Location Spoofing
A Dangerous Vulnerability for GNSS

Dinesh MANANDHAR

Center for Spatial Information Science

The University of Tokyo

dinesh@iis.u-tokyo.ac.jp

UN-Nepal Workshop on the Applications of Global Navigation Satellite Systems

12 – 16 DEC 2016, Kathmandu, Nepal

What is Location Spoofing?

- Location Spoofing is to FALSIFY Location as if it is TRUE Location

Spoofer transmits signal similar to signals from satellites.
The receiver can't distinguish between the SPOOFER signal and Satellite Signal.

GPS Spoofing Poses Risk of Future Havoc

GPS 'Spoofing' is No Joke: Dangers of GPS Data Hacking Realized

GNSS spoofing will attain virus status, warns expert – GPS World

Hacking Global Positioning System with GPS 'Spoofing' Can Lead To Fatalities
http://www.techworm.net/2016/11/gps-spoofing-dangers-gps-data-hacking.html

Dangers of GPS spoofing and hacking for location based services

Faking of GPS Data a growing and potentially lethal danger – The Japan Times, FB

The Japan Times
INCORPORATING The New York Times
Monday, November 28, 2016

Aftershock renews re

Fukushima jolt sparks Kansai rethink of Fukui restart plans

Eric Johnston
STAFF WRITER
Kyoto

The magnitude-7.4 aftershock that rocked Fukushima Prefecture and its vicinity last week, more than five years after the mega-quake and tsunami of March 2011, triggered fresh nuclear concerns in the Kansai region, which hosts Kansai Electric Power Co's Mihama plant in Fukui Prefecture.

The aftershock came as the Nuclear Regulation Authority approved a two-decade extension for Mihama's No. 3 reactor on Nov. 16, allowing it and two others that have already been approved to run for as long as 60 years to provide electricity to the Kansai region.

Residents need to live with the fact that they are close to the Fukui reactors, which are at least 40 years old. Despite reassurances by Kepco, its operator, and the nuclear watchdog, worries remain over what would happen if an earthquake similar to the one in 2011, or even last week, hit the Kansai region.

Kyoto lies about 60 km and Osaka about 110 km from the old Fukui plants. Lake Biwa, which provides water to about 13 million people, is less than 60 km away.

In addition to Kepco's 40-year-old Mihama No. 3, reactors 1 and 2 at the Takahama nuclear power plant in Fukui are 42 and 41 years old, respectively.

In the event of an accident, evacuation procedures for about 253,000 residents of Fukui, Shiga, and Kyoto prefectures who are within 30 km of the plants would go into effect.

But how effective might they be?

The majority does not live in Fukui, just over half, or 128,500, live in neighboring Kyoto, especially in and around the port city of Maizuru, home to a Self-Defense Forces base. Another 67,000 live in four towns in Fukui and about 58,000 live in northern Shiga Prefecture.

Plans call for Fukui and Kyoto prefecture residents to evacuate to 29 cities and 12 towns in Hyogo Prefecture and, if facilities there are overwhelmed, to Tokushima Prefecture in Shikoku. Those in Shiga are supposed to evacuate to cities and towns in Osaka Prefecture.

In a scenario put together by Kyoto Prefecture three years ago, it was predicted that tens of thousands of people would take to available roads in the event of an nuclear accident. A 100 percent evacuation of everyone within 30 km of a stricken Fukui plant was estimated to take between and 29 hours, depending how much damage there to the transportation i structure.

But Kansai-based anti clear activists have criti local evacuation plans as i unrealistic for several rea

First, they note that th gion around the plants g lot of snow in the winter, w could render roads, even i intact after a quake or oth aster, much more difficu navigate, slowing evacua even further.

Second is the radia screening process that been announced in of local plans drawn up by K and Hyogo prefectures.

While automobiles w be stopped at various ch points along the roads lea out of Fukui and given ra tion tests, those inside w not be tested if the vehic itself has radiation levels b the standard.

