FOI – Swedish Defence Research Agency Research for a safer and more secure world



GNSS threats – Jamming and spoofing Robust

Fredrik Marsten Eklöf fredrik.eklof@foi.se, 0709-277426



Vulnerability GNSS

- Interference (unintentional)
- Jamming signal denial
 - GNSS is vulnerable/sensitive to jamming (RF) due to the low received signal power
 - A low power jammer can achieve high relative power levels compared to the GNSS-signals
- Spoofing Deception
 - The purpose with spoofing is deceive one or several GNSS-receiver and the system
 - Generate erroneous PNT solution



Main reason for the sensitivity towards jamming is the large distance to the satellites



Google search: GPS/GNSS Jammers





Is universal, suitable for all kinds of cars





Interference

- Unintentional interference and jamming
- STRIKE3 (EU funded project)
 - 500 000 events detected
 - 70 000 estimated to be intentional jamming ("Personal / Privacy / Protection Device" - PPD)
 >15 000 denied GNSS
- http://gnss-strike3.eu/











Jamming

- Jamming (by state actors) experienced during military exercises
 - ➢ e.g. ZAPAD17, Trident Juncture, …
 - Denies GNSS for civilian airliners, ships, etc
- Also commonly experienced close to conflict areas
 - Syria (Russian Khmeimim Air Base)
 - ≻ Libya
 - Korean Peninsula
 - Persian Gulf





Internet GPS-jammer

Custom declaration:

- Declared as car adapter to avoid customs
- Contains no packing material of Chinese wood



SHENZHEN TAYX TECHNOLOGY DEVELOPMENT CO., LTD 593, 2ND BUILDING, CITY OF DESIGN, ZHENHUA WEST RD, SHENZHEN, CHINA 172... 4066-755-5880 6239

COMMERCIAL INVOICE



GNSS-jammers

- <u>http://www.cell-</u> jammers.com/gps-jammers
- <u>http://www.alljammer.com/</u>
- <u>http://www.thesignaljammer.</u> <u>com/categories/GPS-</u> <u>Jammers/</u>
- <u>http://www.jammerfromchin</u> <u>a.com/categories/GPS_Jam</u> <u>mers/</u>

LL-JAMMERS.	СОМ		Stype -		
ofessional jammer pro	ovider				Welcome to cell-jammers.
				Seard	h entire slore here
ME ABOUT US	ONLINE CATALOGUE	DEM SERVICE BL	.OG CON	ITACT US	
> GPS Jammers					
Y CART	GPS Jammers				
ave no items in your ing cart.	Cell-iammers.com manufa GPS JAMMER,GPS CAR JA professional manufacturer	cturing and wholesale GP MMER,GPS L1 L2 L5 JAM and wholesaler factory.	S JAMMER,GPS MER,ANTI TRACI	L1 JAMMER,HANDHOLD GPS . KING DEVICE,GPS SIGNAL JA	JAMMER,HIGH POWER GPS JAMMER MMER, Order best GPS JAMMER from
OUCT CATEGORIES	18 Item(s)	,			Show 48 T per page
CDMA/3G Jammers		11.00			PROTECT YOUR IDENTITY
immers		nu,			
nmers	1	-			
Jammers					
/Factory Jammers	SKU: GM08/PRO	SKU: GM08P/EU 8 BANDS GSM C	DMA 3G 4G	SKU: GM06/A 6 BANDS	SKU: BAG01 CELLPHONE GPS STGNAL
Talkie Jammers	SIGNAL JAMMER BLOCK GSM,3G,4G LTE,GPS	ING GPS L1 WIFI LO: PHONE JAMMER,	ACK CELL BLOCKING	GSM/3G/4G/WIFI/RADIO/RE JAMMER	MOTE TRANET KING BLOCKER POUCH CASE BAG. PREVENT
/XM 4G Jammers	ONE,SUPPORT 2 HOURS CONTINUE WORKING	AND 4G MOBILE IN ONE (FOR EU	PHONE ALL ROPE)	******** 2 Reviews \$210.00	\$18.00
uetooth Jammers	*****	*****	Reviews		
lammers	\$335.00	\$300.00			
	H ADD TO CART	H ADD TO CART	Г	🐂 ADD TO CART	📜 ADD TO CART
Recorder Jammers	Add to Wishlist Add to Compare	Add to Wishlist Add to Compare		Add to Wishlist Add to Compare	Add to Wishlist Add to Compare
umera Jammer & Detectors	s 111hii	Li Li	d c	L L L L L L	11
e Inspection System					
none Recorders			Щ		
ARNING!				and a second sec	
ngly advise that you check cal laws before purchasing ducts! We strongly oppose	SKU: GM09/EU 8 BANDS GSM DCS 3G 4 LTE(FOR EUROPE) WIFI G	SKU: GM09/US G- 8 BANDS GSM D PS- LTE(FOR USA) W	ICS 3G 4G- IFI GPS-L1	SKU: GM08/US 8 BANDS GSM DCS 3G 4G- LTE(FOR USA) WIFI GPS-L1	SKU: GM04/G HIGH POWER GSM/CDMA/DCS/PHS/GPS L1



