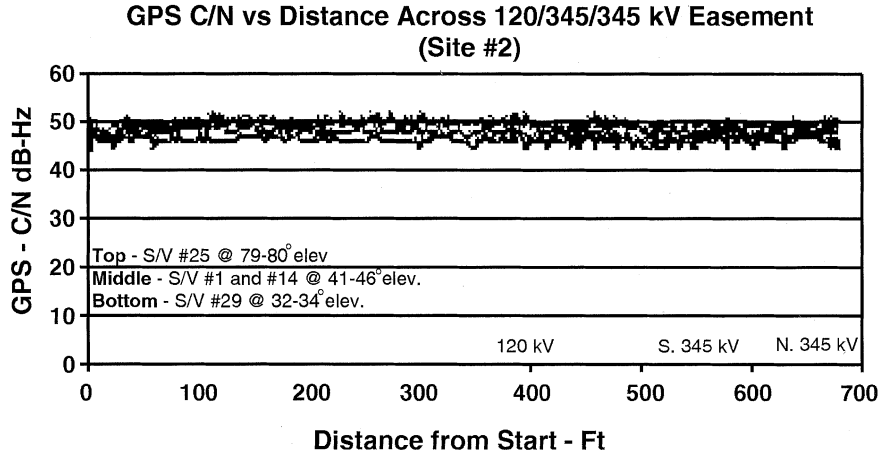


Fig. 7. Plot of GPS satellite C/N rato versus distance across site #2 120 kV/345-kV easement.

source (e.g., proximity to spark plugs on an all-terrain vehicle). During the course of the measurements reported in this paper, the GPS receiver was operated close to a number of gap discharge sources on distribution lines with no effect on receiver performance. The distance to the source is most likely the main factor in the lack of an observed influence on GPS receivers. Of course, the design characteristics of the GPS receiver/antenna system is always important in overall performance.

IX. GPS Satellite Anomalies

There is another type of GPS receiver problem not caused by scattering of incomming signals or noise in the GPS carrier bandwidth. GPS receivers may experience problems when a GPS satellite exhibits operational anomalies, such as low power, PRN code generation error, or outages. These events are rare but do happen. It is important to be aware of these events because the resulting loss of signal lock could erroneously be attributed to any nearby power lines. In one 3-mo period in 1998, a total of 107 anomalies, an average of 1.2 per day, were observed for satellites that could be seen over the continental United States [21]. The satellite anomalies included brief generation and transmission of nonstandard C/A or P-codes, maintenance problems, and short-term disruptions in the navigation message. The average duration of outages was about 6 s, ranging from a few seconds to 93 s. These satellite anomalies can cause positioning errors outside of specified accuracy and loss of lock. The period of time affecting the user includes the outage duration plus the time to reacquire the satellite signal and is receiver dependent. For example, on November 26, 1998, a triple outage sequence ocurred on the L1 signal of satellite PRN# 15. These outages occurred in succession, seperated by variable lengths of time and spread over a period of about 3–4 min (44 s for the first signal outage, 8 s for the second, and 16 s for the third). Receivers of different designs took from several seconds to over 2 min to reacquire the satellite signal after the outages [21]. Research has been done on algorithms for GPS receivers to perform on-board interference detection and monitoring to improve performance [22]. The design and performance of GPS receivers can be variable, but changes in hardware and software continue to improve receiver performance.

X. Conclusions

This paper reports on an evaluation of the possibility for power line conductors to affect GPS receivers used near power lines. The following conclusions were reached.

- A simple model has been used to show that electromagnetic scattering of GPS signals by power line conductors is unlikely to cause significant signal degradation. Carrier-to-noise ratio measurements under transmission lines in foul weather support this conclusion for practical situations. Even if there were significant attenuation due

to scattering for one satellite signal, it is unclear if this would cause a problem. This is because a GPS receiver relies on a dispersed constellation of satellites (at least four and often more). However, loss of lock on just one satellite could potentially affect accuracy due to an increase in dilution of position error caused by poor satellite constellation geometry.

- A theoretical evaluation of transmission line corona noise at the GPS carrier frequency did not indicate that corona noise could affect GPS receiver performance. Measurements made in foul weather confirm this conclusion. Specifically, it was noted that there was no loss of lock of satellite signals as a GPS receiver was moved across a power line easement.
- The GPS receiver was operated close to a number of gap discharge sources on distribution lines with no effect on receiver performance. GPS receivers may experience problems when a GPS satellite exhibits operational anomalies, such as low power, PRN code generation error, or outages. These events are rare but do happen. It is important to be aware of these events because the resulting loss of signal lock could erroneously be attributed to any nearby power lines.
- Further work might include an analysis of degraded performance due to steel lattice towers and signal scattering from bundled conductors in corona.

ACKNOWLEDGMENT

This work greatly benefited from the contributions of EPRI project manager F. Young, on advice and assistance from Dr. A. Lange (Trimble Navigation), and the assistance with field measurements by B. Whitney (Detroit Edison Company).

REFERENCES

[1] J. Spilker and B. W. Parkinson, Eds., *Global Positioning System: Theory and Applications*, 1996, vol. 163 164, Progress in Astronautics and Aeronautics.
[2] P. Enge and P. Misra, "Scanning the special issue/technology on global positioning system," in *Proc. IEEE*, vol. 87, Jan. 1999.
[3] "GPS operational advisory- status list," in *Daily Update of GPS Satellite Status*: NISWS- Navigation Inform. Service Watch Stand. U.S. Coast Guard Navigat. Cent., 2001.
[4] A. Kleusberg and P. J. Teunissen, Eds., *GPS for Geodesy*, 2nd ed. New York: Springer, 1998.
[5] *Geodesy for the Layman*, Fifth ed: National Ocean. Atmos. Admin., U.S. Dept. Commerce, 1985.
[6] E. D. Kaplan, Ed., *Understanding GPS Principles and Applications*. Norwell, MA: Artech House, 1996.
[7] D. G. Fink and D. Christiansen, *Electronics Engineers' Handbook*, 3rd ed. New York: McGraw-Hill, 1989.
[8] S. Haykin, *Communication Systems*. New York: Wiley, 1983.
[9] *TSIP Reference Manual*, Trimble Navigation, Sunnyvale, CA, 1999.
[10] *Trimble GPS Operation Manual*, pt. 38 747-00, Trimble Navigation, AUTHOR: WHERE IS TRIMBLE NAVIGATION?, 1999.
[11] *Transmission Line Reference Book, 345 kV and Above*, Second ed., Electric Power Res. Inst., Palo Alto , CA, 1982.
[12] F. W. Warburton, T. Liao, and N. A. Hoglund, "Power line radiations and interference above 15 MHz," *IEEE Trans. Power App. Syst.*, vol. PAS-88, pp. 1492–1501, Oct. 1969.
[13] V. L. Chartier, R. Sheridan, J. N. DiPlacido, and M. O. Loftness, "Electromagnetic interference measurements at 900 MHz on 230 kV and 500 kV transmission lines," *IEEE Trans. Power Delivery*, vol. PWRD-1, pp. 140–149, Apr. 1986.
[14] R. G. Olsen, S. D. Schennum, and V. L. Chartier, "Comparison of several methods for calculating power line electromagnetic interference levels and calibration with long term data," *IEEE Trans. Power Delivery*, vol. 7, pp. 903–913, Apr. 1992.
[15] S. D. Schennum and R. G. Olsen, "A method for calculating wideband electromagnetic interference from power line corona," *IEEE Trans. Power Delivery*, vol. 10, pp. 1535–1540, July 1995.
[16] W. E. Pakala and V. L. Chartier, "Radio noise measurements on overhead power lines from 2.4 to 800 kV," *IEEE Trans. Power App. Syst.*, vol. PAS-90, pp. 1155–1165, May/June 1971.
[17] M. Loftness, *AC Power Interference Manual*. Tumwater, WA: Percival, 1996, pt. 98 501.
[18] C. A. Balanis, *Advanced Engineering Electromagetics*. New York: Wiley, 1989, pp. 614–625.
[19] R. G. Olsen and D. C. Chang, "Current induced by a plane wave on a thin infinite wire near the earth," *IEEE Trans. Antennas Propagat.*, vol. AP-22, pp. 586–589, July 1974.
[20] *Standard for Interfacing Marine Electronic Devices*, NMEA 0183, Ver. 2.30, Mar. 1, 1998.
[21] J. W. Lavrakas and D. Knezha, "GPS receiver responses to satellite anomalies," in *Proc. National Tech. Meeting*, San Diego, CA, Jan. 25–27, 1999.
[22] B. C. Barker and S. J. Huser, "Protect yourself! Navigation payload anomalies and the importance of adhering to ICD-GPS-200," in *Proc. Int. Tech. Meeting Inst. Navigat.*, Nashville, TN, Sept. 15–18, 1998.

J. Michael Silva (M'76–SM'84) received the B.S. degree in engineering from the University of Alabama, Tuscaloosa, in 1971, and the M.S. degree, also in engineering, from Auburn University, Auburn, AL, in 1976.

He has been actively involved in electric power research for most of his 30-year professional career. He has worked for the Southern Company, the Electric Power Research Institute, GAI, and he founded Enertech Consultants, Campbell, CA, in 1982, where he serves as President. He has directed pioneering efforts in instrumentation for personal exposure measurements and software for electromagnetic field modeling. He recently led a team that has developed a personal GPS logger for scientific and medical research applications using state-of-the-art GPS technology.

Mr. Silva is a member of the Institute of Navigation and is a registered professional engineer in seven states and the Territory of Guam.

Robert G. Olsen (S'66–F'92) received the B.S. degree in electrical engineering from Rutgers University, New Brunswick, NJ, in 1968 and the M.S. and Ph.D. degrees in electrical engineering from the University of Colorado, Boulder in 1970 and 1974, respectively.

He has been a member of the electrical engineering faculty at Washington State University, Pullman, since 1973. He has been a visiting scientist at GTE Laboratories, Waltham, MA; ABB Corporate Research, Västerås, Sweden, and the Electric Power Research Institute, Palo Alto, CA; and has been a Visiting Professor at the Technical University of Denmark. His research interests include high-voltage systems, electromagnetic interference from power lines, the electromagnetic environment of power lines, electromagnetic compatibility, and electromagnetic scattering.

Dr. Olsen presently serves as the chair of the IEEE Power Engineering Society Corona Effects Fields Working Group and is Associate Editor of the IEEE TRANSACTIONS ON ELECTROMAGNETIC COMPATIBILITY.

Evaluation of the Potential for Power Line Noise to Degrade Real Time Differential GPS Messages Broadcast at 283.5–325 kHz

J. Michael Silva, *Senior Member, IEEE*

***Abstract*—The new Nationwide Differential Global Positioning System network uses the 283.5–325 kHz band to broadcast differential GPS (DGPS) correction messages. Concern has been expressed that power line corona and gap discharge noise could degrade the performance of DGPS receivers using this band. Previous work on power lines and the AM broadcast band identified corona and gap discharges as broadband noise sources in the LF/MF bands. The potential to locally degrade performance of DGPS receivers relatively close to some power facilities appears possible for certain situations. The extent of any DGPS interference problem will depend on receiver/antenna design and placement, signal strength, power line design, weather conditions, and characteristics of the noise source. Also affecting DGPS receiver performance can be the presence of any nearby nonpower line RF noise sources such as electronic devices or equipment internal to the user's vehicle.**

***Index Terms*—Corona, electromagnetic interference, global positioning system (GPS), interference, noise, power transmission lines.**

I. Introduction

THE CIVILIAN use of the global positioning system (GPS) is growing at an increasing rate. GPS accuracy is being improved with augmentations such as differential GPS (DGPS). With DGPS, corrections are provided to users to improve accuracy by compensating for some of the errors inherent in autonomous GPS use. The DGPS correction messages can be made available by various methods, but the focus of this paper is the network of LF/MF broadcast stations operated by the United States and other governments. The potential for interference is well known to power engineers due to experience with the AM radio broadcast band. Anecdotal reports by agricultural users of coastal DGPS stations indicate that power line RF noise, under certain conditions, can be a problem for DGPS receivers. Some GPS receiver manuals also mention the potential for noise/interference problems near to electric power lines. However, there is little or no engineering information on the potential for electric power line noise due to corona or gap discharges to affect DGPS use. The importance of this issue is underscored by the implementation of the Nationwide Differential GPS network of DGPS stations planned to cover the entire United States by 2002. This paper will describe GPS, DGPS, and provide measurement data to evaluate the potential for electric power line corona or gap discharge noise to affect DGPS broadcasts in the 283.5–325 kHz band.

Manuscript received January 29, 2001. This work was supported in part by EPRI (Contract WO 7319-01) and by Enertech Consultants.

The author is with Enertech Consultants, Campbell, CA 95008 USA.

Publisher Item Identifier S 0885-8977(02)02734-6.

II. GPS Overview

The Global Positioning System (GPS) is a satellite-based radionavagation system developed by the U.S. Department of Defense to provide worldwide coverage and year-round navigation and positioning data primarily for the U.S. military [1]. Over the past decade or so, GPS has evolved beyond its original use to become a dual-use technology with extensive civilian use in a expanding variety of applications. At present, 28 GPS satellites are in place [2] at an altitude of about 20 200 km above the earth, located within six orbital planes of four satellites with active on-orbit spares. Each satellite travels at about 4 km/s and completes an orbit of the earth in approximately 12 h [3]. GPS satellites are equipped with highly accurate atomic frequency standards that keep time to within 3 ns. This precision in time measurement is at the heart of the GPS system function. In general, position and velocity information is determined by trilateration, which uses the ranges or distances derived by measuring the radio wave travel time of each satellite's special signal to compute a three-dimensional position (a process called ranging). For three-dimensional (3-D) navigation, the GPS receiver requires range information from at least four satellites; the fourth satellite is needed to adjust for receiver clock errors. There are a number of error sources for autonomous receiver operation, including: satellite clock and orbit errors, ionosphere and troposphere delay, multipath, receiver noise, and errors due to satellite constellation geometry. Positioning error is a dynamic concept, changing over time. Methods have been developed to remove or minimize these errors.

III. Differential GPS

Many civilian and commercial GPS applications now require greater accuracy than provided by the civilian standard positioning service (SPS). For example, many transportation applications such as harbor navigation, positive train control, and precision agriculture need accuracies of 5–10 m or better [3]. Fortunately, methods have been developed to augment SPS and increase accuracy for the operations of a single, autonomous GPS receiver [1], [3]–[6]. One method to improve accuracy involves using ground stations that compare a GPS-derived position with a known location to compute a correction that can be used to remove clock, orbit, and atmospheric delay errors. This correction information can then be broadcast to nearby users for real time

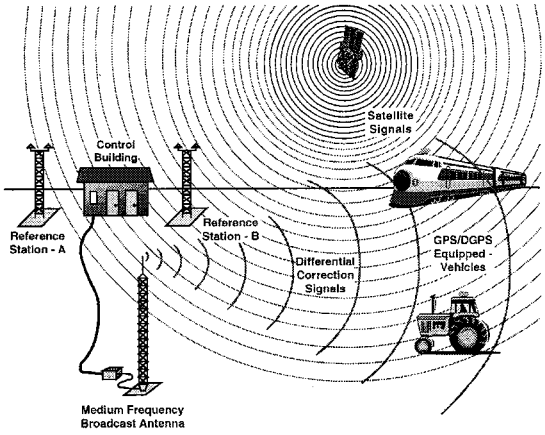


Fig. 1. Conceptual diagram of differential GPS (DGPS) station.

Fig. 2. Proposed NDGPS reference station locations.

position adjustments or stored for post-processing the raw data at some convenient time. This approach, known as Differential GPS (DGPS), can significantly increase accuracy. With DGPS, two GPS receivers are used: a reference unit and a mobile or rover unit. The reference receiver is placed at a stationary location with a position previously determined to a high degree of accuracy by surveying. This reference receiver determines its position using GPS signals and a computer derives the position error and calculates differential corrections that can be applied by the rover to yield a more accurate position. A range rate correction term is also broadcast and it can be used in the event that subsequent correction messages may not be received. The range rate message allows the computation of a current correction from an older range correction using the range rate correction and time of the older range correction.

The differential corrections can be broadcast at frequent intervals in a specified format by a low–medium frequency radio station. Other differential correction broadcast methods exist (commercial satellites and FM radio) but are not covered here. Users with mobile GPS receivers that are equipped to receive and process these corrections in real time can enjoy significant accuracy improvements; e.g., to within 5–10 m, and in some cases in the 1-3 m range or better [1], [3]. A conceptual DGPS station is depicted in Fig. 1.

DGPS removes common errors (satellite clock and orbit errors, atmospheric delay errors) from mobile receivers using the same satellites as the reference station and enhances real-time accuracy. However, the accuracy of the differential correction decreases with significant distances away from the reference station, e.g., beyond about 150–250 miles, when the errors may no longer be spatially correlated between the reference station and mobile receiver [1], [3], [7]. The differential correction data are also stored at selected sites called continuously operational reference stations (CORS) and other reference sites such as the DGPS network operated by private organizations and government agencies. This stored differential correction data can be accessed via the Internet to post-process uncorrected data for situations where real-time DGPS is not required. DGPS is an accuracy-augmentation of GPS that has been successfully used for many applications. In the future more DGPS ground stations will be established and will facilitate new commercial and public safety applications of GPS technology [8]. At present, 34 countries [9] have installed DGPS radiobeacon networks and more are considering adoption of this standard method developed in the United States.

IV. Nationwide Differential GPS Network

In 1996, a Presidential Directive, based on a report by the National Science and Technology Committee, set specific goals for a Nationwide Differential Global Positioning System (NDGPS). These goals include: strengthened national security, integration of GPS into nonmilitary applications, encouraging private sector investment in GPS, and promoting safety and efficiency in transportation and other disciplines [8], [10], [11]. Subsequently, the Department of Transportation (DOT) formed an interagency Executive Steering Group that produced a report on NDGPS identifying many public safety applications, including saving lives on the railroads and highways. In 1997 the U.S. Congress authorized the Department of Transportation to establish, operate, and maintain a Nationwide Differential Global Positioning System as soon as practicable.

The baseline architecture for the NDGPS is the existing United States Coast Guard (USCG) maritime local area DGPS stations [8]. In March 1999, DOT announced the expansion of the existing USCG DGPS network to service the interior portions of the contiguous United States, Hawaii, and Alaska. Key applications of NDGPS presented to Congress were positive train control (preventing collisions, avoiding over-speed derailments, and other safety and economic benefits), public safety and traffic management, control functions for vehicles, notification of emergency conditions, and natural resource and emergency infrastructure mapping. Under NDGPS, the existing network of 54 USCG maritime radiobeacons would be increased with the addition of about 67 new DGPS stations over a three to four year period (Fig. 2). The NDGPS network is presently expanding across the United States and new DGPS stations were installed in 1999 and 2000 [3], [8]. NDGPS provides free DGPS service and it is already in wide use and should be fully operational in all 50 states within about two years (depending on funding). Electric utilities should become

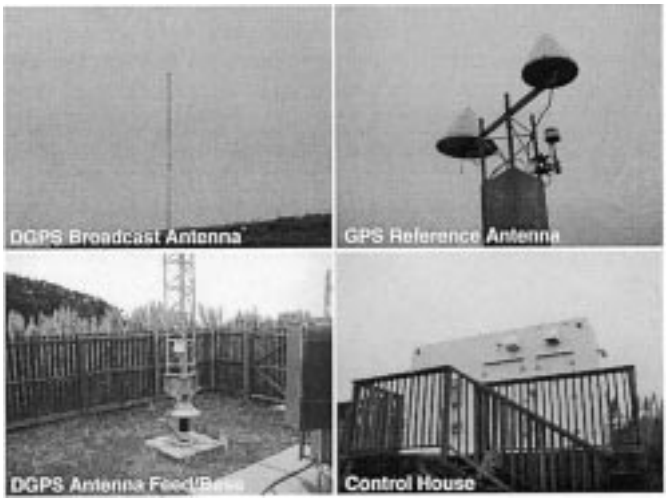


Fig. 3. NDGPS 287 kHz station at Pigeon Point, CA.

familiar with NDGPS plans, operational characteristics, and assets within and near to their service territory.

A typical NDGPS station (Fig. 3) is an unmanned facility that continuously broadcasts a radio signal in the 283.5–325 kHz band. The primary mode of propagation for these low–medium frequency radio signals is by groundwave [12],[13]. Each NDGPS station has a pair of GPS reference antennas (one for standby) mounted on 30-ft tall masts, a control building, ancillary equipment, power supply, communications links, and a broadcast antenna. There are two general designs for the broadcast antenna [8]. The original network of USCG stations have approximately 90–120 ft tall broadcast antennas and the newer stations have 299-ft tall antennas. Most of the new NDGPS stations utilize existing Ground Wave Emergency Network (GWEN) relay-node facilities that have been decommissioned by the U.S. Air Force.