If the radiation is a standard, one person, a

KANSAI PERSPECTIVE

A turbine at the No. 3 reactor of Kansai Electric Power Co.'s

Dinesh Manandhar, a project associate professor at the University of Tokyo, speaks about the danger of GPS spoofing — the falsification of location data — at the university's Komaba campus in Meguro Ward, Tokyo, on Oct. 5. SHUSUKE MURAI

Falsification of location data puts lives at stake in digital age

GPS spoofing poses risk of future havoc, expert warns

Shusuke Murai
STAFF WRITER

With a plethora of location-based services hitting the market, GPS appears to be an essential feature in today's digitally driven world.

But Global Positioning System data can be used to create serious problems — even life-threatening ones — if control falls into the wrong hands, an expert warns.

"From car navigation systems to 'Pokemon Go' ... too many things today use GPS as a reliable source of location information," Dinesh Manandhar, a project associate professor at the University of Tokyo, said in a recent interview. "People trust the location information from GPS satellites like God."

Manandhar is developing systems to prevent what's called GPS spoofing — the falsification of location data.

Spoofing is easy, he said, and only requires an instrument called a GPS simulator. Used by manufacturers to test the accuracy of their products, GPS simulators generate the same kind of signals as GPS satellites, and can thus alter the location information received by devices such as smartphones, car navigation systems and others devices.

By using a GPS simulator, which cost about ¥1 million but could get cheaper in the future, "you can falsify your smartphone's ... information and make it look like you are going back and forth between Tokyo and Hawaii within just three minutes," Manandhar, 52, said in Japanese.

"Pokemon Go" has been a prime target of GPS spoofers. Some players are tweaking the GPS information in their smartphones to let them catch rare characters in far-flung places without setting foot outside home. Some have even posted YouTube videos showing how to do it.

The game's developer, Niantic Inc., posted a note on its website in August banning players from falsifying their locations. Niantic's terms of use now say that violators can be suspended or have their accounts terminated.

Although the trick hasn't yet led to a major incident, Manandhar said that GPS spoofing could be used to attack someone as compa-

'People trust the location information from GPS satellites like God.'

GPS EXPERT DINESH MANANDHAR

nies continue to turn more of our machines and appliances into remotely controllable objects.

For example, if autonomous cars become popular, a hacker could one day remotely force it to crash into a wall or another vehicle, causing a fatal accident, he said.

GPS spoofing can also be used to break a security technology called geofencing, which uses GPS data to create virtual boundaries that restrict access to classified information when outside certain locations.

"Let's say I were a top manager of a major bank. I could access all the information while sitting at my desk, but I wouldn't be able to access it from the room next to it," Manandhar said. "But people could get access to such information if they disguised the location information received by computer."

Although the dangers of GPS spoofing have been pointed out in academic circles since the early 2000s, businesses ignored them because there weren't many devices making use of location-based technologies, he said.

But today, with the proliferation of GPS-capable smartphones and other networked devices, "anyone can become a target of the attack," he said.

Under the Radio Law, the government forbids public transmission of radio waves — including GPS signals — without permission from the communications minister. Violators can face a maximum prison term of one year or a fine of up to ¥1 million.

Manandhar says that while it is technically possible to alert GPS users when fake signals are received, and to protect them from receiving fake signals at all, many devices don't have anti-spoofing technology installed.

"The products we are designing today are ones that we will use five years later. So we must assume the possible risks and prepare for the threats that might jeopardize our society in the future," he said.

"When PCs became common for many people, the sudden outbreak of computer viruses became an issue around the world, and anti-virus software become an essential tool for everyone to protect their data," he said. "The same thing is now happening around GPS. ... We need a system to fight back against the risk."

Nobel laureate Alexievich warns against human hubris

Corporate concern more focused on Asia than Trump's TPP pullou

Eric Johnston
STAFF WRITER
Osaka

For Kansai business leaders, Asia, particularly East Asia, has long been far more important economically than the United States.

So it was understandable when they reacted coolly to Donald Trump's victory in the U.S. presidential election, with some suggesting it was time to start entertaining the Trans-Pacific Partnership agreement without the U.S.

Yet while senior executives at major corporations who stand to hugely benefit from the trade deal are unhappy, most small and midsize firms who rather do business domestically or primarily in non-American markets, remain ambivalent. Many say they expect Trump's election to have little, if any, impact on the Kansai region, at least in the short term.

