Liable Influences to Increase Security Risk in Global Navigation Satellite System

Tarun Varma[1], Dr. Akhilesh R. Upadhyay[2]
[1]*Research scholar ECE, Mewar University, Rajasthan*
[2] *Director SIRTS Bhopal (MP)*

***Abstract*- Global navigation satellite systems (GNSS) and its application like GPS, Galileo, GLONASS, and Beidou having great impact on society and also build important infrastructure in society. They provide timing and position for various applications. A GNSS is a complex system consisting various satellites, number of ground and monitor stations, telemetry, tracking plus a control centre. Many GNSS receivers represent the user segment. The receivers and the monitor stations receive a weak satellite radio signal under risk condition and thus are susceptible to interference like jamming or spoofing, Meaconing. So in this paper we only talk about the security risks and important factors for risk.**

***Index Terms*- GNSS, Meaconing, Spoofing, Jamming, Intrusion, Interference.**

I. INTRODUCTION

Current Global Navigation Satellite Systems (GNSS) having fewer authentications in the open service signals and so GNSS receivers are not able to protect signal by meaconing or spoofing attacks. These attacks disrupt and interference also capture authenticity of satellite signals like they can delay signals, change their path or re-broadcast signals. Positioning of signal or information is thus system compromised with attack and these services which having fixed location are easily captured by these risks. The risk is the probability about a particular threat that will degrade a particular authenticity [1,2]. The negative impact of a degradation of service, both in probability and in impact of occurrence. Act of God threats can be defined as circumstances or events that cause harm to communication system including Information Technology (IT) systems.

II IDENTIFIED RISK FOR DEGRADING SECURITY IN SATELLITE COMMUNICATION

The top four risks associated with satellite communications systems can be identified as Meaconing, Interference, Jamming, Intrusion, (MIJI) and physical security.

(1) Meaconing/spoofing are such type of system so that they receive our radio signals from navigational aids and rebroadcast them with some alteration on the same frequency to confuse our navigation. The enemy conducts meaconing/spoofing operations against us. A successful spoofing prevents our information, navigation, aircraft and ships from arriving at their desired targets or destinations [1,2,39]. Successful enemy meaconing/spoofing cause systems. The easy accessibility to the GNSS signal combined with a non security feature, as a cryptographic signature, in the signal modulation and data streams, makes civil infrastructures using open GNSS strongly defenseless to jamming and spoofing attacks due to the predictability of open GNSS signals. RFI is considered as the most disruptive event for the GNSS system.

- Aircraft to be misguided and land into enemy zones or enemy airspace.
- Ships also misguide and to be diverted from their desire routes.
- Fighter aircraft or even missile system expend ordnance on false targets.
- Ground stations to receive inaccurate position, locations of the received information.

(2) Intrusion is intentionally inserting additional electromagnetic energy into electromagnetic transmission paths it may be of any manner. The aim is to misguide equipments and operators which create confuse system. Generally the intrusion detection system alert us by protection against false information may be analog or digital into our receiver

paths which is inserted by our enemy. The corrupted information may work to reproduce voice instruction like coded voice instructions, false ghost objects, change of object coordinates for false communication, or even rebroadcasting of pre recorded data transmission over the same channel or link. The wireless communication encourage the use of wireless technology. In our daily life activity we find many devises such as laptops, notepads, PDAs, mobile phone handsets, satellite navigation systems for vehicles, Bluetooth peripherals and other gadgets which is taking advantage of wireless technology .The researcher in this field continue working toward being better in daily services like connectivity, management and security for networks . A temporary network can vigorously form without the requirement of any existing infrastructure using mobile ad hoc networking technology. In a network of autonomous devices, which communicate through wireless medium a distributed, multi-hop network architecture that does not depend on any pre-presented network infrastructure for its deployment

(3) Jamming is intentionally deliberately radiating signals, reradiating signals, or reflecting electromagnetic waves to impair the system of electromagnet devices, equipment, or systems. In most of the applications in wireless communication where security is the major issue, is a dependable and timely raise notification for such massages. To demonstrate this task is, a state-of-the-art alarm raising scheme for wireless communication that is fairly robust against unintentional link failures and investigate in terms of its resistance against jamming attacks. In current schemes blocking alarms by targeted, reactive jamming is not only straightforward, but that this jamming is also unnoticed by existing jamming prevention and detection schemes. To prevent the effective performance by our radios, RADARs navigational aids, satellites communication, and electro-optics etc ,the enemies conduct jamming operation.