Marketing of jammers - YouTube

- <u>https://www.youtube.com/watch?v=JCHcq2Fzsh8</u>
- <u>https://www.youtube.com/watch?v=-6hI5aTV2O8</u>
- <u>https://www.youtube.com/watch?v=Sj6KS6zoiJQ</u>
- <u>http://www.youtube.com/watch?v=uHm8eXyPaNU</u>
- <u>http://www.youtube.com/watch?v=PtHU9pXV0XQ</u>
- http://www.youtube.com/watch?v=-2ozZfKoD4o&list=PL1A88EBEE4CCD08FE
- <u>http://www.youtube.com/watch?v=_VDrH1By0Ss&feature=endscreen&NR=1</u>
- <u>http://www.youtube.com/watch?v=QKZI06cgi8M</u>



Example: Swedish incident

- Nazist ska ha kartlagt journalister döms för grovt vapenbrott – DN 2018-09-05
- "48-åriga xx är aktiv nazist och medlem i Nordiska motståndsrörelsen. Han ska ha förvarat ett stort antal vapen och vapendelar samt kommunikationsutrustning och störsändare."



办	Innehåll A-Ö Anpassa Lyssna Lättläst Teckens	språk Webbkarta English	
Privat Bransch	Om PTS E-tjänster 🛐	Q Press Kontakt	
Telefoni	<u>Startsida</u> / <u>Privat</u> / <u>Radio</u> / <u>Utrustning</u> / Förbud mot störsändare	47	
Internet - Radio	Förbud mot störsändare		
Amatörradio Ansökningshandlingar Båtradio Flygradio Hörselhjälpmedel Nytt tillstånd VHF fritidsbåt Radiostörningar Radiotillstånd Tekniktermer Till branschinformation Täckning Utrustning Förbud mot störsändare Nödsändare	 Det är förbjudet att i Sverige inneha störsändare (till exempel sändare som används för att störa mobiltelefoni). Den som innehar en störsändare i Sverige kan dömas till böter eller fängelse. Användning av störsändare kan orsaka mycket stora skador på kommunikationssystem som är nödvändiga för samhället, till exempel mobiltelefoni eller räddningstjänstens radiokommunikation. Förbudet gäller med några få undantag: Försvarsmakten, Försvarets radioanstalt och Försvarets materielverk får inneha störsändare. Även Polismyndigheten får inneha störsändare för viss verksamhet. PTS och Elsäkerhetsverket får också inneha störsändare i samband med utövande av marknadskontroll. PTS kan även besluta om undantag från förbudet att inneha störsändare för Kriminalvårdsstyrelsen, för att störsändare ska kunna användas på fängelser. Förbudet mot innehav av störsändare följer av 3 kap. 14 § lagen (2003:389) om elektronisk kommunikation samt 14 § förordningen 	 Sweden: Illegal to use and own jamming equipment Number of persons has been convicted Fine from 25 000 skr. 	