The DGPS messages are modulated onto the low–medium frequency carrier wave by minimum shift keying (MSK). With MSK, a binary zero is represented by a linear 90° phase retard relative to the carrier phase in one bit duration and a binary one is represented by a linear 90° phase advance relative to the phase of the carrier in one bit duration [14]. The selected NDGPS transmission rates are presently 100 and 200 bits per second [8]. The DGPS data rates are low, but are more immune to message loss caused by Gaussian noise and achieve higher message throughput under impulse noise conditions. The 99% power containment bandwidth of the MSK modulated signal is equal to 1.17 times the transmission rate [14]. This means the DGPS broadcast information is contained in a relatively small bandwidth (i.e., 117 or 234 Hz).

The USCG specified minimum field strength for coverage of the DGPS broadcast signal is usually 75 μV/m, or 37.5 dBμV/m. Many DGPS sites with a 200 bit/s transmission rate have a specified minimum field strength of 100 μV/m (or 40 dBμV/m). Terrain and atmospheric conditions can significantly affect the specified coverage range. The specified minimum coverages are provided primarily as a guideline for radiobeacon selection purposes. Adequate DGPS reception and correction message decoding is possible at signal strengths below the specified "minimum" strength, depending on factors

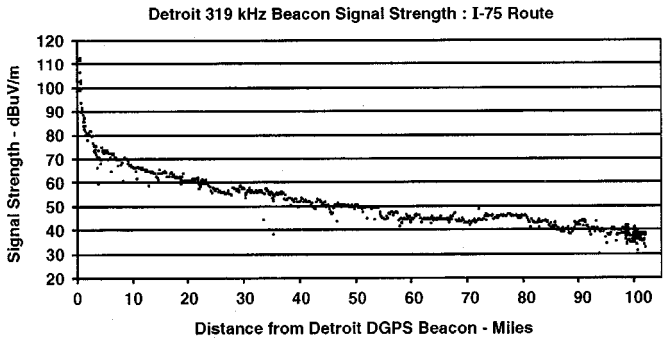


Fig. 4. Signal strength versus distance for Detroit DGPS 319 kHz Beacon.

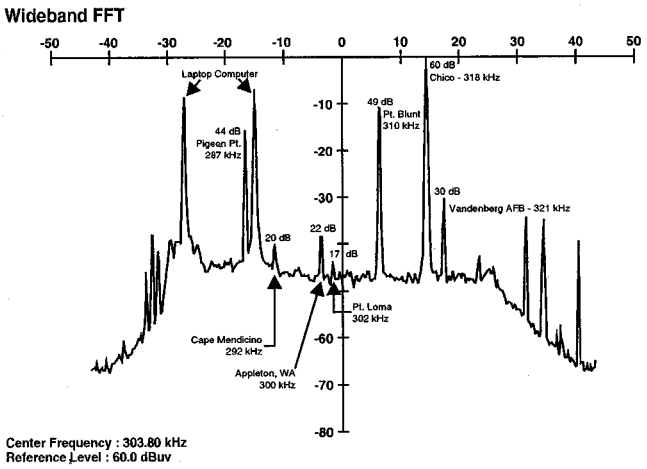


Fig. 5. Signal strength versus frequency: measurements in DGPS band taken in rural area of California.

TABLE I
MEASURED FAIR WEATHER DGPS SIGNAL STRENGTH (dBμV/m)

DGPS Beacon	Site ID	Distance to Beacon	Measured Signal
Chico, CA- 318 kHz	878	119 Mi	60 dB
Point Blunt, CA- 310 kHz	884	49 Mi	49 dB
Pigeon Point, CA- 287 kHz	883	60 Mi	44 dB
Vandenberg AFB- 321 kHz	882	206 Mi	30 dB
Appleton, WA- 300 kHz	871	557 Mi	22 dB
Cape Mendocino, CA- 292 kHz	885	188 Mi	20 dB
Point Loma, CA- 302 kHz	881	424 Mi	17 dB

Note: Laptop computer inside vehicle: 53 dB at ~ 8-10 ft from roof-mounted antenna

such as the level and nature of local noise sources, multipath, receiver design, antenna type, and placement. A plot of DGPS signal strength vs distance is provided in Fig. 4 for the Detroit 319 kHz beacon. A wideband Fast Fourier Transform (FFT) plot in the DGPS band is shown in Fig. 5 for a low noise rural location (central California). The DGPS signal is normalized to the strongest signal within $\pm$44.5 kHz of the center frequency (303.8 kHz). The measured DGPS signal, station ID, and distance is provided in Table I for the stations identified in Fig. 5 plot.

V. Corona and Gap Discharge Noise

Corona is a partial electrical discharge occurring in air near the surface of an energized conductor. It occurs when the electric field at the surface of a conductor exceeds the breakdown strength of the surrounding air [15]. Any conductor surface flaw or irregularity such as a scratch, dust particle, insect, or water drop can concentrate and increase the electric field at this point to the critical level at which a corona discharge occurs. Corona on a high voltage conductor can occur during either the positive or negative half-cycle or at both polarities. Corona discharges can generate visible light, audible noise, and broadband radio frequency (RF) noise. Corona is most often observed on transmission lines in the extra-high-voltage or EHV range (345–765 kV). Radio noise due to corona activity can be present in fair weather due to conductor surface scratches, or nonconductive material on the conductors such as dust, vegetation, or bird droppings. The noise level is higher in foul weather conditions, but also depends on other factors such as the line design, condition of conductor surface, and altitude [16]. During foul weather conditions (rain, fog, sleet, snow), radio noise can significantly increase by as much as 15–25 dB above fair weather levels for the same transmission line [15]–[18]. Radio noise due to corona decreases with frequency, extending from a peak in the low–medium frequency band to low levels at about 10–20 MHz [15], [18]. Corona-generated radio noise is typically measured and calculated in either a 5 kHz (ANSI) or 9 kHz (CISPR) bandwidth with a standardized quasipeak detector; peak and average detector circuits are sometimes used [15]. An important observation is that corona-generated radio noise levels can exceed DGPS broadcast signal strengths, especially in foul weather for lines with high conductor surface gradients.

A gap discharge occurs when two surfaces are very close and at different potentials. Gap discharge sources can be damaged insulators and broken or loose fitting hardware and are generally active only during dry weather. Wet conditions tend to equalize voltages between different parts of the hardware and hence suppress gap discharges [19]–[21]. When a gap discharge is active, the result is a small, intermittent electric arc (spark) between the two surfaces that produces pulses of high frequency electromagnetic waves. These waves can radiate away from the gap source and also propagate along conductors that, in turn, can radiate high frequency noise. Unlike corona, gap discharge noise is characterized by relatively long periods between successive pulses of electromagnetic energy. The RF noise from gap discharges tends to be broadband and spark discharge noise extends over a larger frequency spectrum than corona. RF noise from these sparks tend to dominate those from corona, especially at frequencies above 10–20 MHz and can extend beyond 1000 MHz [19]–[21]. The potential significance of gap discharge RF noise is that its can exceed DGPS broadcast band signal strengths and its broadband spectral content can extend above 1 GHz into the GPS satellite signal band.

VI. Operation of DGPS Receivers Near Corona and Gap Discharge Sources

This paper reports on practical field measurements with typical DGPS receivers near distribution lines, transmission lines, and substations. Of special interest was EHV transmission lines in fair and foul weather and distribution lines with gap discharge sources. At the time of these measurements, the U.S. Department of Defense had implemented dithering of the GPS satellite clock and orbit information to intentionally degrade civilian GPS accuracy by introducing rather large errors. This scheme, called selective availability (S/A), was removed on May 1, 2000.

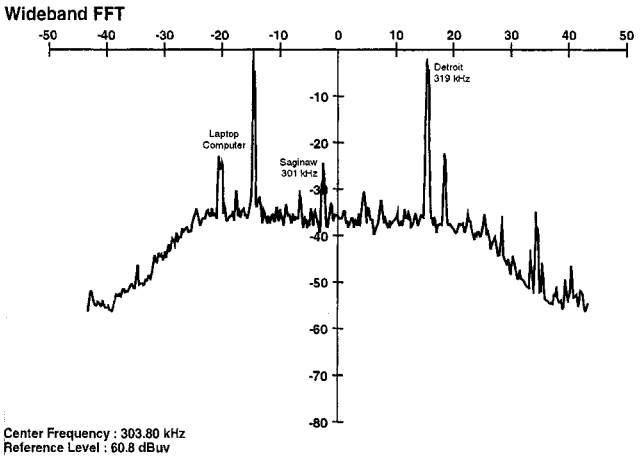


Fig. 6. Signal strength versus frequency in DGPS band: Measurements in shopping center parking lot-steady rain.

The primary equipment used for the field measurements is summarized as follows: spectrum analyzer (Hewlett Packard Model HP8568B, 100 Hz–1.5 GHz), broadband antenna (EMCO Model 6502 active loop antenna, 10 kHz–30 MHz. 60 cm dia.), frequency selective voltmeter (Rycom Model 6020, 0–1500 kHz), Digital GPS receiver (Trimble Navigation, 12 channel/carrier phase filtered with DGPS H-field antenna), and an analog GPS receiver (Garmin, 12 channel and DGPS with either E- or H-field antenna). The analog GPS receiver had an accuracy of about 5–10 m with DGPS augmentation and the digital GPS receiver achieved submeter accuracy in the DGPS mode. GPS parameters and positioning data were recorded using the National Marine Electronics Association (NMEA) data format protocol [22].

A. DGPS Receiver Operation Near Lines in Corona

As described earlier, transmission line corona activity generates broadband radio frequency noise that encompasses the DGPS broadcast band. The potential for corona noise to affect DGPS receiver performance was evaluated by recording signal strength vs frequency plots and logging GPS/DGPS position data near transmission lines in corona. The frequency spectrum plots of Figs. 6 and 7 were made during a steady rain but at locations a few miles apart. Fig. 6 was recorded in a shopping center parking lot, far from power lines. As can be seen in Fig. 6, the ambient noise floor during rain is relatively low (except during lightning discharges when it very briefly jumps up to a high level). In Fig. 7, measurements under a 345 kV transmission line during steady rain reveal an elevated noise floor due to corona activity. The two frequency spectrum plots of Figs. 6 and 7 clearly indicate that corona-generated radio noise can substantially raise the noise floor in the low–medium frequency DGPS band. An elevated noise floor (not shown)

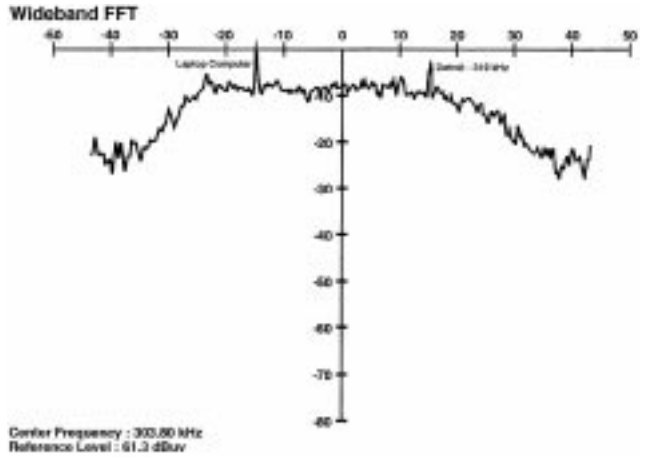


Fig. 7. Signal strength versus frequency in DGPS band: Under 345 kV transmission line during rainy weather (site #2).

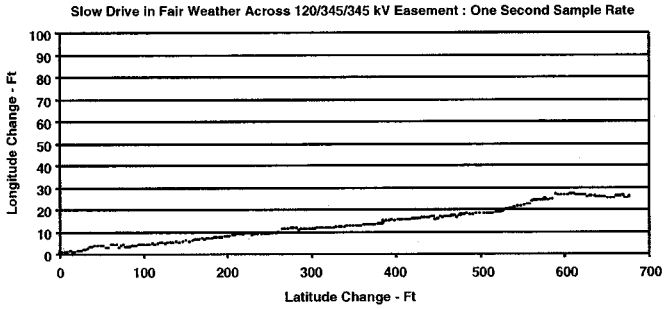


Fig. 8. Plot of positions logged using digital GPS unit (augmented with DGPS)—Taken while driving across 120/345/345 kV easement during fair weather (S/A-ON).

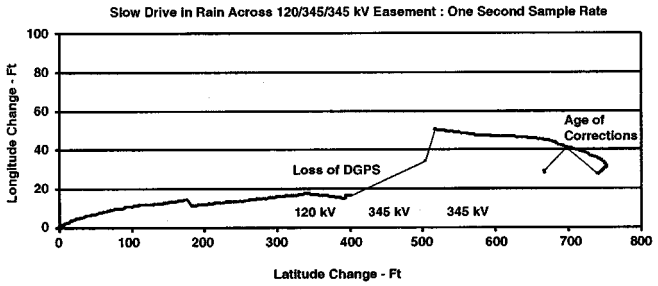


Fig. 9. Plot of positions logged using digital GPS unit (augmented with DGPS)—Taken driving across 120/345/345 kV transmission line easement during rainy weather (S/A-ON).

was also observed for fair weather corona under a twin bundle 500 kV transmission line during a different set of measurements in another state. Elevated in-band noise without an increase in signal strength will result in a lower signal-to-noise ratio (SNR) for a DGPS receiver. Therefore, DGPS receivers operated close to 345–765 kV transmission lines in corona, especially during foul weather, could experience a decreased SNR that may or may not degrade receiver performance. As ambient RF noise in the bandwidth increases, the SNR for the DGPS receiver is further reduced and may approach suboptimal values for receiver performance. This will depend on factors such as the level of corona noise, distance to the line, other ambient or atmospheric noise sources, DGPS signal strength, and receiver/antenna design.

The practical consequences of poor DGPS signal reception are demonstrated in Figs. 8 and 9 for fair weather and rain, respectively. An evaluation of the potential impact of transmission line corona on DGPS receiver performance was conducted at a multiple transmission line easement (double circuit 120 and 345 kV transmission lines). A GPS-equipped vehicle was slowly driven across the easement so that its position, as reported by a digital GPS receiver augmented with DGPS, was logged at one-second intervals. The GPS receiver used a high quality roof-mounted shielded H-field antenna for both GPS and DGPS signal detection. The data were taken on two different days while driving along the same route under the transmission lines (at midspan) for fair weather and in rain. The data collection route across the easement started about 100 m south of the 120 kV line and proceeded laterally to traverse the easement by crossing first under the 120 kV line and then, in succession, under each of the two double circuit 345 kV transmission lines. The plot of positions approximates a straight line in Fig. 8 during fair weather. The vehicle was not driven perfectly straight and position accuracy is within about 1 m or less. In Fig. 9, the same route across the easement is traversed but on a different day during a steady, light rain. As Fig. 9 indicates, the SNR was reduced until it went below the minimum required to maintain lock on the DGPS beacon. The DGPS receiver experienced a loss of the DGPS differential correction messages and suddenly reverted to the standard positioning service with the associated lack of accuracy. Without DGPS the reported position suddenly jumped to a different position with significant error. The magnitude of error for non-DGPS positioning as depicted in Fig. 9 is now much less due to the recent removal of selective availability. As the measurement vehicle continues to traverse the easement DGPS operation is intermittently resumed, albeit with some aging of corrections which is representative of marginal or suboptimum receiver performance. Near the edge of the easement, DGPS corrections are again received on a timely basis and the final few positions shown in Fig. 9 are close to the correct values.

These measurements demonstrate that, even with a very high quality digital GPS/DGPS receiver and antenna, corona noise can degrade DGPS receiver performance in the region near transmission lines. There was no apparent effect on the GPS microwave signal reception quality. However, the DGPS low–medium frequency signals could not be used at some locations close to the 345 kV lines, even with the closest DGPS broadcast beacon only about 20 miles away. Based on limited data for these and for other (unreported measurements) it is estimated that corona-generated RF noise under EHV lines during foul weather has the potential to raise the ambient noise floor by about 20–40^{+} dB in the DGPS band. This is dependent on line design, weather, and ambient noise.

B. DGPS Receiver Operation Near Gap Discharge Sources

Gap discharge sources on power lines can generate radio frequency noise in the DGPS band as previously described. These potential RF noise sources are most commonly associated with ubiquitous distribution lines but can be found on transmission

TABLE II
DGPS RECEIVER PERFORMANCE (dBμV/m) NEAR VARIOUS DISTRIBUTION LINE GAP DISCHARGE SOURCES

Location	DGPS Signal Strength	SNR ~ 100^{+} m Away from Source	SNR Near to Gap Discharge Source
1	52-54 dB	18-22 dB	12-14 dB
2	50 dB	16-17 dB	0-3 dB
3	45 dB	14-16 dB	6-10 dB
4	43 dB	13-16 dB	0-5 dB
5	37 dB	12-14 dB	4-8 dB
6	34-35 dB	17-18 dB	3-5 dB
7	30 dB	16-19 dB	5-7 dB

lines as well. Gap discharge sources (for the measurements reported here) were located either by guidance from a local utility familiar with location and repair of gap sources or by driving and listening to an AM radio tuned off station at 530 kHz. It can be difficult to identify the exact location of a gap source since the electromagnetic energy due to the sparking can be radiated at the source and also propagated along the power line conductors which radiate as well. No attempt was made to find the exact source(s) of gap discharge noise for these measurements. Practical evaluations were performed near a number of gap discharge sources to document the potential for gap noise to affect use of DGPS. Table II summarizes the performance of a high quality GPS/DGPS receiver with a shielded H-field active antenna and advanced multipath rejection features operated near several distribution line gap discharge sources.

Gap discharge RF noise can significantly raise the noise floor in the DGPS band. A frequency spectrum plot of gap-generated RF noise taken near the base of a pole for the DGPS band reveals an elevated noise floor (Fig. 10). It is possible that under certain conditions DGPS receiver performance may be degraded to suboptimal levels by gap discharge noise sources. Of course this will depend on many factors such as DGPS receiver and antenna design, signal strength, noise level, distance from source, and weather (gap sources are often quiet during wet weather).

An evaluation of the potential impact of gap discharge noise on DGPS receiver performance was conducted at a location where power line gap discharge noise was known to exist. A method similar to the corona evaluation of the previous section was used to document DGPS receiver performance. A GPS-equipped vehicle was slowly driven along the shoulder of a road that was parallel to a distribution line with a gap noise source(s). During measurements the vehicle position reported by the digital GPS receiver, augmented with DGPS, was logged at one-second intervals. The GPS receiver used a high quality roof-mounted shielded H-field antenna for both GPS and DGPS signal detection. The measurements were taken driving close to several distribution line poles in fair weather. The SNR of the DGPS receiver began to decrease and increase as the distribution line poles were approached and passed by the vehicle (not shown). This noise was also monitored on the vehicle's AM radio. The plot of vehicle positions while driving close to the distribution line is presented in Fig. 11. The sudden changes in position are due to receiver loss of corrections (caused by poor SNR) and subsequent reacquiring of DGPS accuracy as gap

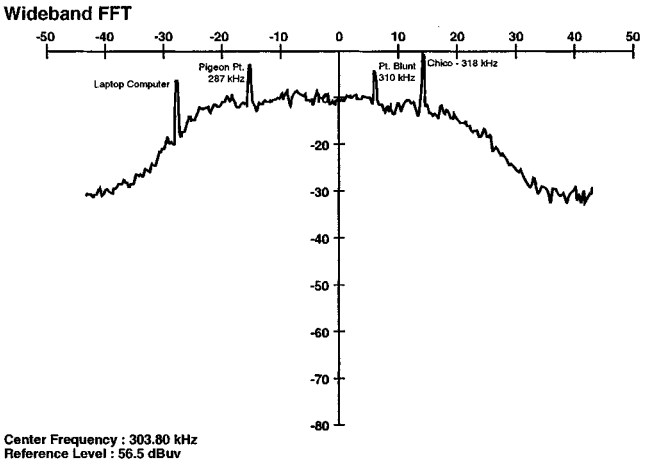


Fig. 10. Frequency spectrum in DGPS band near 13 kV distribution line with gap discharge source(s).

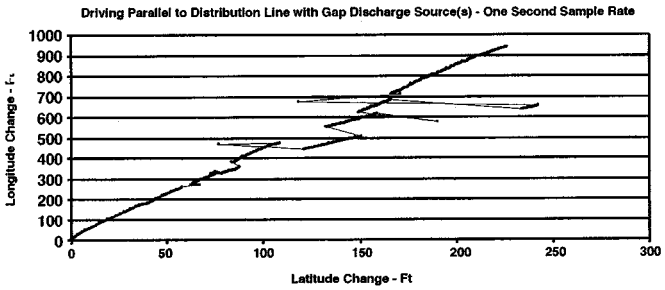


Fig. 11. Plot of positions logged using digital GPS unit (augmented with DGPS)—Driving parallel to distribution line with one or more gap discharge sources (S/A-ON).

noise subsides and SNR improves. The magnitude non-DGPS positioning error is now much less due to the removal of S/A in May, 2000. Not all gap noise sources resulted in this degree of degraded performance. Usually the DGPS receiver was successfully operated close to gap discharge sources on poles (this was not true for the analog receiver, especially when equipped with its rod antenna). Based on limited data and assuming constant signal strength it is estimated that the SNR for a DGPS receiver close to gap sources on poles could be reduced by an average of about 11 dB (a range of about 7–25 dB SNR decrease was observed).