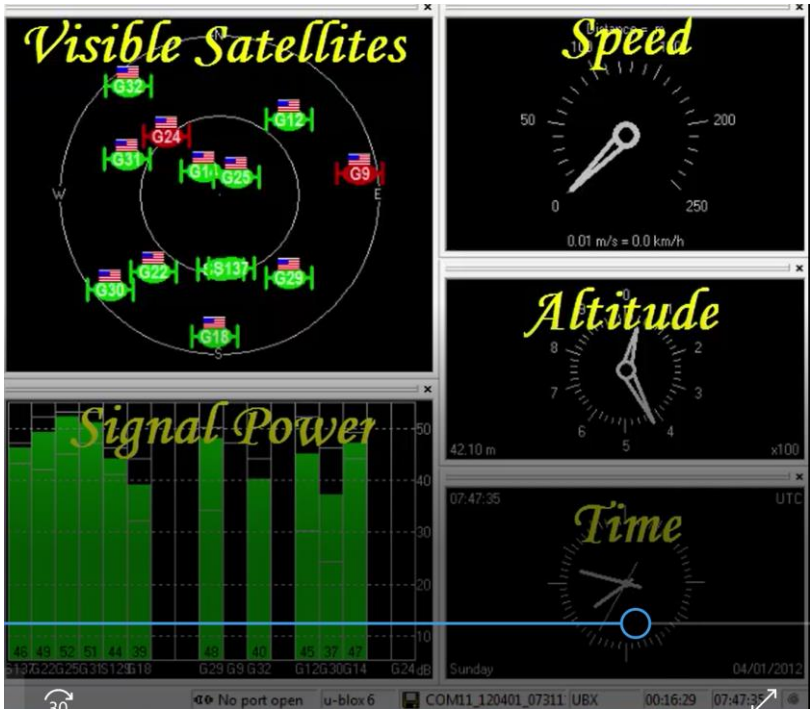
Still, at a news conference earlier this month, the Osaka branch manager of the Bank of Japan, Atsushi Miyanoya, sounded hopeful, saying that Trump as U.S. president could be a plus for Japan because of his promise to rebuild America's infrastructure and reduce taxes.

"If the U.S. economy is revitalized, this will lead to a p tive effect on those K firms that export to the U have production faci there," Miyanova said.

In the immediate after of the election, Kansai's business leaders all expr concern over Trump's flerc position to the TPP. He even last week that he would c it on his first day in office.

"Trump should aim for nomic development u open markets by particip in the TPP and revive his d economic policy," said Hir ki Suzuki, head of the Ki Association of Corporate ecutives (Kansai Keizai D

SPOOFing a Vehicle



The Vehicle is actually in a Parking Area (P).
GPS Receiver is SPOOFed to show that the
Vehicle is Driving along the Route shown in Green Color.

Why SPOOFING is Dangerous compared to Interference & Jamming?

Spoofing	Jamming and Interference
Intentional	Intentional and Non-Intentional
Difficult to Detect	**Can be Detected**
Available of Service but Lead to False Position Data	**Denial of Service**
No Effective Solution for Existing Signals	Many Solutions Exist
Fewer Research and Studies	Many Research and Studies

SPOOFing a Vehicle, VIDEO DEMO

Current Status of Anti-SPOOFing in GNSS

- Currently, there is no solution to prevent SPOOFing.
  - Even newly designed signals in GPS and QZSS do not have Anti-Spoofing capabilities
    - (except P & M codes in GPS)
  - Some signals in GALILEO (PRS and CS, not Open Signals) are said to have Anti-Spoofing capabilities
    - But, PRS and CS Signals are not available for general users and detail information are not available
    - Though Open Signals do not have Anti-Spoofing Capabilities, Proposals are made for Anti-SPOOFing capabilities

Our Solution to Anti-Spoofing

- We are developing Anti-Spoofing Solutions based on QZSS
- The Solution is designed based on QZSS L1S and other new signals
- It can detect both QZSS and GPS SPOOF signals
- By Implementing it, We can provide SPOOF PROOF LBS