 Swedish police inform public regarding jamming equipment

 Specific for remote locking of cars polisen.se

Polisen varnar för störsändare

Låste du bilen?



En ny metod för att stjäla från bilar är att använda en så kallad störsändare. Det är en elektronisk apparat som blockerar/ stör ut den signal som bilnyckeln sänder till bilen när du trycker för att låsa och eventuellt också larma den.

- Kontrollera därför att din bil är låst när du lämnar den. Annars är det fritt fram för gärningsmannen att öppna den olåsta och olarmade bilen och tömma den på innehåll.
- En störningssändare kan variera i utseende och storlek. Den ser vanligen ut ungefär som en handhållen kommunikationsradio med en eller flera antenner.
- Om du inte kan låsa din bil med nyckel när du parkerar på en större p-plats, och det inte beror på dåliga batterier, så ber vi dig att ringa polisen och vara vaksam på personer i den närmsta omgivningen.

Försäkra dig om att bilen är låst när du lämnar den. Om du vill anmäla ett brott eller tipsa polisen, ring 114 14. I akut läge (pågående brott) ring 112.



Example: Norwegian incident

- «Jammet» GPS-signaler luftambulanse på vei til Røyken-ulykke rammet
- Vid en svår trafikolycka där ambulanshelikopter fick avbryta flygning kort efter start då GPS-tappades och flera andra system påverkades
 - "vanliga" ambulanser fick rycka ut
- Nasjonal kommunikasjonsmyndighet (Nkom) gjorde tillsyn i området och påträffade två lastbilar med GPS-störsändare
 - Från postnord.....
- Incidenter/påverkan har inträffat tidigare (10-15 ggr)

Lastebilsjåfører blokkerte GPS-signalene til ambulansehelikopter. Det skjer stadig oftere.

Nasjonal kommunikasjonsmyndighet (Nkom) har tre hypoteser som kan forklare hvorfor lastebilsjåfører kjører rundt med GPS-jammere.

Hans O. Torgersen Per Byhring (multime Publisert: 25.mar.2019 21:34 Oppdatert: 27.mar.2019 11:13

«Jammet» GPS-signaler luftambulanse på vei til Røyken-ulykke rammet



FASTKLEMT: Mannen i stasjonsvognen ble sittende fastklemt etter ulykken. Han ble senere fraktet til sykehus med luftambulansen. Foto: Edgar Dehli



Effect of jamming on GNSS

- Jammer signal blocks the GNSSsignal
- How a GPS-receiver is affected depends on the receiver implementation and jamming waveform
- Usually accuracy is degraded before the receiver can not determine a PNT solution



GNSS deception/Spoofing

- The purpose with spoofing is to force one or several GNSS-receivers to present an erroneous position and/or time
- Possible to locally generate GPS/GNSS signals
 - Public documents describe the GNSS-signals
 - A standard GNSS-receiver will not detect or exclude the false/spoofing signal
- A spoofing attack can be performed in in several different ways and with different type of equipment
 - Complete capability to control the receivers PNT-solution to introducing false/erroneous PNT – solution
- Earlier the spoofing threat was considered to be low but today there is a significant development of methods, techniques and hardware for spoofing
- The Next Big Threat to National Security is 'Spoofing'
 - director of the CIA. Mike Pompeo before the Senate Intelligence Committee on January 12, 2017



~

09:37 2019-11-07

k

sv 💿 🚍 🔱 💁 🎨 💻 🕥 🏴 🔒 🏪 🔩



GNSS deception

- Deception equipment used to be an expensive, exclusive resource; the hardware is now inexpensive (e.g. HackRF One SDR)
- Software easily available on the internet
- The software is easy to use and generates correct GPS-signals that are accepted and used by a GPS-receiver
- The software can be developed to include additional GNSS-signals



1 MSEK



∾GPS-SDR-SIM

GPS-SDR-SIM generates GPS baseband signal data streams, which can be converted to RF using software-defined radio (SDR) platforms, such as bladeRF, HackRF, and USRP.