VII. DISCUSSION

In this paper, performance of LF/MF DGPS receivers is evaluated near to corona and gap discharge sources. During many of the measurements near transmission and distribution lines DGPS receivers were successfully operated. However, locations were found and are reported here where foul weather corona or gap discharge sources have the potential to degrade receiver performance. Not all of these situations resulted in loss of DGPS lock. The incidence, duration, spatial extent, and equipment characteristics of degraded receiver performance due to electric power facilities was not extensively evaluated. Factors such as signal strength, noise level, receiver design, antenna type/placement can affect the performance of DGPS receivers. As a generalization, a low cost, entry level analog

DGPS receiver with a vertical (whip) antenna might experience loss of DGPS within about 20–40 m of a robust gap discharge noise source, while a high quality digital receiver with a shielded H-field antenna, advanced multipath rejection features, low internal noise, and carrier-phase smoothing may be able to adequately receive and process the DGPS signal to within 10 m or closer to the gap source, or not loose DGPS at all. Most of the power system sources with the potential to degrade DGPS receiver performance appear to be limited to within perhaps about 25–75 m of the source; or approximately within the bounds of a typical utility easement. The situation with the potential for the largest spatial coverage may be foul weather corona for some EHV transmission lines.

Power line corona and gap discharge noise has the potential to affect DGPS receiver operation by reducing the SNR. This could lead to either a total loss of the DGPS signal or sporadic message decoding errors that result in an age of corrections problem causing the receiver to use dated correction information. Use of old correction messages is allowed by many receivers for as long as 30 s (or longer). The consequence of using old correction messages is not as serious with the removal of selective availability because S/A was by far the fastest changing and largest source of error.

A general estimate for minimum SNR thresholds for DGPS receivers is about 10 dB for analog-based receivers and 7 dB for DSP designs [23]. These levels (and occasionally a bit lower) were verified in the measurements reported in this paper. However, it should be remembered that receiver design can be highly variable across manufacturers. GPS/DGPS receiver manufacturers should be aware of the electromagnetic environments in which their products are used and should incorporate current technology into receiver design for unimpeded receiver use under typical situations. It is important to recall that receiver design has evolved rapidly and that innovations in technology for both hardware and software will continue to be applied to new receiver designs as GPS/DGPS applications grow.

Finally, the removal of selective availability opens the possibility of extending the signal range of individual NDGPS stations while maintaining existing power levels. If a NDGPS station used a slower rate to transmit its messages then the signal will have a narrower bandwidth (99% of DGPS signal power is contained in a bandwidth of 1.17 times the baud rate). Therefore, there will be less broadband noise in the smaller signal bandwidth and overall SNR will improve for the same power to the antenna, thereby increasing station range and coverage. It remains to be seen what actions, if any, are taken by the NDGPS network to take advantage of this opportunity.

VIII. Conclusion

The future of GPS is bright and applications will grow as GPS accuracy is improved with augmentations such as the Nationwide Differential GPS initiative. This paper reports on an evaluation of the possibility for power line corona and gap discharge sources to affect DGPS receivers operated close to power lines. The following conclusions were reached.

- The use of GPS will increase and applications will diversify as more accuracy is offered at no cost by the new Nationwide DGPS network. This network is comprised of low–medium frequency radio stations that continuously broadcast differential corrections in a standard format. The NDGPS network is presently expanding across the United States. It is already in wide use and should be fully operational in all 50 states within about two years. Electric utilities should become familiar with NDGPS plans, operational characteristics, and assets within and near to their service territory.
- Basic GPS use appears to be unaffected by power facilities. The potential to degrade performance of DGPS receivers due to broadband corona and gap discharge noise was found for certain situations close to electric power facilities. However, this is dependent on the DGPS receiver/antenna design and placement, DGPS signal strength, power line design parameters, weather conditions, characteristics of electromagnetic energy emitted by the power system source, and the presence of other nearby RF noise sources such as electronic devices or equipment internal to a vehicle.
- The potential for degraded DGPS receiver performance is dependent on specific local conditions and appears to be limited to areas relatively close to some power facilities, perhaps within a typical easement.
- The impact on positioning accuracy due to temporary loss of DGPS signals may now be less for some applications due to the recent removal of the large errors caused by selective availability.

Acknowledgment

The author would like to thank the EPRI project manager was F. Young. The author relied on advice and assistance from engineers in the GPS community and from electric utilities. Most noteworthy was the guidance on GPS by Dr. A. Lange (Trimble Navigation) and the assistance on field measurements by B. Whitney (Detroit Edison Company). This work greatly benefited from their many contributions. Additional valuable assistance in the form of technical discussions was provided by Dr. R. Olsen (Washington State University) and J. Radice (U.S. Coast Guard).

References

[1] B. W. Parkinson and J. J. Spilker, Eds., "Global positioning system: Theory and applications, Volumes I and II," in *Progress in Astronautics and Aeronautics*. Piscataway, NJ: AIAA, 1996, vol. 163 & 164.
[2] "GPS status list," NISWS—Navigation Information Service Watch Stander, U.S. Coast Guard Navigation Center, Daily Update of GPS Satellite Status, Jan. 15, 2001.
[3] P. Enge and P. Misra, "Scanning the special issue/technology on global positioning system," *Proc. IEEE*, vol. 87, pp. 9–15, Jan. 1999.
[4] G. T. Kremer *et al.*, "The effect of selective availability on differential GPS corrections," *Navigation*, vol. 37, no. 1, Spring 1990.
[5] D. Pietraszewski *et al.*, "U.S. Coast Guard differential GPS navigation field test findings," *Navigation*, vol. 37, no. 1, Spring 1990.
[6] P. Lomis *et al.*, "Correction algorithms for differential GPS reference stations," *Navigation*, vol. 36, no. 2, Summer 1989.
[7] E. D. Kaplan, Ed., *Understanding GPS Principles and Applications*. New York: Artech House, 1996.
[8] U.S. Department of Transportation, "Programmatic environmental assessment: Nationwide differential global positioning system," U.S. Dept. Transportation, Dec. 1998.
[9] (2001) Trimble Navigation Internet Web Site

[10] "U.S. Global Positioning System Policy—Fact Sheet," The White House Office of Science and Technology Policy, Nat. Security Council, Washington, DC, Mar. 29, 1996.
[11] U.S. Department of Commerce, "A technical report to the Secretary of Transportation on a national approach to augmented GPS services," U.S. Dept. Commerce, NTIA Rep. 94-30, Dec. 1994.
[12] P. K. Enge *et al.*, "Coverage of DGPS/radiobeacons," *Navigation*, vol. 39, no. 4, Winter 1992–1993.
[13] P. K. Enge and K. E. Olson, "Medium frequency broadcast of differential GPS data," *IEEE Trans. Aerosp. Electr. Syst.*, vol. 26, pp. 607–617, July 1990.
[14] U.S. Department of Transportation, United States Coast Guard, "Broadcast Standard for the USCG DGPS Navigation Service," U.S. Dept. Transportation, United States Coast Guard, COMDTINST M16577.1, Apr. 1993.
[15] *Transmission Line Reference Book—345 kV and Above*, 2nd ed: Electric Power Research Inst. (EPRI), 1982.
[16] P. S. Maruvada, *Corona Performance of High-Voltage Transmission Lines*. Philadelphia, PA: Research Studies, 2000.
[17] "Addendum to interferences produced by Corona effect of electric systems: Description of phenomena and practical guide for calculation," in *International Conference on Large High Voltage Electric Systems (CIGRE)*: prepared by Working Group 36.01, (EMC Aspects of Corona, Electric and Magnetic Fields), July 1996.
[18] *IEEE Standard Procedures for the Measurement of Radio Noise From Overhead Power Lines and Substations*, ANSI/IEEE Std. 430-1986, Feb. 1986.
[19] "The ARRL RFI Book," in *Electrical and Power-Line Interference*: The American Radio Relay League, 1998, ch. 11.
[20] "The location, correction, and prevention of RI and TVI sources from overhead power lines," in *IEEE Tutorial Course Text: 76 CH1163-5-PWR*: IEEE Power Eng. Soc., 1976.
[21] M. O. Loftness, *Power Line Interference: A Practical Handbook*: National Rural Electric Cooperative Association, NRECA Res. Project 90-30, 1992.
[22] "Standard for interfacing Marine electronic devices—NMEA 0183," National Marine Electronics Association, Ver. 2.30, March 1, 1998.
[23] "Private communication: Telephone discussion on DGPS signals and receivers with Mr. Jim Radice, Engineer, U.S. Coast Guard," unpublished, Oct. 1, 1999.

J. Michael Silva (M'76–SM'84) received the B.S. degree from the University of Alabama, Tuscaloosa, in 1971 and the M.S. degree from Auburn University, Auburn, AL, in 1976, both in engineering.

He has been actively involved in electric power research for most of his 30-year professional career. He has worked for the Southern Company, the Electric Power Research Institute, GAI, and founded Enertech Consultants, Campbell, CA, in 1982, where he serves as President. He has directed pioneering efforts in instrumentation for personal exposure measurements and software for electromagnetic field modeling. He is presently leading a team that has developed a personal GPS logger for scientific and medical research applications using state-of-the-art GPS technology.

Mr. Silva is a member of the Institute of Navigation and is a registered professional engineer in seven states and the Territory of Guam.

Discussions and Closures

Discussion of "Evaluation of the Potential for Power-Line Noise to Degrade Real-Time Differential GPS Messages Broadcast at 283.5–325 kHz"

Vernon L. Chartier

After reading this paper[1] a couple of times, I wondered how it made it through the IEEE peer review since the paper has several errors and other problems. Here are the most obvious ones. First, Figs. 6 and 7 are mislabeled. These plots are not signal strength versus frequency. The units for signal strength are decibels microvolts per meter and not decibels microvolts. Also, in reporting electromagnetic-interference (EMI) measurements, the detector that was used to measure field strength must be specified, such as peak, quasipeak, average, root mean square (rms), as well as the bandwidth. Second, the x-axes of Figs. 6, 7, and 10 are not frequency. I am not sure what you call an axis that is $\pm$ a center frequency, but it definitely is not frequency since radio noise meters and spectrum analyzers are not capable of measuring EMI at a negative frequency. Third, the author says that the ambient noise floor in Fig. 6 is relatively low. What is the author defining as ambient noise, and how does a reader of this paper determine if the ambient noise is low when the author does not report the measurements in the correct units? There are number of manmade signals and noise sources in the middle-frequency (MF) and high-frequency (HF) bands, and many of those sources can be found in shopping center parking lots. Also, depending upon the region, the time of the year, and the time of day, atmospheric noise can be very high or very low in these bands. The voltage seen on a spectrum analyzer is also a function of the sensitivity of the receiver and the antenna. Fourth, a bidirectional loop antenna was used to make the measurements, but the author does not say how it was oriented. Fifth, the units and bandwidth for signal-to-noise ratios must also be specified, or they have very little meaning.

There are other problems with this paper. The author says "corona-generated radio noise is typically measured and calculated in either a 5-kHz (ANSI) or 9-kHz (CISPR) bandwidth with a standardized quasi-peak detector." ANSI standard C63.2-1996 specifies the same QP detector as IEC/CISPR 16.

The author says, "corona is most often observed on transmission lines in the extra-high-voltage (EHV) range (345–765 kV)." If the statement is taken at face value, it means that corona from lines operating above 765 kV are not a problem, and it means that the 230-kV lines in the U.S. that are noisier than some 345- and 500-kV lines are not a problem. Even 138- and 115-kV lines have corona, especially in foul weather. The magnitude of the corona is largely dependent on electric field at the surface of the conductor, which depends on the voltage and the geometry of the line.

Why did the author focus on foul-weather noise when that is not the predominant weather pattern? It is well known that there are 500- and 765-kV lines in the U.S. that are noisier in fair weather than many 345-kV lines are in foul weather. Readers of this paper cannot determine the noise level of this particular 345-kV line because not only does the author not report the measurements in the correct field-strength units, but he also does not provide the geometry of the line.

Manuscript received January 29, 2001.

The author is a Power System EMC Consultant residing at 13095 SW Glenn Court, Beaverton, OR 97008-5664 USA (e-mail: vlchartier@ieee.org).

Digital Object Identifier 10.1109/TPWRD.2002.805035

[1]J. M. Silva, *IEEE Trans. Power Delivery*, vol. 17, pp. 326–333, Apr. 2002

Finally, I wonder why did the Electric Power Research Institute spend research funds on these measurements. The manufacturers of digital global positioning systems (DGPS) readily admit that power-line noise can cause interference. Therefore, they know that the use of DGPS is limited unless greater immunity is built into these instruments through hardware and/or software. There are regions of the U.S. where atmospheric noise in the summer months is much higher than corona noise from power lines in the MF and HF band, which would indicate that the use of DGPS during those periods is difficult.

In summary, it appears that the only thing this effort proved was that corona and gap-type noise have the potential to degrade the performance of DGPS receivers, a fact already known by these receiver manufacturers.

Closure to "Evaluation of the Potential for Power-Line Noise to Degrade Real-Time Differential GPS Messages Broadcast at 283.5 to 325 kHz"

J. Michael Silva

The author would like to thank Mr. Chartier for his discussion and is pleased to provide this closure. The discusser initially raises the question of peer review. The IEEE peer reviewers all commented that the paper was "well written" and "timely," and one reviewer commented that this work allows readers "to achieve an extraordinary understanding in a short time of the potential and real problems of GPS interference issues." The author also submitted this work to independent technical review by several engineers who have experience in electromagnetic interference (EMI) and who did not have the difficulty expressed by the discusser.

In the above paper,[1] one of the main purposes of Figs. 6 and 7 is to graphically depict a low signal-to-noise ratio for the reader. This is done by presenting fast Fourier transform (FFT) plots within the differential GPS (DGPS) band of 283.5–325 kHz at locations far from and close to a double-circuit 345-kV transmission-line corridor during rain. The reader can clearly see the effect of broadband corona noise for a DGPS receiver. The discusser is concerned over the statement that Fig. 6 depicts a "relatively low ambient noise floor." A number of ambient measurements away from the transmission-line corridor were made in addition to Fig. 6 and all showed a similar magnitude noise floor. Relative to the transmission-line location, the noise floor was low and the signal-to-noise ratio was high. As stated in the paper, occasional distant lightning discharges significantly raised the noise floor, but only temporarily. This atmospheric noise is characterized as impulse noise, and the DGPS signal format is designed to resist temporary atmospheric noise impulses. The DGPS broadcast format used in the nationwide DGPS (NDGPS) network features a number of message types. The actual differential corrections are broadcast in what is called a Type-9 message, which is a partial correction set for up to three satellites (e.g., if the receiver is using eight GPS satellites, it will take three Type-9 messages to receive the full set of corrections). Therefore, occasional

Manuscript received January 29, 2001.

The author is with Enertech Consultants, Campbell, CA 95008 USA.

Digital Object Identifier 10.1109/TPWRD.2002.805033

[1]J. M. Silva, *IEEE Trans. Power Delivery*, vol. 17, pp. 326–333, Apr. 2002

Interference Effects on the Global Positioning Satellite Signals

Wan Aziz W.A[1] and Low, T.Y.[1]

[1]*Department of Geomatic Engineering*
Faculty of Geoinformation Science & Engineering
University Technology Malaysia
81310 Skudai, Johore, Malaysia

Abstract Nowadays, the Global Positioning System (GPS) has emerged as a universal cornerstone for much of our technological infrastructure. GPS is a space-based radio navigation satellite service that provides universal access to position, velocity, and time information. Thus, the worldwide availability of GPS signal coverage has been responsible for many exciting developments in the field of positioning for geoscientific applications. However, The GPS signals can be corrupted, either intentionally or unintentionally by strong interfering sources. The interference sources such as microwave transmission towers, radar frequency and multipath (caused by extraneous reflections from nearby metallic objects, ground or water surfaces reaching the antenna) can affect GPS applications particularly in geodetic field work. This paper therefore highlights the interference effects on GPS signals. Some experimental results are presented and discussed.

1. Introduction

The NAVSTAR Global Positioning System (GPS) is a space-based radio navigation satellite service that has revolutionized navigation. It is an ingenious combination of applied science and technology for providing worldwide and round-the-clock information on navigation and position determination. Therefore, for the past ten years, we have witnessed a dramatic increase in the use of the GPS technology for many types of scientific applications. For examples, the Maritime and Waterways (Search and rescue, harbour approach navigation), Railroad (Vessel traffic services, Railroad fleet monitoring), Public Transportation (Accident location reporting Tracking and recovering stolen vehicles, Bus fleet on-the-road management), Telecommunication (Border surveillance, Precise timing for messages) Electric Power (Synchronization of frequency/phase, cellular radiotelephone base station time base, Fault event location) and Surveying (National spatial data infrastructure, Hazardous and structural monitoring).

Like most surveying technologies, GPS surveying techniques are not infallible. For all of its technological splendour, GPS has its weaknesses. The principal of these is the low power level radiated by the satellites, which introduces vulnerability to interference. As new wireless applications and technologies continue to develop, conflicts in spectrum use and system incompatibility are inevitable, for example the ultra wideband (UWB) signals and electrical interference. UWB signals are characterized by modulation methods that vary pulse timing and position rather than carrier-frequency, amplitude, or phase. Electrical interference can result from electrical storms, power lines, 2-way radios, nearby electric motors, microwave towers, cellular phones, vehicular electrical equipment such as alternators and ignition

0-7803-8102-5/03/$17.00 © 2003 IEEE

systems on spark-ignition engines, and pulsed interference from airport communication radar signals. Several authors reported already GPS interference in different countries [1]. None of these is believed to be a real problem to GPS, but we should be aware of them, nonetheless. Some of these have at times produced interference to GPS receivers. The objective of this study was to measure the degree of interference to GPS signals in positioning task, particular investigations will be concentrated in biases and errors in observed coordinates.

2. Review on the GPS and Signal Interferences

The main goal of the GPS is to provide worldwide, all weather, continuous radio navigation support to users to determine position, velocity and time throughout the world. The technical and operational characteristics of the GPS are organized into three distinct segments: the space segment, the operational control segment, and the user segment – see Figure: 1. The operational GPS constellation uses 24 satellites, of which 3 are spares, orbiting in precise 12-hour orbits. The satellites are controlled via a worldwide network of tracking stations, with the Master Control situated at Falcon AFB in Colorado. The Master Control station measures signals from the satellites to incorporate into precise orbital mathematical models, which are then used to compute corrections for the clocks on each satellite. These corrections and orbital (ephemeris) data are then uploaded to the satellites, which then transmit them to GPS user's receivers.

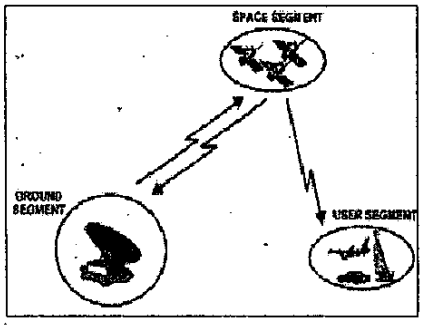


Figure 1 The GPS Segments

Each GPS satellite transmits data on two L-band modulate frequencies, L1 and L2. The L1 signal (transmitted at 1575.42 MHz) carries two codes, a Coarse/Acquisition (C/A) code and a Precision (P) code. The L2 signal (transmitted at 1227.60 MHz) carries only the P code, which is encrypted so only the military and other "authorized" receivers can interpret it. Both L1 and L2 signals are use to determine distance between satellite and the receiver by measuring the radio travel time of the signals. Details of the GPS signals can be found in [2].

The following information provides an overview on electromagnetic radiation. This has been included to aid understanding of test results and is not meant to be definitive. No background information is provided on multipath since it is assumed readers will have an understanding of this phenomenon. Electromagnetic radiation as it relates to electrical noise arises in two forms. One, *intrinsic noise*, is the result of the random movement of electrons within the circuit elements of the electrical device itself. The second form is *interference*, which occurs as a result of signals being emitted from other circuits or systems. This is known as *interference.*, [4]. This electrical noise corrupts the signal of interest and introduces an uncertainty into the information that it contains. It was expected that electromagnetic radiation emitted from the high voltage transmission lines would be the most likely cause of any inconsistency with GPS positioning mode. This interference could be arriving at the GPS receiver through any element of the receiver acting as an antenna. The effects that the electrical noise has on the GPS system will be dependent on the circuitry used.. The electrical noise could cause errors in either, or both, the measurement of the signal timing and the phase of the signal. The electrical noise will manifest itself in the form of an electric field and a magnetic field around the high voltage wires.