Windows build instructions

Start Visual Studio.
 Create an empty project for a console application.
 Or the Solution Explorer at right, add "gpssim.c" and "getopt.c" to the Souce Files folder
 Select "Release" in Solution Configurations drop-down list.
 Suid the solution.

Building with GCC

\$ gcc gpssim.c -lm -O3 -o gps-sdr-sim

Generating the GPS signal file

A user-defined trajectory can be specified in either a CSV file, which contains the Earth-centered Earth-fixed (ECEP) user positions, or an NMEA GGA stream. The sampling rate of the user motion has to be 10Hz. The user is also able to assign a static location directly through the command line.



https://github.com/osqzss/gps-sdr-sim

Spoofing – SDR (software defined Radio)

- The presentation describes in detail how a GNSS SDR spoofer can be developed
- The problems are described and solutions are presented
- For the developed SDR spoofer the scenario can be generated with input from Google Maps
- Demonstrates that the SDR spoofer can be used against GNSS-receivers in different applications
 - Mobile phones (NEXUS 5, Iphone6, Samsung Note 3)
 - UAV (DJI drone)
 - Vehicle navigationsystems

https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20p resentations/DEFCON-23-Lin-Huang-Qing-Yang-GPS-Spoofing.pdf





Links: spoofing

- GPS Spoofing w/ BladeRF Software Defined Radio Series #23
 - <u>https://www.youtube.com/watch?v=VAmbWwAPZZo</u>
- Real-time GPS positioning with bladeRF
 - <u>https://www.youtube.com/watch?v=uf2vatqek_o</u>
- Generate a GPS signal and send it with HACKRF One, to deceive GPS receivers
 - <u>https://www.youtube.com/watch?v=nUrw9aHrKTY</u>
- Legal GNSS Spoofing and its Effects on Autonomous Vehicles
 - <u>https://www.youtube.com/watch?v=gxwkovHh3Ac</u>
- Simulation for GPS/GNSS Jamming and Spoofing
 - <u>https://www.youtube.com/watch?v=8al-lbg4PGM</u>



Spoofing incidents: Spoofing in the Black Sea

- Between June 22-24, a number of ships in the Black Sea reported erroneous GPS-positions
 - The reported positions were located at an airport
- This was most likely a real spoofing attack
 - Several ships were affected at the same time and area
 - ships reported that their positions would periodically "jump" from the true location to the incorrect location.
- The location of the spoofer has been estimated to Russian territory, close to Spoofing in th the Black Sea coast.



Spoofing in the Black Sea: What really happened? GPS world, October 11, 2017 - By Michael Jones

Spoofing

- GNSS spoofing (by state actors)
 - Over 1 300 spoofing events in waters around Russia found by analyzing maritime AIS data
 - Numerous reports from Moscow (around Kremlin)
 - Motivation protection of president Putin, critical facilities, etc



Spoofing

- GNSS spoofing attack against an autonomous car
- The autonomous car deviated from the path with 10 meters and drove of the road

Simulerad gps-attack fick testbilen att köra av vägen



Ett forskningsinstitut i Texas har utvecklat ett test som visar hur autonoma fordon påverkas när gps-signalen manipuleras. Institutets bil avvek tio meter från sin kurs, och körde av vägen.

Recommendations

Civil community

- Important that civilian actors prepare to meet the threat against GNSS from jamming and spoofing
- Possible to achieve significantly higher robustness both on receiver and system level
- Galileo Public Regulated Service (PRS)