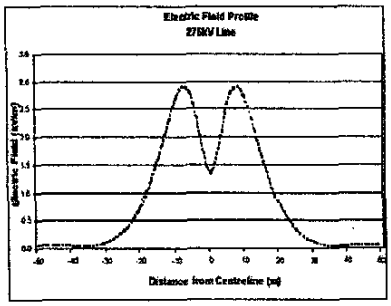


Figure 2 The Electrical Field produced from Transmission Line

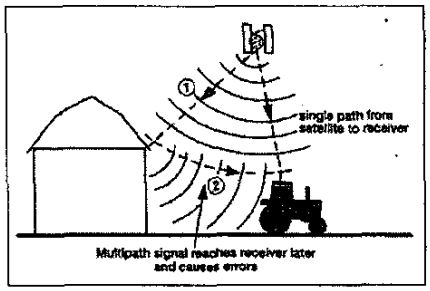


Figure 3 The Multipath Effects

Figure 2 displays the strength of the electrical field produced from a 250 kV transmission line in relation to a ground distance at right angles to the lines away from a point directly beneath the centre of the transmission lines. It indicates that at approximately 30 metres from the centre line most of the electrical field influences are minimal.

The carrier wave propagates along a *straight* line (not quite, there are small bending effects due to the presence of the atmosphere). Multipath is caused by extraneous reflections from nearby metallic objects, ground or water surfaces reaching the antenna – see Figure: 3. In other words, the GPS signals can sometimes "bounce" off of objects in their path and cause the signal to reach the receiver on a different path. This has a number of effects: it may cause signal interference between the direct and reflected signal (see Figure 3) leading to *noisier* measurement, or it may confuse the tracking electronics of the hardware resulting in a biased measurement that is the sum of the satellite-to-reflector distance and the reflector-to-antenna distance. The multipath can affect each satellite-receiver combination independently, and hereby it is not reduced in the double differencing. Thus, the main problem when handling multipath is that there is no general model to correct for it. It behaves differently for difference frequencies, geometries and receiver locations, and there are no mathematical correlations among them.

3. Experimental

In our experiments, four test sites have been chosen, and they are noted as Test Site I, II, III and IV, respectively.

Test site I represented 'ideal' site known as Bukit Komenwel (Ia) and 'interference site of high voltage' known as Salak Selatan (Ib) – see Figure: 3 . Both test sites are in in Kuala Lumpur and it is configured by five GPS stations. Since no multipath was expected at this site, and there were no obstructions to the satellite window, it was expected that very few incorrect initializations would be recorded at this site. The Geo-Explorer 3 GPS receiver has been used for this experiment. To evaluate the integrity of this receiver a large amount of data was collected and statistically analyzed. The data was collected with a minimum of human intervention.

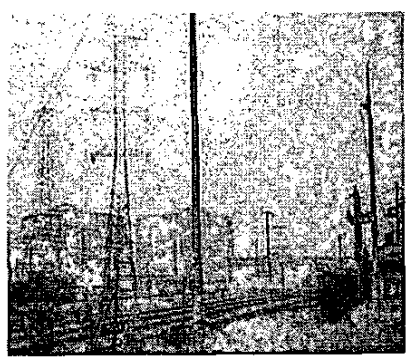


Figure 4 The Test Site I

Test Site II located in Johore Bahru was also chosen to determine the effect of High Voltage power lines on the system's ability. The first test station (Stn. 1) at this site was marked directly beneath power lines and the other station (Stn. 2) is approximately 30 metres away from a transmission tower structure – see Figure: 5. The Trimble 4800 Series GPS receiver has been used to perform this task.

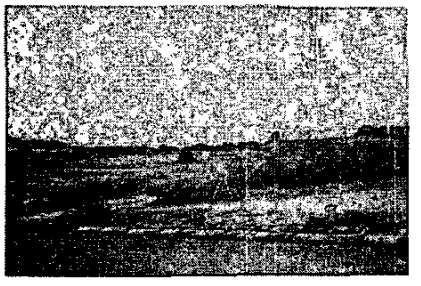


Figure 5 the Test Site II

Test Site III was located in Bayan Lepas International Airport, Pulau Pinang . The survey is consisted of one based point about 300 m from the air-traffic control towers (DCA02) in length, and the other point was about 10 km baseline from the airport (P314). The method of GPS observation was in relative mode using the Leica 300 Series GPS receivers. Two relative stations about 20m apart, (namely Stn. 1 and Stn. 2) were also established with respect to these based (control) points – see Figure: 6. Their corresponding relative distance is about 2km and 8 km away from P314 and DCA02, respectively. As a matter of fact, this experiment has been carried out in conjunction with the monitoring survey of the KOMTAR building, the highest building in the northern region – see [6] for details. The sky view at the based stations and relative stations is very good, i.e. no satellite passed obstruction.

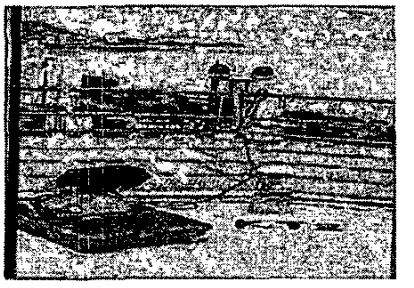


Figure 6 The Test Site III

Test Site IV was in the UTM Campus to study the effect of multipath in GPS observations. The Trimble 4800 Series GPS receiver is used to collect the data within 2 days of observations. For the Day1 observations, the 'normal GPS antenna' is used and for the Day2 observations, the 'ground-plane GPS antenna' is used. The ground- plane antenna is specifically designed for multipath error reduction (although is quite heavy). One station (namely Stn. 1) is established near the building (mosque) and the static GPS observation is carried out with respect to the base stations G1 and G11. The corresponding distance of Stn. 1 with respect to G1 and G11 is about 1.5km and 100m, respectively.

4. Results and Analysis

The standard deviation of the horizontal coordinates (X, Y) for both test site I(a) and I(b) is summarized in Table: 1. The Root Mean square (RMS) value is also illustrated in Figure: 7. In generally, it can be seen from Table: 1 that the standard deviation of the observation for the object points is quite significant for the test site I (b), i.e. the area of Salak Selatan as this site is exposed to the high voltage transmission power lines. Similarly, the RMS value is much lower for the test site I(a) compared with test site I(b) in Salak Selatan.

TABLE 1

The Standard Deviation for Test Site I

GPS Stn.	Std. Deviation Test Site I(b)		Std. Deviation Test Site I(a)	
	X	Y	X	Y
1	1.4708	1.4145	0.1678	0.3104
2	1.9537	1.0299	0.5957	0.3595
3	1.6457	0.6641	0.0978	0.3227
4	0.7108	0.2977	0.3695	0.5640
5	0.6537	0.3561	0.3154	0.4423

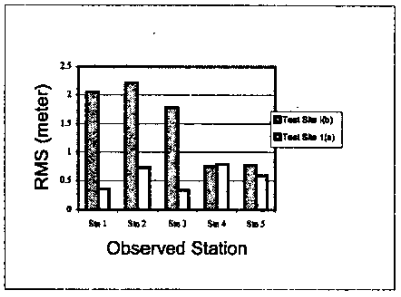
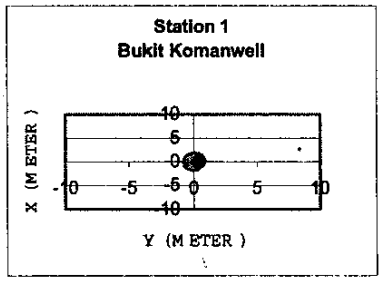


Figure 7 The RMS values for the Test Site I

One of the station at the Test Site I (i.e. station 1) has been computed for its 2D-coordinate position during the experiment, and the corresponding results is graphically shown in Figure: 8. In general, it can be seen that the accuracy in X and Y coordinates for Bukit Komenwel site is less than 1 m compared with the one at Salak Selatan site. The scattered X, Y coordinates for this test site is between ±1 to ±5 m.



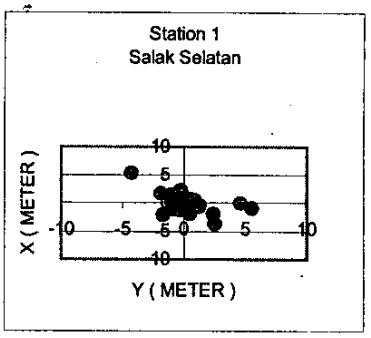


Figure 8 The Scattered X, Y Coordinate Values for Test Site I – Station 1

The result for the test site II is illustrated in Figure: 9. The residual distances shown in this figure indicates that the value is rather significant at test site II Stn. 1 because this station is located directly beneath the high voltage power lines (see dashed lines). The corresponding value is between –0.01 m to 0.04 m compared with the one from the test site Stn. 2 (which is about 30 meter away from the high voltage power line). The overall value at this station is about ± 0.01 meter only.

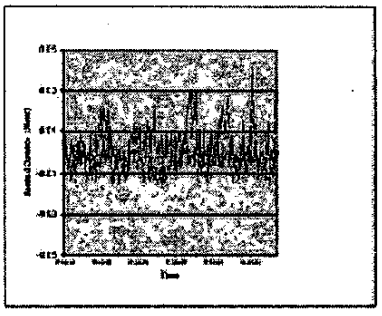
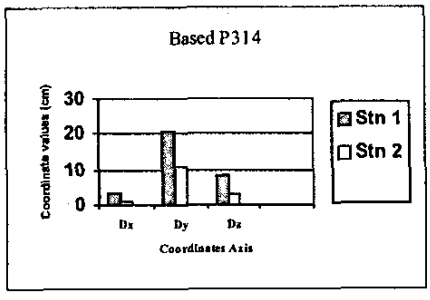


Figure 9 The Residual Distance for Test Site II – Stn.1 and Stn.2

The experiment for the Test Site III was also processed with respect to both based (fixed) stations P314 and DCA02, and it's result is shown in Figure: 10. From this figure, it is clearly shown that the coordinate values differences from the mean value

during the observation is rather significant for the based station DCA02 (near the airport) compared to based station P314, although the sky view and also the Dilution of Position (the satellite-receiver geometry) at these stations is less than 3.



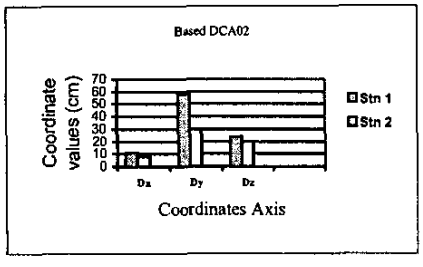


Figure 10 The Coordinate Difference between P314 and DCA02 for Test Site III

For the Test Site IV, the multipath effect is summarized in Table: 2. From this table, the ratio between Day1 and Day2 observation is clearly shown that the ground plane antenna is significantly reduce the multipath errors compared with the normal GPS antenna. The ratio is defined as the relationship between two variances in the integer ambiguity resolution (for fixed solution only). The higher ratio value will show the better GPS solutions. Similarly, it also can be seen from this table that the RMS values for Day2 observations is much better than (lesser values) the Day1 observation for both GPS baselines. The difference in the RMS value is between 0.001m to 0.003m for the observations. This experiment shown that the use of ground-plane GPS antenna is subsequently provides superior multipath reduction compared to normal antenna and it is very useful in Real Time Kinematic (RTK) GPS mode.

Table: 2 – The Results from Test Site IV

From	To	RMS Day1 Day2	Ratio Day1 Day2
G1	Stn. 1	0.018 0.015	3.95 4.37
G11	Stn. 1	0.011 0.009	4.28 4.73

5. Conclusions

GPS is a powerful enabling technology that has created new industries and new industrial practices fully dependent upon GPS signal reception. Up to now we have been treating the calculations that go into GPS very abstractly, as if the whole thing were happening in a vacuum. But in the real world there are lots of things that can happen to a GPS signal. For example, the presences of electromagnetic interference, ultrawideband and multipath have been shown to significantly impair the process of integer ambiguity resolution. The conclusions will be of value to individuals who are planning to carry out the GPS measurements beneath high voltage power lines, or other areas in which significant signal interference may be present. However, it must be recognized that since the data was not collected in a strictly controlled environment, the results quoted in this paper should be used as a guide only and should not be considered definitive.

6. References

[1] Butsch, F. ,1997 : " GPS interference problems in Germany" . Proc. ION Annual Meeting, Albuquerque, N.M., USA.

[2] Rizos, C.,1996 : "Principles and Practice of GPS Surveying". GMAT5222 Course Note, UNSW, Australia.

[3] Haagmans, M. E. ., 1994: "GPS signal reception problems: the situation in the Netherlands". GPS Niusbrief, May 1994, p. 67-69.

[4] Fish, P.J., 1994: "Electronic Noise and Low Noise Design.",The Macmillan Press, Hampshire London.

[5] Low, T.W., 2003 : "Kesan Talian Elektrik Kuasa Tinggi Tehadap Isyarat GPS"- Projek sarjana muda FKSG, UTM.

[6] Wan. A.A., 2002: " The IRPA Vot No. 72308 Unpublished Research Report" , RMC, UTM.

THE MECHANISM AND EXPERIMENTAL STUDY ON THE INTERFERENCE OF HIGH VOLTAGE LINES TO NAVIGATION SYSTEM

L.J. FAN†‡, X.C. PAN†, Z.X. HUANG† and X.D. ZU†

†*ZNDY, School of Mechanical Engineering, University of Science and Technology, Nanjing 210094, Jiangsu, China.*
‡*Special equipment inspection institute, Hefei 230000, Anhui, China.*
Pxc_nust@163.com

***Abstract*— This essay conducts the mechanism analysis and experimental study on the interference of high voltage lines to the navigation system of UAV and shows that the essence of the interference is that air becomes corona plasma after the ionization under high voltage. In addition, when GPS signals pass through this area, some frequency channel will be absorbed. Therefore, the propagation of electromagnetic waves is prevented. The UAV tries to get GPS positioning signal by flying through high voltage area in a low height, resulting in the loss of GPS signal received by the navigation system. Through the measurement and comparison of the electromagnetic wave spectrum traveled through corona plasma, the corona plasma's absorbing of electromagnetic wave is observed.**

***Keywords*—high voltage line; corona plasma; electromagnetic wave; refraction resonance; absorption prevention.**

I. INTRODUCTION

The altitude of ultralow altitude UAV is between 0 and 100m and such UAV is widely used in agricultural plant protection, power line patrol and other fields. There exists a large number of lines whose high voltage range, from several to hundreds of kVs, may cause serious interference to the navigation system of UAV. This can lead to the loss of GPS data of the navigation system and accidents and it might even hit the transmission lines and insulated terminals causing a serious electric accident (Liu *et al*., 2011; Chen *et al*., 2008; Yin *et al*., 2009).

The interference of high voltage line to the GPS system of UAV draws the attention of many scholar and technological personnel and they focus on the study on the mechanism of interference and the protection. At present, the commonly accepted explanation is that the high voltage lines generate strong electromagnetic radiation field and the radiated electromagnetic field interacts with the UAV navigation system through coupling, which leads to the error of navigation system (Zhang *et al.*, 2011; Wu *et al.*, 2009). However, such explanation does not explain the phenomenon that UAV does not interfered while flying above the electrical lines higher than the high voltage line.

Theoretically, the frequency of electromagnetic radiation is very long and it is difficult to slot coupling (Liu *et al.*, 2000; Liu *et al.*, 2008; Xiao *et al.*, 2007) with the navigation system of UAV. Through the generation and diffusion of corona plasma, this essay believes that the essence of high voltage line's interference to UAV is that air is ionized under high voltage to form a plasma. The plasma has a strong shielding effect on the GPS signal transmitted by the satellite causing the loss of signal of the navigation system (Das, 2017). Meanwhile, through the experiment of receiving GPS navigation data while the UAV flies through high voltage line area in low attitude and the measurement and comparison of the electromagnetic wave absorption spectrum while electromagnetic wave through the corona plasma, it proves the absorption of electromagnetic wave by corona plasma.

II. THE GENERATION AND DIFFUSION OF CORONA PLASMA

Due to the high voltage electric field, the air is ionized and generates corona plasma. Because the mass of the positive charge in the corona plasma is larger, the motion is slow, and the range of motion is much smaller than that of the electron. Therefore, the charged particles in this paper mainly refer to the electron (Dey, 2017).

When the charged particle is generated, it will move under the action of electric field and magnetic field, and its motion is very complicated. Considering the effect of magnetic field is much smaller than that of electric field, which is:

$$\vec{E} >> \vec{v} \times \vec{B} \tag{1}$$

Where $\vec{E}, \vec{v}, \vec{B}$ respectively refer to electric field intensity, charged particle velocity and magnetic field intensity and the effect of magnetic field on the motion of charged particles can be ignored. Therefore the problem can be simplified to the motion of charged particles in an electric field. Then the corona induced by this motion is discussed.

It is assumed that the electric field on the surface of the conducting wire is constant and equal to E_c

$$E_c = \frac{U}{r_0 \ln \frac{2h}{r_0}} \tag{2}$$

Where h refers to the lead height, U the

voltage of the lead and r_0 the semi-diameter of the lead. h is much greater than the semi-diameter of lead r_0, therefore the electric field intensity E in the space near the conductor is similar to the electric field of coaxial cylindrical capacitor，so:

$$E = \frac{U}{r \ln \frac{R}{r_0}} \tag{3}$$

Where R refers to the inner radius of coaxial cylindrical capacitor. So:

$$Er = \frac{U}{\ln \frac{R}{r_0}} \tag{4}$$

This is constant, then:

$$Er = E_c r_0 \tag{5}$$

Therefore the ion speed is:

$$v = \frac{dr}{dt} = kE = kE_c \frac{r_0}{r} \tag{6}$$

The formula above can be rewritten as follows:

$$dt = \frac{rdr}{kE_c r_0} \tag{7}$$

Integrating on half cycle and considering $r_{\max} >> r_0$, the formula above can be rewritten a

$$r_{\max} \approx \sqrt{kTE_c r_0} \tag{8}$$

put $T = 0.02s$, $r_0 \approx 1.25cm$, $k = 1.8\frac{cm/s}{V/cm}$, $E_c \approx 3MV/cm$ into the formula above, so $r_{\max}$=2.2m.

As it is seen, the effective diffusion distance of charged particles is very large. After the charged particles are generated, diffusion escape and compound disappearance happen, meanwhile a new plasma is formed by the ionization of the air in the electric field, and the dynamic equilibrium is reached forming stable distribution of plasma corona region.

III.SCATTERING OF ELECTROMAGNETIC WAVE BY CHARGED PARTICLES

The plasma corona region will obviously produce refraction and reflection of electromagnetic wave, which will affect the propagation of electromagnetic wave. The propagation of electromagnetic wave in charged particles can be analogous to the propagation of electromagnetic wave in a conducting medium and the propagation constant of electromagnetic wave in conductive medium is

$$\gamma = \sqrt{j\omega\mu(\sigma + j\omega\varepsilon)} \tag{9}$$

where ω refers to angular frequency, μ permeability, ε dielectric constant and σ conductivity. The development of the formula above concludes an attenuation constant

$$\alpha = \omega\sqrt{\frac{\mu\varepsilon}{2}\left(\sqrt{1+\frac{\sigma^2}{\omega^2\varepsilon^2}} - 1\right)} \tag{10}$$

and a phase shift constant

$$\beta = \omega\sqrt{\frac{\mu\varepsilon}{2}\left(\sqrt{1+\frac{\sigma^2}{\omega^2\varepsilon^2}} + 1\right)} \tag{11}$$

As it is seen, the amplitude attenuation and phase shift will occur when the electromagnetic wave propagates in the charged particles and , so that the amplitude of the GPS signal is weakened or the error occurs.

IV. EXPERIMENTAL VERIFICATION

A. Experimental arrangement

The experiment can be divided into two parts, which respectively test the corona plasma shielding effect to GPS navigation signal from satellite and the absorption spectrum to electromagnetic wave causing by corona plasma. The framework of the control system of UAV is:

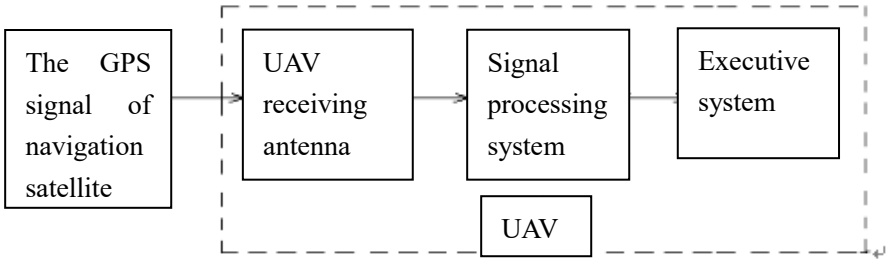


Figure 1. The framework of the control system of UAV.

Table 1. The statics of data losing of 10 flights.

Time	12:35:58	12:35:59	12:35:60	12:36:01	12:36:02	12:36:03
Nº. of valid read data	4	3	3	0	4	8
Nº. of data lost	4	5	5	8	4	0

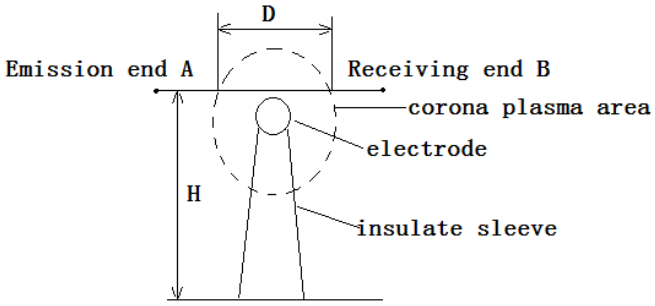


Figure 2. Emission-absorption spectrum text experiment.

After the GPS signal from navigation satellite is accepted by UAV and receiving antenna, it is sent to executive system by signal processing system and then the cruise mission in various locations is completed. Therefore the receiving of GPS signal by navigation satellite is a key point. Once this signal is lost, the UAV will not complete given cruise mission.

①Shielding of high voltage transmission line to GPS data of UAV

Made the UAV flied in a low attitude. To ensure safety, make UAV respectively fly below and above the 220kV industrial transmission line. Moreover, made the UAV flied at a vertical distance of 5m and 10m respectively with a GPS signal frequency of 1268MHz. The result was:

While flying below the line, the UAV lost control for 8 times. The GPS date in the black box showed that the data during the losing-control period was lost. The part of the data when the UAV flied below the lines from 12:35:58 to 12:36:03 were shown in following form. The data were read 8 times per second in the experiment:

Meanwhile, it was also found that the time of missing data was continuous.

The out-of-control situation was not found in the experiment while flying over the lines and there was not losing of GPS data in the black box.

②Absorption of electromagnetic wave by plasma

The GPS signal comes from positioning satellite and it travels in the form of electromagnetic wave. The plasma has the effect of attenuation and phase shift on the electromagnetic wave. Therefore, through observing the incident electromagnetic wave absorption spectrum, it proves the interference and shielding of GPS signal produced by corona plasma generated by high voltage line. The experimental arrangement was like:

Electric pulses from a pulsed source were transmitted through a broadband antenna and then electromagnetic wave were transmitted, the electromagnetic wave traveled through the corona plasma generated by electrode loaded 200kV direct current high voltage, and the received signal was measured at the receiving end by the same broadband receiving antenna. Through the comparison of emission spectra and receiving spectra, the absorbing of electromagnetic wave by corona plasma was observed. In order to obtain enough wide frequency range bandwidth, the electric pulses wave in time domain is double exponential wave, the experimental principle is shown in Fig. 2.

Assume that in Fig. 2 the corona plasma area is nearly circular, keeping the Link Lines of emission-reception parallel to ground. Obviously, changing the height H between the transmitting end and the ground can change the distance D that electromagnetic wave travel in corona plasma, because it is related to the distance for electromagnetic wave attenuation when it travels through corona plasma, and if plasma have shielding and interference on the electromagnetic wave, the receiving spectrum will be different. In the experiment, the minimum height H is about 1.5m, the receiving spectrum was read when height H was raised per 15cm, Fig. 3 is the emission spectrum. The Fig. 4 to Fig. 7 are respectively the receiving spectrum when the heights are1.65m,1.8m,1.95m,and 2.1m.The same attenuator is used in various heights

It can be seen from Fig. 3 and 7 that the plasma has obvious shielding for electromagnetic wave within the frequency between 320MHz and 900MHz. Meanwhile, the receiving spectrum is obviously different at different distance.

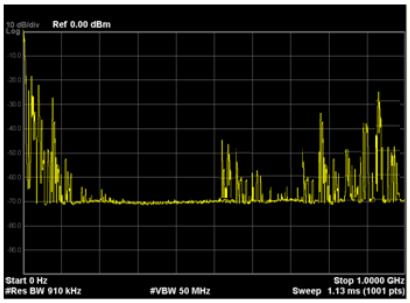


Figure 3. Emission spectrum.

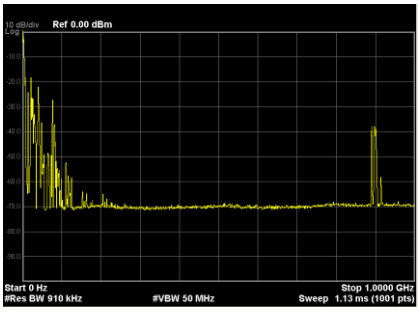


Figure 4. Receiving spectrum at H=2.1m.

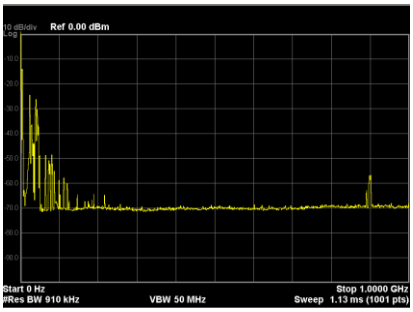


Figure 5. Receiving spectrum at H=1.95m.

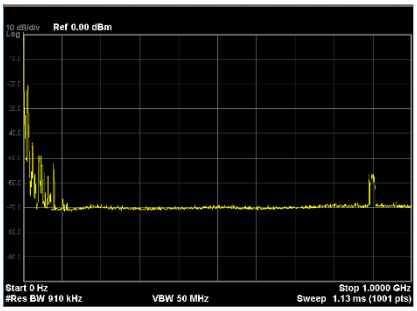


Figure 6. Receiving spectrum at H=1.8m.

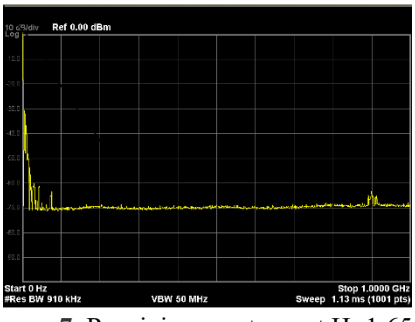


Figure 7. Receiving spectrum at H=1.65m.

B. Experimental analysis

It can be seen from the receiving experiment on GPS receiving data, the loss of receiving data happens when UAV flies below high voltage line area and there is not such situation when it flies above the high voltage line. Because the high voltage line can generate corona plasma, it proves that the loss of GPS navigation data is related to the shielding of electromagnetic waves by plasma. It is worth noting that, even when the UAV flies through the high voltage line, there is no interference of receiving data, which in turn confirms the statistical characteristics of the corona plasma fluctuations.

To explain with the experiment of emission spectrum and receiving spectrum where within the frequency scope between 320MHz and 900MHZ, the plasma has obvious interference and shielding to electromagnetic wave and the phenomenon of interference and shielding from plasma can be explained on the attenuation of electromagnetic wave and phase shift. In the formula (10) and (11), it refers to attenuation and phase shift of electromagnetic wave propagating in plasma. Due to different incident angles, the plasma has different reflection and refraction on the electromagnetic wave. So the electromagnetic wave amplitude and phase in the plasma region are different. Meanwhile, due to different atmospheric conditions, altitude and air humidity, the physical characteristics such as plasma density and equilibrium distribution are different. Therefore, it is quite difficult to get the relationship between attenuation factor, phase shift factor and the incident angle accurately. However, it proves that the shielding and interference of electromagnetic wave by corona plasma exists.

V. CONCLUSIONS

This essay discusses the conditions where high voltage lines generate corona plasma and analyzes diffusion of plasma in the electrical field of high voltage line. Through the GPS signal obtained by UAV while flying below and above the high voltage lines respectively, it finds that the loss of GPS navigation date happens when the UAV flies below the lines and not when it flies over the limes. Through the measurement and comparison of the electromagnetic wave spectrum while the electromagnetic wave traveled through the corona plasma, the shielding and interference effect of corona plasma on electromagnetic wave is observed. This proves that the signal loss of UAV navigation system is because air is ionized under high voltage environment into corona plasma, which has strong shielding effect on the GPS signal sent by satellites.

ACKNOWLEDGEMENTS

This work was supported by the National Natural Science Foundation of China (Grant Nos. 11502118).

REFERENCES

Chen, X.B., Y.L. Ma and Z.J. Xu, "Research on Transmission-lines-cruising technology with the Unmanned Aerial Vehicle", *Southern Power System Technology*, **2(6)**, 59-61 (2008).

Das, U.J., "Heat and mass transfer of Mhd visco-elastic oscillatory flow through an inclined channel with heat generation/absorption in presence of chemical reaction", *Latin American Applied Research*, **47(2)**, 47-52 (2017).

Dey, D., "Hydromagnetic oldroyd fluid flow past a flat surface with density and electrical conductivity stratification", *Latin American Applied Research*, **47(2)**, 41-45 (2017).

Liu, S.K., J.M. Fu and Y. S. Chen. "Numerical. Analysis on slot coupling effects of FREMP". *Journal of Microwaves*, **16(2),** 182-186 (2000).

Liu, X. F., Z.Y. Gan and X.W. Zhang, "Calculation of active interference in Aeronautical Radionavigation Stations caused by UHVAC Transmission Line", *Power System Technology*, **2**, (2008).

Liu, X.F., H. Yin and X. Wu, "Test and analysis on effect of high voltage transmission lines corona radio interference and scattering to GPS signal", *High Voltage Engineering*, **37(12)**, 2937-2944 (2011).

Wu, X., N. Li and G.Z. Zhang, "Limits and design control of radio interference for 1000KV AC transmission lines", *High Voltage Engineering*, **8**, 1791-1795 (2009).

Xiao, D.P., W., P. He and J. Xie, "Study on corona discharge characteristic of high voltage transmission line and calculation of its electromagnetic radiation field", *Power System Technology*, **31(21)**, 52-55 (2007).

Yin, H., X.H. Zhang and X.W. Zhang, "Interference analysis to aerial flight caused by UHV lines using airborne GPS", *Geomatics and Information Science Journal of Wuhan University*, **34(8)**, 774-777 (2009).

Zhang, Y. M., G.Z. Zhang and B.Q. Wan, "Electromagnetic environment of 1000KV AV single-circuit compact transmission lines", *High Voltage Engineering*, **37(8)**, 1888-1894 (2011).

Received: December 15th 2017
Accepted: June 30th 2018
Recommended by Guest Editor
Juan Luis García Guirao

Array 8 (2020) 100048

Contents lists available at ScienceDirect

Array

journal homepage: www.elsevier.com/journals/array/2590-0056/open-access-journal

Security challenges to smart agriculture: Current state, key issues, and future directions

Angelita Rettore de Araujo Zanella [a,b,*], Eduardo da Silva [c], Luiz Carlos Pessoa Albini [b]

[a] Catarinense Federal Institute, Rod. SC 135, Km 125, Campo Experimental, Videira, Brazil
[b] Department of Informatics, Federal University of Paraná, Rua Cel. Francisco Heráclito dos Santos, 100, Curitiba, Brazil
[c] Catarinense Federal Institute, Rod BR 280, km 27, Araquari, Brazil

ARTICLE INFO

Keywords:
Smart agriculture
Security
Open-field agriculture

ABSTRACT

Smart agriculture integrates a set of technologies, devices, protocols, and computational paradigms to improve agricultural processes. Big data, artificial intelligence, cloud, and edge computing provide capabilities and solutions to keep, store, and analyze the massive data generated by components. However, smart agriculture is still emerging and has a low level of security features. Future solutions will demand data availability and accuracy as key points to help farmers, and security is crucial to building robust and efficient systems. Since smart agriculture comprises a wide variety and quantity of resources, security addresses issues such as compatibility, constrained resources, and massive data. Conventional protection schemes used in the traditional Internet or Internet of Things may not be useful for agricultural systems, creating extra demands and opportunities. This paper aims at reviewing the state-of-the art of smart agriculture security, particularly in open-field agriculture, discussing its architecture, describing security issues, presenting the major challenges and future directions.

1. Introduction

Agriculture is the most important provider of food and plays an essential role in economic growth. The Food and Agriculture Organization of the United Nations (FAO) states that global demand for food must grow to 70% by 2050 to meet demand. While current production suffices to feed the entire world population, 500 million people still suffer from malnutrition, and over 821 million go hungry. The United Nations estimates that the world's population will increase by over 2 billion people, most living in urban areas. More than half of this increase will occur in India, Nigeria, Pakistan, the Democratic Republic of Congo, Ethiopia, the United Republic of Tanzania, Indonesia, Egypt, and the United States. Projections show India and Nigeria to account for the increase of approximately 473 million people between 2019 and 2050 [1]. This population increase represents a challenge to reach the goal of zero hunger defined in the text *Sustainable Development Goals* (SDGs) [2]. These expectations for the coming years influence the global demand for food. It may be difficult to meet 40% of water demands by 2030, and the degradation of 20% of arable land will reduce food supply. Therefore, food production requires more resources than currently available and more sustainable systems to increase cultivation rates and reduce the use of natural resources [3].

Annual cereal production must increase by 3 billion tons, and meat production has to grow over 200% by 2050 to meet the demand [4]. Cereal supplies will depend on the increase in yields. This increase requires the improvement of cultivation practices, structural changes towards larger farms, and the ability to adapt technologies [5]. Although it may be possible to meet the growing demand, it is not clear how to achieve it sustainably and inclusively. Then, there is a crucial need to streamline the farming system transformation at extraordinary speed and scale-up [4]. At the same time, the *Fourth Industrial Revolution* (Industry 4.0) and the *Internet of Things* (IoT) provide new technologies and innovations. These new technologies and innovations applied in agriculture are called *smart agriculture*, *smart farming*, or *Agriculture 4.0*. These terms are used interchangeably throughout this paper. Agriculture 4.0 can provide information on improving plantation productivity without increasing the crop area, optimizing irrigation processes by consuming less water and energy, or providing resources to control pests more efficiently, for example. These will be possible by integrating technologies for environmental measurements, prediction, and automation tools. New capabilities created by smart farming can optimize agricultural processes, allowing production to escalate while using fewer natural

* Corresponding author. Catarinense Federal Institute, Rod. SC 135, Km 125, Campo Experimental, Videira, Brazil.
E-mail addresses: angelita.zanella@ifc.edu.br, gelirettore@gmail.com (A. Rettore de Araujo Zanella), eduardo.silva@ifc.edu.br (E. da Silva), albini@inf.ufpr.br (L.C. Pessoa Albini).

https://doi.org/10.1016/j.array.2020.100048
Received 22 July 2020; Received in revised form 13 October 2020; Accepted 16 October 2020
Available online 21 November 2020

resources.

Smart farming combines different technologies, devices, protocols, and computing paradigms to enable the farmers to make the most out of innovations. Innovations in agriculture are called the "*digital agricultural revolution*'' and will transform all aspects of agriculture, resulting in more productive, efficient, sustainable, inclusive, transparent, and resilient systems. Nevertheless, integrating technologies into the agricultural sector depends on the complexity and maturity of technologies such as mobile devices, precision agriculture, remote sensing, big data, cloud, analytics, cybersecurity, and intelligent systems [4]. Although there are several security issues related to the smart farming, such as compatibility, heterogeneity, constrained devices, processing, and protection of massive data, few resources have been incorporated in Agriculture 4.0 so far. Therefore, this paper addresses the security challenges in these systems.

To build robust and efficient systems, Agriculture 4.0 must ensure (i) the correct and complete generation, transfer, and processing of data, and (ii) that the system has adequate security features to prevent attacks. Data integrity is essential to enable the proper operation of data-driven technologies, such as analytics and smart systems. Malfunctioning hardware or attacks, whether directed to the system or using the system as an intermediary for external attacks, can put security at risk. Heterogeneity of resources raises a lot of security concerns, such as keeping privacy, maintaining trust and reliability, which can be crucial to meet the demand and potential of emerging applications [6,7].

Since smart agriculture integrates elements from the traditional Internet, IoT, cellular, and wireless networks, it may incorporate all security problems these technologies present. It also deals with new special security issues such as data and device integrity, data accuracy, and availability. In smart farming, the devices (sensors and actuators) and communication systems are exposed to climatic fluctuations (sun, rain, snow), natural events (lightning, hail), engines (used in agriculture), power line transmissions (common in some rural regions), wandering animals, people and agricultural machinery. These elements make smart farming vulnerable to problems that have not been addressed in other contexts so far.

For instance, smart agriculture has devices installed in open areas and exposed to external agents such as animals, humans, or agricultural machinery. These agents can unintentionally remove the sensor from the original location or damage them. Most times, the devices cannot use protection boxes to prevent these external agents from approaching as in other scenarios, such as in smart cities. The lack of protection leaves devices vulnerable to security incidents and reveals a distinctive feature concerning applications in agricultural systems.

Another threat is *agroterrorism*, which has been around since the 6^{th} century B.C [8]. This type of terrorism can have several objectives, such as causing financial damage, fear, and social instability [9,10]. Through crises in agriculture and the food industry, terrorists can stimulate social unrest and loss of trust in government, which can serve a variety of interests in the globalized world. For example, terrorists and governments in trade disputes may want to cause economic damage to a nation, economic opportunists may attempt to manipulate markets, and unbalanced or disgruntled people may commit attacks with idiosyncratic or narcissistic motivations [8]. New technologies, such as smart agriculture, can contribute to the evolution of agroterrorism, creating *cyberagroterrorism*. It might use computer systems in agricultural environments to damage crops, livestock, and generate financial losses. Cyberagroterrorists can act both locally, on farms, and online, operating the attacks through cyber resources.

This article presents special security issues in Agriculture 4.0. The aim is to highlight the main solutions in this area and discuss security threats. Section 2 reviews smart agriculture and the architecture used by most systems. Section 3 outlines the major security threats from a layered perspective. Section 4 summarizes the current state of intelligent agriculture applications. The last section presents the key challenges in this area and points to future directions.

2. Smart agriculture overview

Agriculture has undergone several revolutions, which improved the sector's efficiency and profitability. The plant domestication (10,000 BC) led to the world's first societies and civilization. In recent centuries, agricultural mechanization (between 1900 and 1930) introduced machines and implements to mechanize work, increasing farmworker's productivity. The Green Revolution (about the 1960s) enabled farmers to use new crop varieties and agrochemicals. In the late 20^{th} century and early 21^{st} century (from 1990 to 2005), biotechnology allowed the creation of plants with pre-selected traits, such as increased yield and resistance to pests, drought, and herbicide. Now, the digital revolution could help humanity to survive and thrive long into the future [4]. Fig. 1 presents an overview of major agricultural revolutions, that preceded the digital revolution.

The first steps toward the digital revolution focused on automation techniques, including few computational functionalities [11,12]. Next, smart agricultural systems had sensors to collect climate or environmental data. Sensors connect to a constrained border device, named gateway, linked to a local computer through a network connection, frequently wireless. The local computer receives data from the gateway, stores it in a database, and shows processed information on a web page. Local systems did not integrate with external systems or the Internet.

In recent years, the scenario has changed, with researches in artificial intelligence and machine learning focusing on agricultural contexts, irrigation, animals, and farms. In the irrigation field, monitoring, controlling, and decision-making solutions attempted to save water and improve production [13–18]. Some studies focus on hydroponic [19], horticulture [20], vineyards [21] and leaf disease detection [22]. General-purpose systems [23–25], just implement IoT technologies and resources or design web-services [26], alert services [27], traceability resources [28] and control on the cloud [12]. Although there are several solutions in Agriculture 4.0, they are still immature and provide a low level of intelligence. Many of these proposals are automation-restricted, with sensors and actuators sending data to the gateway. In most cases, there is no integration with the Internet, though in a few cases, local systems store data in the cloud.

The above systems have been built up in architecture (see Fig. 2) that consists of perception layer devices, network layer capabilities, edge resources, and cloud-based applications and services [29,30]. The perception layer includes sensors, GPS, tags RFID, cameras, actuators, and any other devices responsible for collecting data from the farm environment and acting to modify them. These devices do not have the computational capacity to process or store data and perform at the edge or the cloud. This layer connects to edge resources via network technologies, which is usually a Wireless Sensor Network (WSN).

The edge layer may contain a variety of resources such as security features, data filters, decision-making capability, diversified processing, in-out interface, and the gateway. Including one or more resources at the edge depends on the features of the appliance. Some appliances support only the retransmission of data, while others have the computational capability to perform more tasks. More robust gateways can process data, make decisions, send commands to actuators and data to the cloud. The Internet Service Provider (ISP) connects the gateway to the cloud. The cloud processes and stores data to provide end-users with information and services. Data processing is a challenge, considering a large mass of data produced by the perception devices reaching the Big Data world, and the financial cost of processing in the cloud.

Processing everything in the cloud, as proposed by many solutions, implies enormous bandwidth requirements and high financing costs. It can be advantageous to use a robust gateway and perform part of the processing at the edge. Moving part of the subsystems to the edge may reduce the financial costs of smart farming. Data consumed or preprocessed at the edge saves bandwidth and can reduce the computing resources required from the cloud, protects privacy, and preserves the battery life of some devices. Thus, the cloud could store and process

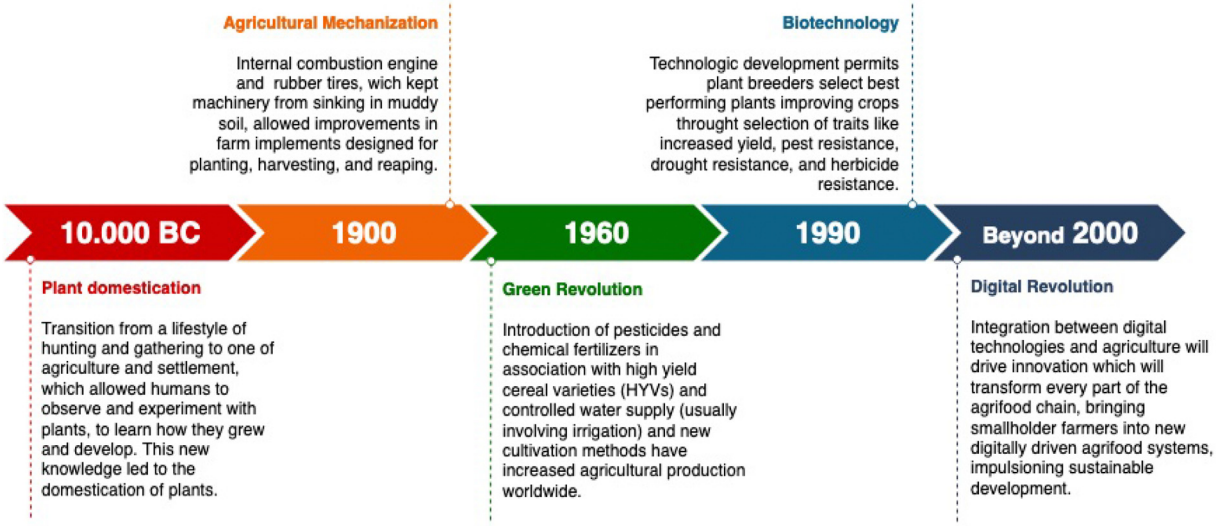


Fig. 1. Agricultural revolutions.

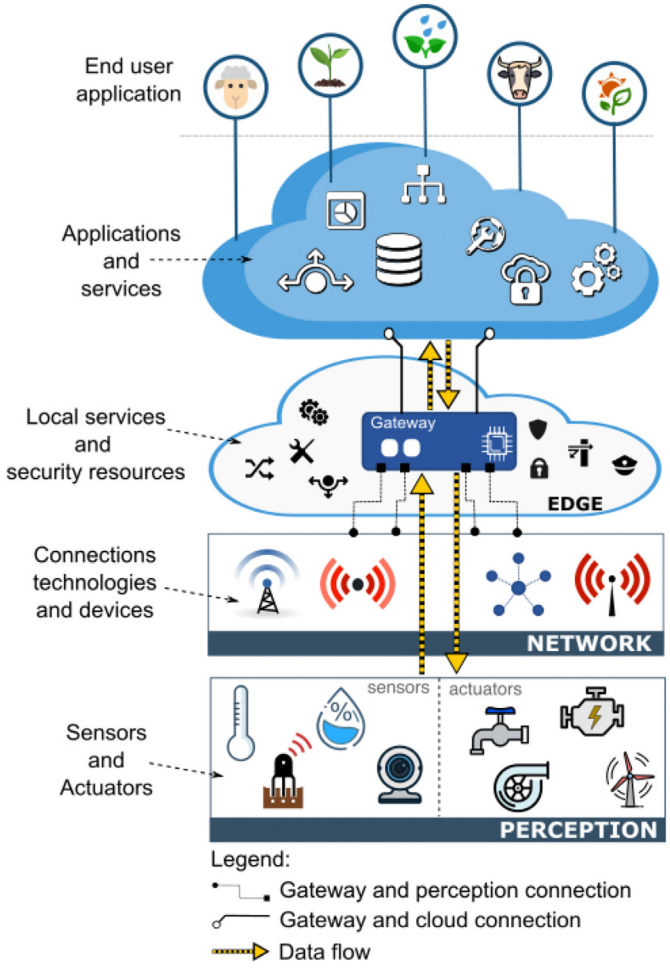


Fig. 2. Structure of smart agriculture components.

massive data, make decisions, and interact with the user. Processing big data to make decisions at the edge may require tools like artificial intelligence.

The improvement of devices and communication technologies will make it possible for more computational resources to be integrated into systems. Such integration aims at meeting different demands of agricultural automation, farm management, and precision farming [12,30]. Solutions must evolve to management systems rather than just monitoring, which can result in new challenges and possibilities. Another issue is the security of data. From the detection up to the storage and decision-making in the cloud, it is mandatory to provide data privacy, reliability, and accuracy. Security issues in smart farming are a great challenge and will be detailed in section 3.

3. Smart agriculture security threats

As discussed in Section 2, smart systems have four layers: (*i*) perception layer; (*ii*) network layer; (*iii*) edge; (*iv*) application. Table 1 shows the resources responsible for collecting, transporting, processing, and storing data at each layer. The set of devices, protocols, and technologies use the data to monitor environments and automate farming activities [29]. Storage, management, and data processing combined with Internet connectivity bring several issues and security threats. Fig. 3 summarizes attacks on smart agriculture in the layered perspective.

Security incidents may be accidental or intentional. Animals, farm working, and machinery can easily access farming environments and cause incidents. Additionally, smart systems comprise heterogeneous devices and software from distinct manufacturers installed between growth areas and the cloud. These specific features might make several security breaches and could result in incidents that compromise the smart system. Nevertheless, this topic has not been studied in most systems in use so far.

The system design should consider compatibility with distinct devices, protocols, subsystems, and multi-access methods. Smart Agriculture uses *machine-to-machine* (M2M) communication and devices manufactured by different vendors. However, most security mechanisms were developed for the communication model used by TCP/IP networks. These mechanisms usually ignore the existence of multiple heterogeneous devices communicating simultaneously. Security features created for TCP/IP networks can divide the relationship between smart farming devices, reducing their efficiency. Multi-access methods and heterogeneity hinder security, interoperability, and network coordination, increasing security vulnerabilities [31].

Agriculture 4.0 is exposed to a vast spectrum of cyberattacks. Security concern needs to be part of the system, maximizing their potential. Among these issues, there is also access control, management, information storage, data integrity, and reliability. Most of the security problems are quite common in other systems, but some are present only in those

Table 1
Smart agriculture elements.

Layer	Resource	Description
Perception	Sensor and Camera	Small devices to collecting environment data, such as humidity and temperature.
	Actuator	Devices or systems for changing the environment state. Example: sprinkler, ventilation, and irrigation systems.
	Tag RFID	Small devices to storing data, such as livestock identification number.
	GPS	A System that provides geolocation of agricultural machinery, farm resources and may assist precision farming system.
Network	Connection Technologies	Devices and technologies to interconnecting remote devices and transferring data. Example: router, access points, protocols.
Edge	Security features	Security protocols and schemes for ensuring the availability, integrity, and confidentiality of the system and data.
	In-out interface	Software and hardware interface for communication beyond the local area.
	Diverse resources	Software features applied to decision-making, processing data and so on.
	Gateway	System located at the edge of the network, connected with farm devices (perception layer) and the cloud. This system can process data, store small amount of data and communicate with the cloud.
Application	Database	System for storing data produced by the smart system.
	Web tools	Resources for exchanging data between the remote application and provide access to the end-user application on the Internet.
	Decision-making	System to making-decisions to change the state of the environment.
	End-user application	Software for presenting information to the user.

that operate in open-field systems, such as smart agriculture. Although privacy is unnecessary in most contexts, others might require it. This work addresses all security requirements regardless of the context. Therefore, the developer must select the features related to each system. Here we introduce some of the current security issues in Agriculture 4.0, describing the most relevant threats in each layer separately.

3.1. Security issues at perception layer

The perception layer mainly deals with physical devices, such as sensors and actuators. They can be installed in small farm areas, such as those found in Europe, or scattered along with large farms, current in the USA, Australia, and Brazil. Physical devices may malfunction because of accidental or intentional human action, viruses, malware, or cybercriminals. There are many kinds of sensors and technologies used by smart farming applications, and this variety enables several security threats just as follow:

Random sensor incidents - It is the unintentional physical modification of a perception device that diverts it from the regular operation. Smart systems developed for small or large farms may have devices installed outdoors. In many cases, these devices do not have tamper-resistant boxes, as this would make it expensive. The lack of tamper-resistant boxes exposes the device to interactions with external agents such as people, animals, or agricultural equipment. A farmworker or wild animal may accidently collide with a sensor, moving or removing the device from its original location, violating system integrity. Farm equipment, such as a tractor, may hit the device causing temporary or permanent physical damage, leading to data corruption, data unavailability, or damage to the device. This threat is not exclusive to smart farming but may be present in other contexts, such as smart cities. However, it is a relevant issue because it can have a deep impact on the reliability of the solution. In most cases, there is no way to avoid this threat, though it is necessary to identify it to avoid its effects.

Autonomous system hijacking - It consists in hijacking autonomous systems such as tractors, drones/UAV, and sowing robots. Several farming activities use autonomous systems, such as drones and robots. Drones could spray pesticides and fertilizers, and robots may perform weeding and disease detection. If a malicious agent hijacks an autonomous system, the hijacker can remotely control and guide without authorization. This type of attack could have several impacts, from the unavailability of the system to perform a task to its complete damage or crop damage.

Autonomous system disruption - It is an intentional modification of autonomous system resources. Autonomous tractors, robots, and UAV (Unmanned Aerial Vehicles) are technologies increasingly present in precision agriculture, especially in large farms. These equipment have a series of features that are essential to their operation, such as sensors, cameras, GPS, maps, and remote-control systems. If an opponent modifies one or more components, the autonomous system may work improperly or suffer/cause accidents. Malfunctions could result in severe losses, resulting from incorrect soil or crop management, damage to crops, buildings, equipment, and machinery, including the autonomous tractor itself.

Optical deformation - It is the deformation of images from cameras installed in robots or autonomous devices. Some autonomous systems have cameras to capture images. The cameras usually have an essential function in the system, and the captured images should have a minimum quality. Cameras are usually vital to the system. Pictures must meet a minimum quality standard in order to ensure the whole process to run smoothly. Below standard pictures may mislead the harvesting system into picking spoiled or unripe fruit or even damaging the fruit trees.

Irregular measurement - It consists of abnormal measurements or readings caused by data corruption, energy depletion, electromagnetic

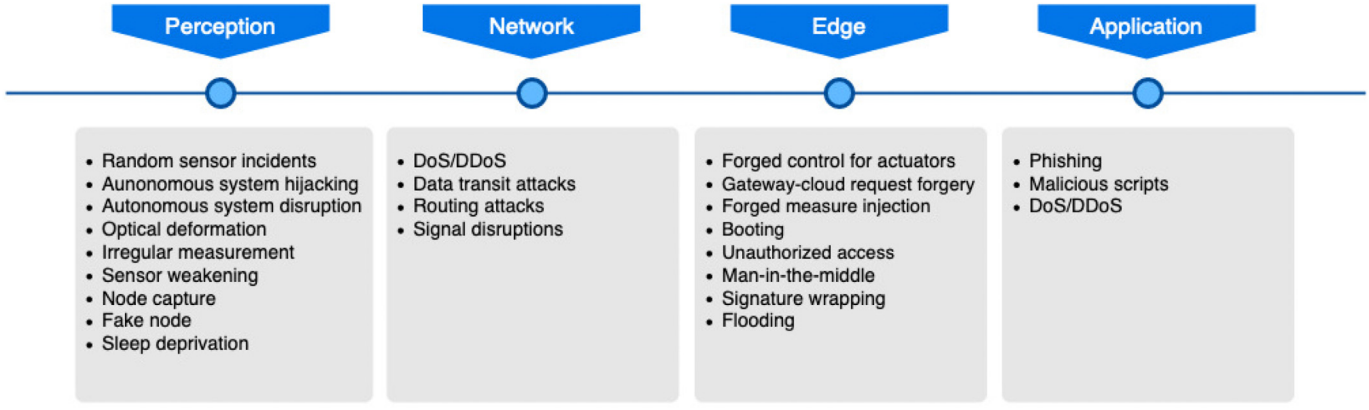


Fig. 3. Smart agriculture main attacks.

interference, interception of variable connectivity, severe weather, malfunctions, or false inputs. In some regions, usually in large farms, high-voltage grids pass over agricultural areas and can generate an electromagnetic field, causing distortions or data corruption. Power depletion of battery-powered devices, variable connectivity, or malfunctioning of some device components can cause irregular readings, compromising data availability or integrity, which results in inaccurate data. Inaccurate data can be dangerous for decision making, resulting in incorrect data analysis, and reducing system's accuracy.

Sensor weakening - This is the normal degeneration of sensors because of processes such as corrosion, oxidation, dust accumulation, and saturation. Some sensors used in smart farms can suffer gradual degradation for exposure to environmental conditions and physical-chemical or climatic phenomena. For example, wind speed sensors installed in dusty environments can suffer from dust accumulation, which gradually prevents the rods from moving. Humidity sensors can saturate when exposed to high humidity levels. Sensors built with copper may suffer oxidation. This way, the sensors register incorrect or irregular measurements. The natural degradation of the sensors requires their periodic replacement. However, some events may expect device degradation, causing failures earlier than expected. It is still not possible to avoid the natural degradation of the sensors. However, it is necessary to detect sensor weakening, to prevent the use of inaccurate data by the system.

Traditional network and IoT attacks can affect the security of smart farming applications, for example:

Node capture - It consists of the physical capture of a node or device. This operation could be performed by entirely replacing the device or modifying components of hardware or software [32,33]. Node capture may not generate a significant impact if performed on a single node and might not trigger other attacks. However, after capturing a device, the opponent may modify the hardware or software, gain access to the system, or inject false data. A node capture breaches the integrity of the system and can potentially interfere with decision-making. It might also damage the cultivation and cause financial loss. For example, a hostile actuator in an irrigation system could never start irrigation or flood the crop. A dissatisfied employee or commercial competitor who has physical or logical access to the system could perform this attack for several reasons.

Fake node - An adversary adds fake or malicious nodes to the system to disrupt their operation [31]. A node capture could trigger this attack and lead to node replication. This kind of attack usually aims at both to manipulate data or to shutdown services and devices. In a system with insufficient or fraudulent identity control, malicious sensors could send wrong data interfering with decision-making, or inject multiple packets into the network causing a denial of service, or sleep deprivation. Likewise, actuators may act maliciously, hostile gateways may send false commands to legitimate actuators, or act as black holes to cause harm.

Sleep deprivation - This attack aims to drain the battery of the device until depleting it. Smart farming sensors are energy-restricted and usually use power batteries. To reduce the power consumption and prolong battery life, the nodes should enter in sleep mode when they are not working [34,35]. Sleep deprivation attack sends sets of apparently legitimate requests so that the devices remain awake as long as possible. Therefore, the battery of the device will deplete, and the node shuts down [34,35]. Once the sensors turn off, sensed data is no longer sent, compromising decision-making, and system efficiency.

Since Agriculture 4.0 systems are open-field, they are susceptible to environmental conditions, climate fluctuations, and human action. Weak security measures could affect the reliability and trust of the system, exposing them to accidental use of corrupted data, remote control, and physical damage. Sensors do not have computational resources that allow the adoption of traditional security methods, such as cryptography, which makes security even more challenging. Therefore, adding innovative security solutions to this layer is as challenging, as necessary.

3.2. Security issues at network layer

The network layer transmits data from the perception layer to the most robust computational unit, usually the cloud. The transmission of a large amount of data over a wide transmission area makes this layer susceptible to attacks, which generally threaten confidentiality and integrity [36]. Although the existing communication network has relatively complete security protection measures, there are still some common threats that can compromise network resources [31,37]. Major security issues in the network layer are as follow:

DoS/DDoS - It is a transversal attack that affects all layers. Denial of Service (DoS) aims to prevent access to services or devices either by overloading the network or by exploiting protocol vulnerabilities that lead to the collapse of resources, such as CPU and memory [38]. There are several ways to achieve this attack, such as flooding servers or routers with numerous requests. Flooding attacks can cause network delays, disable devices, and make the service unavailable. When the attacker uses multiple sources to flood the target, then such an attack is termed as a Distributed Denial of Service attack (DDoS). Although such attacks were not designed specifically for smart systems, Internet connectivity, pervasiveness, heterogeneity, and high vulnerability of these systems make them prone to such attacks [39]. In farming systems, DoS attacks could prevent measurements from reaching the edge or cloud on time, delay commands to actuators, and make services unavailable.

Data Transit Attacks - Some attacks intend to intercept data exchanged between network components to find sensitive information [7]. Different connection technologies connecting distinct points on the network and wireless networking carrying clear (unencrypted) data make these systems susceptible to data breaches [7,40]. An opponent could conduct traffic interception through malicious access points or by man-in-the-middle attacks [40]. Traffic interception exposes sensitive information such as unique identifiers, access credentials, or cryptographic keys. Other transit attacks can corrupt network traffic, enabling malicious control, or even compromising the entire system.

Routing Attacks - They intend to alter network routes to achieve control of traffic. IoT networks may have malicious nodes that try to redirect routing paths during the data transmission process. Attacks such as sinkhole and wormhole could subvert the communication network and get unauthorized access. The sinkhole is routing attacks where a rival announces a shorter routing path and draws nodes to route traffic through it. Malicious routes allow disrupting the traffic flow [7,41]. In a wormhole, an opponent creates a tunnel between two nodes for fast packet transferring to create a shortcut on the network and control traffic [7,42]. During these attacks, the recipient may receive the information late, receive partial or changed information, or not receive one data [41,42].

Network layer resources on smart farming and IoT systems have some common security vulnerabilities. However, smart farming can consist of multiple systems and integrate technologies and subsystems from different vendors. Therefore, integrating systems and technologies requires caution to avoid incompatibilities. Likewise, the security features of these systems and technologies cannot be fully trusted, as they may contain vulnerabilities embedded in the system or generated by the integration process.

3.3. Security issues at edge

The edge contains critical elements monitoring and controlling subsystems, communicating with all layers, and accessing strategic resources. The processing of massive amounts of data generated by perception layer can be local, instead of centralized in the cloud. This would save energy, bandwidth and cloud-processing costs. Due to the distributed architecture of edge computing, this layer might provide services with faster response and higher quality, in contrast with cloud

computing [33]. Direct connection to cloud and perception resources make the edge a strategic point, making security a fundamental requirement to ensure system reliability. Major edge security issues are the following.

Forged controls for actuators - It is the injection of false measures/data to manipulate the system. The perception devices are usually resource constrained and do not support complex security features. Typically, the gateway receives the data in plain text. The gateway may receive data from the perception or cloud by Supervisory Control and Data Acquisition (SCADA) systems or other control systems. An opponent who knows the data patterns sent by the sensors to the gateway or cloud can use a computational device to inject the same data pattern into the system. If the control system receiving the data at the gateway does not have sufficient security mechanisms, the data will be accepted and may propagate through the system. False data will cause incorrect decision making. For example, to manipulate a smart irrigation system, an opponent could inject incorrect soil moisture measurements.

Gateway-cloud request forgery - Gateway and cloud are connected through an Internet Service Provider or cellular network. Usually, the cloud is connected to the Internet and therefore exposed to a wide variety of attacks. An Internet adversary could impersonate a gateway and forge requests for the cloud. From these requests, the adversary could modify parameters in smart farming, control requests for vulnerable services, or manipulate system resources. The gateway is usually a constrained resource, but the cloud has the computational capability to incorporate robust security mechanisms. These mechanisms must be incorporated into the system to maximize system reliability.

Forged measure injection - It consists of the injection of false measurements/readings to manipulate the system. Perception devices generally are resource-constrained and do not support complex security features. In general, data exchange with the gateway is done in plain text, creating several vulnerabilities. An opponent who knows the patterns of data sent by sensors to the gateway or the cloud can use a computational device to inject the same data pattern into the system. Sending false data could result in wrong decision-making. For instance, to manipulate an intelligent irrigation system, an opponent may inject incorrect soil moisture measurements.

Booting - IoT evolution has driven the development of low-cost and resource-constrained devices. These devices are becoming smaller and cheaper. However, innovations do not advance into the field of security [43]. Smart agriculture uses resource-constrained artifacts in the perception and edge layers. Usually, these artifacts have few security features and rarely include boot protection. Lack of security processes on booting, leaving devices vulnerable to attacks [44]. For instance, SD-cards and USB sticks may contain malicious scripts that could run at startup [43]. Malicious boot processes could trigger a series of attacks to the edge with weak protection. Those processes could open back doors or allow elevation of privileges. Insufficient computing resources and direct connection to perception and the cloud make it imperative to protect the start-up process.

Unauthorized access - Authentication and access control are crucial elements of security. Access control is a technology that satisfies properties such as confidentiality, integrity, and availability [45]. Providing adequate access control to the edge elements is essential as these can usually communicate with perception and the cloud. In particular, the gateway is a critical element as all data pass through it. Limited or insufficient authentication and access control mechanisms allow an opponent to access the gateway by cloud connection. For the large number of things communicating with edge devices or services, authentication methods need to be scalable, easily manageable, and requiring minimal human intervention [33,45]. However, several agricultural systems use gateways with weak or insufficient access controls. Researchers developing projects to smart agriculture do not discuss the use of access control resources, and existing commercial solutions rarely change the credentials after deployment.

Man-in-the-middle - In this attack, an opponent intercepts a communication to collect information or even replace it. Compromised devices or malicious nodes can trigger several internal or external attacks in systems with weak or missing security [46,47]. Many solutions use communication protocols that use the publish-subscribe model with a broker, which effectively acts as a proxy. These protocols allow decoupling the publishing and subscribing clients from each other, authorizing messages to be sent to an unknown destination. An attacker who achieves the broker control and becomes a man-in-the-middle may obtain full control of communication without being noticed by the clients [7].

Signature wrapping - This attack modifies the original message by injecting a fake element to perform an arbitrary Web Service request while authenticating yourself as a legitimate user [48]. Web services for edge to cloud communication usually use XML signatures. An adversary, who breaks the signature algorithm, can perform operations or change the heard message by exploiting protocol vulnerabilities, such as the step [7]. An opponent may control the actuators or manipulate the decision-making systems by using malicious messages.

Flooding - This is a DDoS attack where many packets are sent to a system or network to overload it. In farming systems, infected devices could start a flood attack toward the edge devices to compromise the Quality-of-Service (QoS) or even to stop it. A hostile device at the perception layer or a malicious portal in the cloud could send multiple requests to service until their exhaustion. These attacks could impact severely on the systems, overloading the edge and resulting in a denial of service. Flooding could also be performed at the network layer and in the cloud [6,7].

Edge resources provide computing services for clients or applications and can connect to distinct features from all layers. Both locally and externally processed data pass-through this layer. Protecting devices from remote access and using appropriate cryptographic resources are key security challenges. Therefore, it is imperative to achieve security features to avoid compromising data and edge resources.

3.4. Security issues at application layer

The application layer aims at providing services to end-users, storing data, and making decisions within the system. Security issues in this layer focus on preventing data theft and ensuring privacy and are specific to different applications. Some applications comprise a sub-layer, which supports services, and helps intelligent resource allocation [7,33]. Each application has distinct characteristics, and it is impossible to predict all vulnerabilities which could affect them. Therefore, the security issues listed below are some threats that might affect cloud-based applications and services.

Phishing - It is a virtual pest that aims to fraudulently obtain confidential user data, such as ID and password. Phishing usually achieves end-user from fraudulent emails or websites [49,50]. An opponent who accesses the system with administrative credentials may send fraudulent commands to actuators and change system settings. In critical cases, the attacker could interfere with decision-making processes or other internal processes. It is impossible to avoid this type of attack, but secure access control systems can mitigate it. However, the most efficient protection would be to have the users themselves keep vigilant while surfing the net [33].

Malicious scripts - The connectivity of agricultural solutions to the Internet allows them to interact with other online services and users. This interaction makes them targets for malicious scripts such as Java applets, Active-X scripts, and cross-site scripting (XSS) [33,36]. Malicious scripts can mislead customers, inject malicious information, access sensitive information, and break security mechanisms. Cybercriminals often make this attack by personal, financial, and political ends. From malicious scripts, they can damage or disrupt the service operation, displaying unwanted advertisements, and extorting money [51].

Denial of Services - This attack causes service interruptions by overloading the network traffic or by flooding the service with multiple requests [52]. Weak security configurations enable an adversary to start

this attack from the Internet or a subsystem [7]. Such attacks deprive legitimate users of using the services, prevent the proper processing or storage of non-persistent information, reduce the efficiency of critical systems (such as environmental controls in mushroom greenhouses), and may even cause a complete system shutdown.

The application layer includes cloud-based applications and services, so it has all cloud security issues. The cloud exposes applications and resources to Internet-based attacks becoming urgent to take preventive security measures. Usually, security focuses on privacy and access control to protect the many sensitive data stored and processed in the cloud. However, it is essential to consider more than just privacy and access control, adopting security measures to ensure the availability and integrity of the complete system.

Smart farming systems incorporate a set of devices, with greater or lesser levels of limitations, that interact with each other. Many weak points are because of the constraints of the devices, which make it impossible to use existing tools and security techniques. Technologies developed for other systems, such as IoT or Industry 4.0, support security, but using them requires processing and memory resources that some devices do not have. However, it is necessary to know the existing vulnerabilities and create mechanisms to mitigate the effects of incidents. Then, security measures can be done at the highest layers and on devices equipped with the necessary resources. Top-layer appliances with robust computing capabilities could adopt more robust security mechanisms to ensure efficient and reliable operation.

4. Current state of security in smart agriculture

In the past few years, there has been a growing effort to develop smart systems to improve agricultural activity. Farmers usually conduct these activities in open-field or greenhouses. This work focuses on open-field agriculture, as it is an immature area with security features limited to access control and web encryption. Therefore, it analyzes smart agriculture projects and explores information on the security features implemented by them.

In this scope, most efforts focus on irrigation processes, disease detection, crop management, and traceability. The control may be automatic or manual. In both cases, the system uses sensors for monitoring and actuators for changing the environment. The decision about actuators' actions may be made automatically by the system or manually by a user. Some projects only automate the farms, while others integrate industry 4.0 or IoT technologies.

It is relevant to show that most current smart agriculture projects are based on IoT technologies and may direct inherit its security flaws. Others do not consider security at all. Protocols such as MQTT and CoAP disable security features by default, and the developer must enable them according to the requirements of each project. Since researchers do not report security features enablement, they probably remain disabled. Table 2 presents a taxonomy of current smart agriculture security resources.

The paper of [13] presents a system to predict irrigation requirements based on climate and environmental information. The system uses data collected by sensors to predict soil moisture and provides irrigation suggestions. End-user interacts with the system from a web page. The authors do not show any security features, validation processes, or failure checks in the collecting, transferring, or storing phases. The lack of security makes systems vulnerable to all attacks presented in Section 3, i.e., the system is highly insecure. Incidents leading to corruption or inaccuracy of data result in prediction errors and wrong decisions. Wrong decisions can damage the cultivation and reduce the adoption of the system.

Similarly [17], develops a system to monitor fields through soil moisture, temperature, humidity, and light levels. Irrigation control can be manual or automatic through the web or mobile applications. The system description does not contain information on any security features, which exposes the system to the full range of attacks presented in the previous section. Control of actuators driven by commands from a web system without strict security features is an excellent opportunity for malicious opponents, who may use malicious scripts and unauthorized access to manipulate the system.

[18] propose a smart irrigation system to control irrigation devices. These devices are remotely controlled by a server and managed from a web application. There are no details about security resources, creating the chance for opportunistic adversaries to gain improper access to the system, inject forged measures, forge controls for actuators, or conduct any previously reported attacks to deviate the system from its regular operation.

[19] introduce a Hydroponic Farming Ecosystem (HFE) to monitor the growing environment. The control is automatic, and the user may use a web interface to monitor the farming. Automated systems require rigorous protection to avoid or detect random sensor incidents, sensor weakening, false data injection, and other threats that could corrupt data and disturb the system's reliability. However, HFE fails to provide mechanisms to avoid the threats introduced in Section 3.

[22] have designed an intelligent solution for the detection of leaf diseases. The system identifies leaf diseases based on data of sensors and images from cameras. The end-user interacts with the system by a mobile or web application. This paper does not discuss the implementation details or security. If this system is part of a disease control process and receives corrupted or malicious data, the images suffer optical deformation, or an opponent compromises system, then security incidents can hinder disease detection and cause misuse of agricultural resources. In critical cases, this may cause loss of the entire production.

[28] introduces NETPIE, a system that provides information about agricultural products. Using a set of perception devices, NETPIE controls and monitors the growing environment. The production information is summarized and saved in a QR code and available to the customer. Just like the other presented systems, NETPIE does not discuss security resources. Any of the attacks that disrupts data accuracy may break the reliability of the information summarized in the QR code.

[12] present a cloud-based Wireless Sensor and Actuator Network (WSAN) communication system to monitor and control farm devices. The system monitors environmental conditions, predicts the irrigation requirements, and acts automatically on the environment. The paper describes the system architecture, including appliances and protocols, allowing the WSAN to remain vulnerable to the attacks shown in Section 3.

Table 2
Taxonomy of security in smart agriculture.

Security target	Security Resources	Solutions
Not considered	None	Sales et al. [12], Goap et al. [13], Mahalakshmi [14], Rajalakshmi and Mahalakshmi [17], Zhao et al. [18], Ruengittinun et al. [19], Thorat et al. [22], Yoon et al. [23], Wongpatikaseree et al. [28]
Data Exchange	HTTPS	Khelifa et al. [11], Minh et al. [25]
Access Control	IP Authentication	Nageswara Rao and Sridhar [15]
	User and Device Management	Oliver et al. [21]

Likewise [23], propose a smart farming system for data exchange between the server, the gateway, and the nodes. The paper describes the construction of the system but does not mention any user interaction or remote control and does not demonstrate any security concerns. Because it is a system for data exchange, the most critical attacks are those that affect the network layer, such as DoS, signal disruption, data transit, and routing.

Similarly [14], introduces an automated irrigation system. The paper presents the step-by-step construction of the system, which monitors and controls water flow remotely. Although the system controls and monitors irrigation devices, there is no evidence of the addition of security capabilities. Attacks on the perception layer, as well as attacks that cause a denial of service, can damage correct system operation. Unauthorized access, malicious scripts, and false data injection can deliberately manipulate the system.

On the other hand, some solutions add a small level of security. The [11] strategy, for instance, includes encryption in the communication between cloud and user applications. This proposal intends to create a smart irrigation system controlled remotely by the user. Farmers manage the irrigation process from a mobile application. This strategy uses HTTPS to encrypt the communication between the server and smartphone. The use of cryptography protects data in transit, preventing an adversary from intercepting the communication, obtaining sensitive information, and impersonating the mobile application. However, there is no information about other security features deployed by the system, which exposes the system to other previously presented attacks.

Another proposal that uses HTTPS is that of [25], which has developed an intelligent system to manage and control mushroom and hybrid maize farms. This system automatically controls the production environments remotely. The webserver uses HTTPS for user communication, protecting data in transit. However, this security feature is insufficient, considering that the system automatically controls the water pumps, light levels, and fans. Automated controls, especially for environmental control systems for crops as sensitive as mushrooms, demands accurate security features to avoid that Random Sensor Incident, Irregular Measurement, and Sensor Weakening, Forged Measure Injection, or Forged Controls for Actuators affect the system accuracy.

On the other hand [21], introduce a system called SEnviro. This system is designed to remotely monitor vineyards and predicts some diseases. The paper presents the developed platform and does not discuss prediction. The system includes a user and device manager, which permits to manage authorized users and devices to interact with the system. Access control prevents unauthorized devices or users from gaining access to the system and acting maliciously. Nevertheless, this resource is insufficient to protect a platform designed to predict disease and remotely monitor, as it does not prevent events that could interfere with the accuracy of the data or that could take the system to an unreliable state.

In the same way [15], proposes a remote crop-field and automatic irritation monitoring system using IoT technologies. The system uses collected data from sensors to estimate the quantity of water required for irrigation. The system uses measurement data to estimate the volume of water for irrigation. As well as the access control presented by Ref. [21], the authentication scheme used by Ref. [15] avoids unauthorized access to the service but does not protect the edge and other subsystems. Weak protection of automatic control systems is critical, as incidents that affect data accuracy or cause system malfunctions can result in significant losses to the plantation.

Summarizing the related papers, from a security perspective, they use sensors and actuators without any security features. Besides, there is no security information on the gateway. Systems developed so far do not present information about transmission privacy or device authentication. Features such as access control, identity management, or encryption add a bit of security to Internet communication. Table 3 shows that little security in farming systems is limited to privacy and reliable data transmission between the user and the cloud or between the gateway and the cloud.

Table 3
Security features added to Agriculture 4.0

Layer	Security issues	Security Resources	Papers
Application	Data thefts	HTTPS	Khelifa et al. [11], Minh et al. [25]
	Sniffing	HTTPS	Khelifa et al. [11], Minh et al. [25]
	Access Control	IP Authentication	Nageswara Rao and Sridhar [15]
		User and Device Management	Oliver et al. [21]
	Phishing attack	Use not reported	Open issue
	Malicious scripts	Use not reported	Open issue
	Deny of services	Use not reported	Open issue
Edge	Man-in-the-middle	Use not reported	Open issue
	Booting vulnerabilities	Use not reported	Open issue
	Unauthorized access	Use not reported	Open issue
	Signature wrapping	Use not reported	Open issue
	Flooding	Use not reported	Open issue
	Forged control for actuators	Use not reported	Open issue
	Gateway-cloud request forgery	Use not reported	Open issue
	Forged measure injection	Use not reported	Open issue
Network	DoS/DDoS	Use not reported	Open issue
	Data transit attacks	Use not reported	Open issue
	Routing attacks	Use not reported	Open issue
	Signal disruptions	Use not reported	Open issue
Perception	Random sensor incidents	Use not reported	Open issue
	Autonomous system hijacking	Use not reported	Open issue
	Autonomous system disruption	Use not reported	Open issue
	Optical deformation	Use not reported	Open issue
	Irregular measurement	Use not reported	Open issue
	Sensor weakening	Use not reported	Open issue
	Node capture	Use not reported	Open issue
	Fake node	Use not reported	Open issue
	Sleep deprivation	Use not reported	Open issue

Many solutions for smart farming only include security mechanisms in the application layer. While [12,13] use HTTPS for communication between the cloud and the end-user application, most systems use the HTTP, CoAP, and MQTT protocols without any integration with SSL or TLS protocols. Similarly, many proposals do not implement access control or use it with limited resources. The absence of robust security features for communication between the cloud and the end-user creates several security breaches. There is no information about configuring security features in database management systems or using secure data search techniques in web applications. Thus, these features are probably not included.

Currently, smart agriculture is an easy target for malicious agents. Attacks may have several motivations, such as commercial, ideological, or even terrorist reasons. For instance, terrorist groups can inflict economic harm to a nation, economic opportunists may try to manipulate markets, and an individual employee may proceed with an attack for a variety of reasons [8]. Thus, it is urgent to add security as an essential resource for smart farming, contributing to the development and popularization of reliable and efficient systems.

5. Improvements and enhancements required for upcoming applications

Devices from traditional Internet have many security features built into them, like firewalls, authentication, and access control schemes, and so on. However, these security shields are missing on Agriculture 4.0 or limited in use. Sometimes this is due to smart farming is still emerging,

sometimes because the resources are inadequate for this technology or the absence of professionals to manage these resources. Also, a well-defined framework and standard to guide an end-to-end application development are not available yet. Usually, solutions are not standalone, but it is an embedded product that integrates many individuals and industries and requires an architecture that can handle heterogeneity, interoperability, and numerous devices. This architecture should allow multiple access, in a secure and coordinated way, to avoid data loss and compromise the system efficiency. Security resources presented in Table 4 may improve smart farm security in different scenarios.

On the perception layer, devices could be resistant packaging to prevent some sensor incidents and autonomous system disruption. However, this can be very expensive to use for some low-cost systems or those using many sensors. If it is not possible to avoid incidents, then it is necessary to use techniques to prevent disrupted data from affecting system accuracy and influencing decision-making. Therefore, it is essential to develop security schemes to detect sensor or incidents and avoid the use of corrupt or inconsistent data. On the other hand, Autonomous Tractor is robust equipment that requires more precision and reliability. The tractors have a structure to support the inclusion of tamper-resistant boxes. Thus, it is possible to prevent a malicious employee or a commercial competitor from modifying or damaging these subsystems, for example.

GPS is an essential component of many autonomous systems, whether tractors, drones, or UAVs, and requires security to prevent threats that affect their accuracy [53,54]. Therefore, it is necessary to invest in mechanisms to protect the GPS used by autonomous systems. Violations of the GPS can result in significant physical damage to the Autonomous System, the crop, or the farm. Similarly, manufacturers of these systems must create strategies to protect the remote control system, including, but not limiting to, features such as data encryption and access control.

Irregular measurement, sensor weakening, optical deformation, and signal disruption could trigger inconsistent data resulting in incorrect decision-making. Usually, it is not possible or quite difficult to avoid such threats, but it is necessary to prevent inconsistent data from propagating through the system. Inconsistencies can be misinterpreted as attacks and inadequately handled by security systems. Thus, it is essential to identify both attacks to the system, Sensor Weakening, Irregular Measurement, Optical Deformation, and Signal Disruption to prevent the system from generating or using incorrect data that makes the system operate unreliably. Some solutions designed for errors, faults, and failures detection, such as those proposed by Ref. [55,56], could be adapted for this purpose.

Table 4
Security resources to improve security in smart agriculture.

Security resources	IoT Resource	Security threats
IDS	Cloud, gateway	DoS/DDoS, autonomous system hijacking, forged control for actuators, gateway-cloud request forgery, forged measure injection, flooding, XSS attack, SQL injection, infiltration, port scan, backdoors, worms, routing attacks, and others cyberattacks
Anomaly detection system	Data, services	Random sensor incidents, autonomous system disruption, optical deformation, irregular measurement, sensor weakening, gateway-cloud request forgery, forged measure injection, data transit attacks and others cyberattacks
Cryptography	Data, communication link	Forged measure injection, false data injection, eavesdropping, traffic interception, man-in-the-middle, data capture
Authentication	Services, devices	Forged control for actuators, gateway-cloud request forgery, fake node, forged measure injection, false data injection, advanced persistent attack, malicious scripts, unauthorized access
Access Control	Services, devices	Unauthorized access
Firewall	Cloud, gateway	Unauthorized access
Anti-virus/ malware	Cloud	Phishing, virus, worm
Specialized solutions	Applications, services, protocols	Node capture, autonomous system hijacking, routing attacks, sleep deprivation, signature wrapping
Open Issue		Booting

Other preventive measures include the use of big data algorithms to filter data [57], and Intrusion Detection Systems (IDS) to detect data intruders. However, including IDS in smart farming can be challenging as there is usually no IT department to manage the system, and the farmer does not have the technical knowledge to maintain this resource. Therefore, IDSs developed for Agriculture 4.0 need to be transparent, as far as possible, and easy to manage. Besides, most IDSs analyze network traffic patterns [58,59], which may be efficient in identifying DoS/DDoS, forged control for actuators, gateway-cloud request forgery, forged measure injection, and other network-bound attacks but is inefficient in identifying failures, data noise, and false data injection. For these threats, it is possible to use a set of strategies, such as anomaly detection, encryption, and authentication.

Some attacks require additional preventive measures. For example, integrity verification protocols [32] or schemes capable of identifying malicious nodes [60,61] could identify or mitigate autonomous system hijacking, node capture attacks. Systems designed for low power consumption networks may detect sleep deprivation [62]. Artificial intelligence algorithms and machine learning could discover forged control for actuators, gateway-cloud request forgery, forged measure injection, and false data injection [63]. Solutions like XPath and FastXPath can mitigate signature wrapping attacks [48].

Authentication services applied to devices and services at all layers can make it difficult or limit forged control for actuators, gateway-cloud request forgery, forged measure injection, and prevent unauthorized access. The edge is the middle element, and it becomes a critical security point, which needs strict access controls, and schemes to avoid false data injection. However, the current access control systems may not be efficient in the context of smart agriculture. Access controls that require human intervention are impractical in intelligent agriculture because of the characteristics of the machines and users involved. For example, end-user authentication may use user and password-based or biometric schemes. Key-based access schemes could be feasible for systems that include up to a hundred devices or services, as long as they do not require periodic modification. However, some solutions may incorporate more features or demand periodical key updating to achieve an adequate level of security. The large number and variety of devices used by smart farming require new authentication schemes to manage them by the user [37,64], who usually does not have the technical knowledge to manage authentication services. New authentication schemes must be transparent to the user, lightweight to operating on constrained devices, and efficient.

Gateways must have security features to prevent unauthorized remote access and control by malicious agents. Barriers like firewalls, Intrusion Prevention Systems (IPS), authentication, and access control schemes can be useful, but gateways have restricted resources, requiring lightweight and efficient controls [6,37]. Some gateways are more restricted, making it impossible to use most security mechanisms, which makes this task even more challenging. Others have more computational resources and include a small operating system, limited processor, and little memory. The software developed for these devices should be lightweight and easy to manage to be operated by farmers. Once the gateway accesses many resources and devices, and intermediates communication between the perception and cloud layers, it is a critical element in the smart system and compromising it may affect the whole system.

Traditional cryptographic schemes may be unsuitable in smart systems. The perception layer has constrained devices that do not have the memory, processing power, and energy to compute traditional

algorithms [64]. Encryption is an efficient tool to minimize attacks such as traffic interception, data theft, and sniffing and may be used to hinder attacks such as forged measure injection. This tool can provide reliable data transfer between perception layer devices and the gateway. However, the use of cryptography in intelligent agriculture requires new encryption schemes that are lighter and more efficient than those currently in use.

DoS attacks may affect all services and devices in the system. The perception layer does not have the computational power to run intrusion detection systems. Therefore, firmware should prevent excessive requests from draining system resources. Edge services must accept a limited amount of connections to avoid delays and service disruption. Furthermore, IDSs or anomaly detectors designed for the edge may provide a way to mitigate such attacks. These detectors may identify several threats such as jamming and false data injection [65], malicious devices [66,67], and several routing attacks [68–70]. The cloud could use robust security schemes to mitigate DoS, such as traditional IDSs or anomaly detectors, while configuring services to prevent them from being affected by an excessive amount of requests, both from the system itself and the Internet.

Communication between devices could use one or more technologies, such as LoRa, LoRaWan, Sigfox, Zigbee, and LTE. Some standards allow connecting devices over wide areas, simplifying management and reducing installation and maintenance costs. However, only these features are not enough to guarantee data transmission security. Technologies that support some level of encryption can maximize data transmission security, reducing the risk of traffic interception.

Networks operating over TCP/IP, whether in the perception, edge or cloud, could maximize communication security using protocols lighter and more flexible than HTTP. The HTTP protocol used on the traditional Internet is not suitable for systems such as smart farming because it is computationally complex, incurs an enormous overhead, and is potentially insecure [7]. There are several alternative protocols such as MQTT, SMQTT, CoAP, XMPP, UPNP, AMQP, M3DA, DDS, JMS, and JavascriptIoT. These protocols were developed for industrial communications or IoT and are more suitable for smart agriculture. Some of them have cryptography support, appropriate for networks that have no secrecy in the communication layer. It is important to emphasize that, even if the sensors' data are not sensitive, the system usually exchange private information over the network, such as identifiers and access credentials. Any sensible data transmitted over the network requires secure communication.

The application layer should have more security resources because of the Internet connection. Robust and rigorous access control is essential to prevent unauthorized access and remote control of services and applications. In the cloud, it is imperative to add features such as firewalls for perimeter protection, antivirus, and antiphishing to reduce risks with phishing, malicious scripts, and viruses/worms. Cloud services must restrict connections to other services or users as much as possible to prevent data leakage and denials of service. Using microservices favors environment security if properly configured.

In summary, edge and gateway protection schemes should include features such as compatibility, low resource consumption, and effectiveness. The identity management system must be transparent to end-user and able to work with numerous and different devices, protecting the devices and services. Data must be protected at all stages to ensure system reliability and efficiency. However, system constraints require light and efficient algorithms. The cloud can use security schemes developed for the traditional Internet since this layer has the necessary computational resources for its execution.

6. Conclusion

The agricultural methods modernization is essential to increase production rates and preserve natural resources. Smart agriculture can enhance farming tasks by providing efficient control of actuators, optimizing utility and resource use, managing production, maximizing profit, and minimizing costs. However, to achieve this goal, smart systems must include more computational capabilities, such as edge computing, handling massive data, artificial intelligence resources, and security features. Security requires special attention as constrained devices generate a large volume of data and forward them to the gateway or the cloud. The farming system must protect the data from the detection through to decision-making and storage.

Although many security threats can affect agricultural systems, they still incorporate a few security resources. Possibly this is because these solutions are still in their early stages of development. Most times, there are only automation resources implemented, and these have few computational resources. Thus, security features are not yet on the list of system requirements. However, reaching an additional level of smart farming demands solutions with security mechanisms that give them enough reliability and accuracy to implement these systems on a large scale. As smart farming creates an extra set of challenges, it also presents fresh research opportunities both in security and in other areas of computer science.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] United Nations, Department of Economic, Affairs Social, Division Population. World population prospects 2019: highlights. 2019.
[2] Nation United. Sustainable development goals. https://sdgs.un.org/goals; 2017.
[3] Food and Agriculture Organization of the United Nations - FAO. Strengthened global partnerships needed to end hunger and malnutrition. 2019. http://www.fao.org/news/story/en/item/1194310/icode/.
[4] Trendov NM, Varas S, Zeng M. Digital technologies in agriculture and rural areas - status report, Tech. Rep., Nations. Rome, Italy: Food and Agriculture Organization of the United; 2019.
[5] OECD. Food, A. O. Of the united nations, OECD-FAO agricultural outlook 2020-2029. 2020. https://doi.org/10.1787/1112c23b-en. https://www.oecd-ilibrary.org/content/publication/1112c23b-en.
[6] Varga P, Plosz S, Soos G, Hegedus C. Security threats and issues in automation IoT. In: IEEE international workshop on factory communication systems - proceedings, WFCS, IEEE, trondheim, Norway, ISBN 9781509057887. p. 6. https://doi.org/10.1109/WFCS.2017.7991968}.
[7] Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B. A survey on IoT security: application areas, security threats, and solution architectures, vols. 1–1. IEEE Access; 2019. ISSN 2169-3536.
[8] Olson D. Agroterrorism: threats to America's economy and food supply. https://leb.fbi.gov/articles/featured-articles/agroterrorism-threats-to-americas-economy-and-food-supply; 2012.
[9] Ózvvári L, Kasza G, Lakner Z. Historical and economic aspects of bioterrorism. In: Management, organizations and society; 2017. p. 179–86. https://doi.org/10.18515/dBEM.M2017.n01.ch18. chap. 18, http://real.mtak.hu/39950/1/Management_Organizations_and_Society-Agroinform-2017jan08-DOI_CrossRef-Chapter_3.2.pdf.
[10] Monke J. Agro-terrorism: threats and preparedness, tech. Rep., congressional research service. 2008 {March12,2007}.
[11] Khelifa B, Amel D, Amel B, Mohamed C, Tarek B. Smart irrigation using internet of things. In: 4th international conference on future generation communication technology, FGCT 2015. Luton, UK: IEEE; 2015, ISBN 9781479982660. p. 91–6. https://doi.org/10.1109/FGCT.2015.7300252}. ISSN 2377-262X.
[12] Sales N, Remedios O, Arsenio A. Wireless sensor and actuator system for smart irrigation on the cloud. In: IEEE world forum on Internet of things. Milan; Italy: WF-IoT, IEEE; 2015, ISBN 9781509003655. p. 693–8. https://doi.org/10.1109/WF-IoT.2015.7389138. ISSN 0954-4089.
[13] Goap A, Sharma D, Shukla AK, Rama Krishna C. An IoT based smart irrigation management system using Machine learning and open source technologies. Comput Electron Agric 2018;155:41–9. https://doi.org/10.1016/j.compag.2018.09.040}. ISSN 01681699.
[14] Mahalakshmi M. Distant monitoring and controlling of solar driven irrigation system through IoT. In: National power engineering conference (NPEC). Madurai, India: IEEE; 2018, ISBN 9781538638033. p. 1–5.
[15] Nageswara Rao R, Sridhar B. IoT based smart crop-field monitoring and automation irrigation system. In: 2nd international conference on inventive systems and control, ICISC 2018. Coimbatore, India: IEEE; 2018, ISBN 9781538608074. p. 478–83. https://doi.org/10.1109/ICISC.2018.8399118}. ISSN 1472-4472.

[16] Navarro-Hellín H, Martínez-del Rincon J, Domingo-Miguel R, Soto-Valles F, Torres-Sánchez R. A decision support system for managing irrigation in agriculture. Comput Electron Agric 2016;124:121–31. https://doi.org/10.1016/j.compag.2016.04.003}. ISSN 01681699.

[17] Rajalakshmi P, Mahalakshmi SD. IOT based crop-field monitoring and irrigation automation. In: 10th international conference on intelligent systems and control, ISCO 2016. IEEE, Coimbatore; India; 2016, ISBN 9781467378079. p. 1–6. https://doi.org/10.1109/ISCO.2016.7726900}. ISSN 0018-9197.

[18] Zhao W, Lin S, Han J, Xu R, Hou L. Design and implementation of a smart irrigation system based on LoRa. In: IEEE globecom workshops. Singapore: IEEE, Singapore; 2017, ISBN 978-1-78561-238-1. p. 1–6. https://doi.org/10.1049/cp.2016.1357}.

[19] Ruengittinun S, Phongsamsuan S, Sureeratanakorn P. Applied internet of thing for smart hydroponic farming ecosystem (HFE). In: 10th international conference on ubi-media computing and workshops with the 4th international workshop on advanced E-learning and the 1st international workshop on multimedia and IoT: networks, systems and applications (Ubi-Media 2017). IEEE Inc, Beach RoadPattaya; Thailand; 2017, ISBN 9781538627617. p. 1–4. https://doi.org/10.1109/UMEDIA.2017.8074148}.

[20] Lee M, Kim H, Yoe H. Intelligent environment management system for controlled horticulture. In: 4th NAFOSTED conference on information and computer science, NICS 2017 - proceedings. Hanoi; Vietnam: IEEE Inc; 2017, ISBN 9781538632109. p. 116–9. https://doi.org/10.1109/NAFOSTED.2017.8108049}.

[21] Oliver ST, González-Pérez A, Guijarro JH. An IoT proposal for monitoring vineyards called SEnviro for agriculture. In: Proceedings of the 8th international conference on the Internet of things - IOT '18, 1, ACM New York, santa barbara; United States, ISBN 9781450365642. p. 1–4. https://doi.org/10.1145/3277593.3277625}.

[22] Thorat A, Kumari S, Valakunde ND. An IoT based smart solution for leaf disease detection. In: International conference on big data, IoT and data science, BID 2017, 2018-Janua. Pune, India: IEEE; 2018, ISBN 9781509065936. p. 193–8. https://doi.org/10.1109/BID.2017.8336597}. ISSN 13456652.

[23] Yoon C, Huh M, Kang S-G, Park J, Lee C. Implement smart farm with IoT technology. In: 20th international conference on advanced communication technology (ICACT). Korea (South), Korea (South): IEEE, Chuncheon-si Gangwon-do; 2018, ISBN 9791188428007. p. 749–52. https://doi.org/10.23919/ICACT.2018.8323908}. ISSN 17389445.

[24] Musat GA, Colezea M, Pop F, Negru C, Mocanu M, Esposito C, Castiglione A. Advanced services for efficient management of smart farms. J Parallel Distr Comput 2018;116:3–17. https://doi.org/10.1016/j.jpdc.2017.10.017}. ISSN 07437315.

[25] Minh QT, Phan TN, Takahashi A, Thanh TT, Duy SN, Thanh MN, Hong CN. A cost-effective smart farming system with knowledge base. In: 8th international symposium on information and communication technology - SoICT 2017. Nha Trang; Vietnam: ACM New York; 2017, ISBN 9781450353281. p. 309–16. https://doi.org/10.1145/3155133.3155151}. ISSN 00243795.

[26] Colezea M, Musat G, Pop F, Negru C, Dumitrascu A, Mocanu M. CLUeFARM: integrated web-service platform for smart farms. Comput Electron Agric 2018;154(August):134–54. https://doi.org/10.1016/j.compag.2018.08.015}. ISSN 01681699.

[27] Raducu IG, Bojan VC, Pop F, Mocanu M, Cristea V. Real-time alert service for cyber-infrastructure environments. In: 10th international conference on P2P, parallel, grid, cloud and Internet computing, 3PGCIC 2015. Poland: IEEE, Krakow; 2015, ISBN 9781467394734. p. 296–303. https://doi.org/10.1109/3PGCIC.2015.122}.

[28] Wongpatikaseree K, Kanka P, Ratikan A. Developing smart farm and traceability system for agricultural products using IoT technology. In: IEEE/ACIS 17th international conference on computer and information science (ICIS). Singapore: IEEE, Singapore; 2018, ISBN 9781538658925. p. 180–4. https://doi.org/10.1109/ICIS.2018.8466479}.

[29] Mekala MS, Viswanathan P. A Survey: smart agriculture IoT with cloud computing. In: International conference on microelectronic devices, circuits and systems, ICMDCS 2017. Vellore, India: IEEE; 2017, ISBN 9781538617168. p. 1–7. https://doi.org/10.1109/ICMDCS.2017.8211551}.

[30] Ray PP. Internet of things for smart agriculture: technologies, practices and future direction. J Ambient Intell Smart Environ 2017;9(4):395–420. https://doi.org/10.3233/AIS-170440. ISSN 18761364.

[31] Zhao K, Ge L. A survey on the internet of things security. In: 2013 ninth international conference on computational intelligence and security. Leshan, China: IEEE; 2013, ISBN 9781479925483. p. 663–7. https://doi.org/10.1109/CIS.2013.145}. ISSN 2316-9451.

[32] Agrawal S, Das ML, Lopez J. Detection of node capture attack in wireless sensor networks. IEEE Systems Journal 2019;13(1):238–47. https://doi.org/10.1109/JSYST.2018.2863229. ISSN 19379234.

[33] Lin J, Yu W, Zhang N, Yang X, Zhang H, Zhao W. A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal 2017;4(5):1125–42. https://doi.org/10.1109/JIOT.2017.2683200}. ISSN 23274662.

[34] Sarma R, Barbhuiya FA. Internet of things: attacks and defences. In: 2019 7th international conference on smart computing and communications, ICSCC 2019. Sarawak, Malaysia: IEEE; 2019, ISBN 9781728115573. p. 1–5. https://doi.org/10.1109/ICSCC.2019.8843649}.

[35] Syed A, Shah SH. A comprehensive security model for internet of things. Int J Comput Commun Netw 2019;1(2):38–46.

[36] Kumar SA, Vealey T, Srivastava H. Security in internet of things: challenges, solutions and future directions. In: Proceedings of the annual Hawaii international conference on system sciences. Koloa, HI, USA: IEEE; 2016, ISBN 9780769556703. p. 5772–81. https://doi.org/10.1109/HICSS.2016.714}. ISSN 15301605.

[37] Chahid Y, Benabdellah M, Azizi A. Internet of things security. In: 2017 international conference on wireless technologies, embedded and intelligent systems, WITS 2017. IEEE; 2017, ISBN 9781509066810. p. 1–6. https://doi.org/10.1109/WITS.2017.7934655}.

[38] Vasques AT, Gondim JJ. Amplified reflection DDoS attacks over iot mirrors: a saturation analysis. In: WCNPS 2019 - workshop on communication networks and power systems. IEEE, Brasília, Brasil; 2019, ISBN 9781728129204. p. 1–6. https://doi.org/10.1109/WCNPS.2019.8896290}.

[39] Kolias C, Kambourakis G, Stavrou A, Voas Jeffrey. DDoS in the IoT: mirai and other botnets. Computer 2017;50(7):80–4.

[40] Capellupo M, Liranzo J, Bhuiyan MZA, Hayajneh T, Wang G. Security and attack vector analysis of IoT devices. In: Security, privacy, and anonymity in computation, communication, and storage. Cham: Springer International Publishing; 2017. 978-3-319-72395-2, 593–606.

[41] Pundir S, Wazid M, Singh DP, Das AK, Rodrigues JJ, Park Y. Designing efficient sinkhole attack detection mechanism in edge-based IoT deployment. Sensors 2020;20(5):1300. https://doi.org/10.3390/s20051300}. ISSN 14248220.

[42] Goyal M, Dutta M, IEEE. Intrusion detection of wormhole attack in IoT: a review. In: 2018 international conference on circuits and systems in digital enterprise technology, ICCSDET 2018. Kottayam, India: IEEE; 2018, ISBN 9781538605769. p. 1–5. https://doi.org/10.1109/ICCSDET.2018.8821160}.

[43] Schulz S, Schaller A, Kohnhäuser F, Katzenbeisser S, Boot Attestation. Secure remote reporting with off-the-shelf IoT sensors. In: Computer security – ESORICS 2017, vol. 1. Cham, Oslo, Norway: Springer; 2017. p. 437–55.

[44] L. Garcia, L. Parra, J. M. Jimenez, J. Lloret, IoT-based smart irrigation systems : an overview on the recent trends on sensors and IoT systems for irrigation in precision agriculture, Sensors 20 (4).

[45] Ouaddah A, Mousannif H, Abou Elkalam A, Ait Ouahman A. Access control in the Internet of Things: big challenges and new opportunities. Comput Network 2017;112:237–62.

[46] Navas RE, Bouder HL, Cuppens N, Cuppens F, Papadopoulos GZ. Demo: do not trust your neighbors! A small IoT platform illustrating a man-in-the-middle attack. In: DHOC-NOW: international conference on ad hoc networks and wireless, september. Cham, Saint-Malo, France.: Springer; 2018, ISBN 9783030002473. p. 1–6. https://doi.org/10.1007/978-3-030-00247-3}.

[47] Stojmenovic I, Wen S. The Fog computing paradigm: scenarios and security issues. In: 2014 federated conference on computer science and information systems, FedCSIS 2014, vol. 2. Warsaw, Poland: IEEE; 2014, ISBN 9788360810583. p. 1–8. https://doi.org/10.15439/2014F503}.

[48] Gajek S, Jensen M, Liao L, Schwenk J. Analysis of signature wrapping attacks and countermeasures. In: 2009 IEEE international conference on web services, ICWS 2009. Los Angeles, USA: IEEE; 2009. p. 575–82.

[49] Benavides E, Fuertes W, Sanchez S, Sanchez M. Classification of phishing attack solutions by employing deep learning techniques : a systematic literature review. In: Developments and advances in defense and security. Singapore: Springer Singapore; 2020. p. 51–64.

[50] Guarda T, Augusto MF, Lopes I. The art of phishing. In: Advances in intelligent systems and computing. Cham, Bogots, Colombia: Springer; 2019, ISBN 9783030118891. p. 683–90. https://doi.org/10.1007/978-3-030-11890-7_64}. ISSN 21945357.

[51] Khan N, Abdullah J, Khan AS. Defending malicious script attacks using machine learning classifiers. Wireless Communications and Mobile Computing 2017 2017:9.

[52] Shurman MM, Khrais RM, Yateem AA. IoT denial-of-service attack detection and prevention using hybrid IDS. In: International arab conference on information technology (ACIT), vol. 3. IEEE, Al Ain, United Arab Emirates; 2019.

[53] Manesh MR, Kenney J, Hu WC, Devabhaktuni VK, Kaabouch N. Detection of GPS spoofing attacks on unmanned aerial systems. In: 2019 16th IEEE annual consumer communications networking conference (CCNC). IEEE; 2019. p. 1–6.

[54] Bonebrake C, O'Neil LR. Attacks on GPS time reliability. IEEE Security Privacy 2014;12(3):82–4.

[55] Di Modica G, Gulino S, Tomarchio O. IoT fault management in cloud/fog environments. In: ACM international conference on the Internet of things. New York, USA: ACM; 2019, ISBN 9781450372077. p. 1–4. https://doi.org/10.1145/3365871.3365882}.

[56] Power A, Kotonya G. Complex patterns of failure: fault tolerance via complex event processing for iot systems. In: International conference on Internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData). Atlanta, USA: IEEE; 2019. p. 986–93.

[57] García-Gil D, Luengo J, García S, Herrera F. Enabling smart data: noise filtering in big data classification. Inf Sci 2019;479(2019):135–52. https://doi.org/10.1016/j.ins.2018.12.002}. ISSN 00200255.

[58] Liu L, Xu B, Zhang X, Wu X. An intrusion detection method for internet of things based on suppressed fuzzy clustering. EURASIP J Wirel Commun Netw 2018;(1).

[59] Santos L, Rabadao C, Goncalves R. Intrusion detection systems in Internet of Things: a literature review. In: 13th iberian conference on information systems and technologies (CISTI). Caceres: IEEE; 2018. p. 1–7.

[60] Dimitriou T, Alrashed EA, Karaata MH, Hamdan A. Imposter detection for replication attacks in mobile sensor networks. Comput Network 2016;108:210–22. https://doi.org/10.1016/j.comnet.2016.08.019}. ISSN 13891286.

[61] Smache M, Mrabet NE, Gilquijano JJ, Tria A, Riou E, Gregory C. Modeling a node capture attack in a secure wireless sensor networks. In: 2016 IEEE 3rd world forum on Internet of things, WF-IoT 2016. Reston, USA: IEEE; 2016. p. 188–93.

[62] Jahir Husain A, Maluk Mohamed MA. IMBF counteracting denial-of-sleep attacks in 6LoWPAN based internet of things. J Inf Sci Eng 2019;35(2):361–74.

[63] Mode GR, Calyam P, Hoque KA. False data injection attacks in internet of things and deep learning enabled predictive analytics. In: EEE/IFIP network operations and ManagementSymposium. Budapest, Hungary: IEEE; 2020. p. 1–11.

[64] Partra L, Rao UP. Internet of Things — architecture, applications, security and other major challenges. In: 2016 3rd international conference on computing for sustainable global development (INDIACom). New Delhi, India: IEEE; 2016. p. 1201–6.
[65] Fu Y, Yan Z, Cao J, Koné O, Cao X. An automata based intrusion detection method for Internet of things. Mobile Information Systems; 2017.
[66] Sohal AS, Sandhu R, Sood SK, Chang V. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Comput Secur 2018;74:340–54.
[67] J. Pacheco, S. Hariri, Anomaly behavior analysis for IoT sensors, Transactions on Emerging Telecommunications Technologies 29 (4).
[68] Razaa S, Wallgren L, Voigt T. SVELTE: real-time intrusion detection in the internet of things. Ad Hoc Netw 2013;11(8):2661–74.
[69] Sun Z, Xu Y, Liang G, Zhou Z. An intrusion detection model for wireless sensor networks with an improved V-detector algorithm. IEEE Sensor J 2018;18(5): 1971–84. ISSN 1530437X.
[70] Sedjelmaci H, Senouci SM, Al-Bahri M. A lightweight anomaly detection technique for low-resource IoT devices: a game-theoretic methodology. In: IEEE international conference on communications, ICC 2016, vol. 6. Kuala Lumpur: IEEE; 2016.