(4) Interference is nothing but the electrical disturbance that causes our system to produce undesirable responses in electronic equipment like GPS and GNSS. As a MIJI term, interference refers to the unintentional disruption of the systems of radios, radars, Navigational aids, satellites, and electro-optics. This interference may be of friendly, enemy, or atmospheric. In satellite communications, the transmitted information is focused to various destructions which causes by the transmission medium combined with the mobility of transmitters and/or receivers. Path-loss is an attenuation of the signal power and depend upon the space among the transmitter and the receiver antenna. The cellular systems which use frequency reuse are founded on the physical facts of path-loss. Unlike the transmission in free space, transmission in practical channels, where propagation occurs at atmosphere and near the ground, is manipulated by terrain contours. As the mobile moves, the slow variation in mean envelope over a small region, shadowing, appears because of the variations in large-scale terrain characteristics, such as hills, forests, and clumps of buildings. Compared with the large-scale fading because of the shadowing, multipath fading, also called fast fading, refers to the small-scale fast actuation of the received signal envelope resulting from multipath response and transmitter and/or receiver movement. For example, a navigational broadcast may interfere with commercial communications.

III FACTORS THAT INCREASE RISK IN SATELLITE COMMUNICATION/GNSS

- Attacker know the frequency repetition period.
- Attacker know the coding sequence.
- Interference (Intentionally or Unintentionally).
- Attacker know the location of the signal.
- Strong frequency with respect to our signal.

IV CONCLUSION

MIJI i.e. Meaconing, Jamming, interference and spoofing are the main threats in the GNSS, and community related to satellite communication is currently seeking to resolve these risk by providing strong prevention and countermeasures at the user ends and GNSS signal/ system levels end. This paper has focused on the main aspects of the threat analysis, risks that starts and description of the origin of the threats, the different types of attack that need to be considered including meaconing,interference, spoofing/jamming incidents, their impact at the user

level and on critical infrastructure and some guidelines that could be considered to perform a full risk analysis per user case and application.

REFERENCES

[1] N. D. Pham, "The economics of disruption: $96 billion annually at risk," GPS World, Jul. 2011. [Online]. Available: http:// gpsworld.com/gnss-systemthe-economicsdisruption- 96-billion-annually-risk-11825/, [Accessed: 02-Jan-2016].

[2] M. Thomas, J. Norton, A. Jones, A. Hopper, N. Ward, and P. Cannon, "Global navigation space systems: Reliance and vulnerabilities," Roy. Acad. Eng., London, 2011. [Online]. Available: http://www.raeng.org.uk/publications/reports/global-navigationspace- systems, [Accessed: 02-Jan-2016].

[3] J. A. Avila Rodriguez, "On Generalized Signal Waveforms for Satellite Navigation," Ph.D. disseretation, Univ. FAF Munich, Munich, Germany, 2008.

[4] B. Motella, M. Pini, and F. Dovis, "Investigation on the effect of strong out-of-band signals on global navigation satellite systems receivers," GPS Solutions, vol. 12, no. 2, pp. 77–86, 2007.

[5] R. J. Landry and A. Renard, "Analysis of potential interference sources and assessment of present solutions for GPS/GNSS receivers," in Proc. 4th Saint-Petersburg Conf. INS, 1997, pp. 1–13.

[6] B. Motellaa, A. T. Balaeib, L. L. Prestic, M. Leonardid, and A. Dempsterb, "Characterization of radar interference sources in the Galileo E6 band," Aerotecnica-J. Aerosp. Sci., Technol. Syst., vol. 87, no. 4, 2009.

[7] T. Kraus, R. Bauernfeind, and B. Eissfeller, "Survey of in-car jammers—Analysis and modeling of the RF signals and IF samples (Suitable for Active Signal Cancelation)," in Proc. 24th Int. Techn. Meeting Satellite Div. Inst. Navig. (ION GNSS 2011), Portland, OR, USA, Sep. 2011, pp. 430–435.

[8] R. H. Mitch, R. C. Dougherty, M. L. Psiaki, S. P. Powell, B. W. O'Hanlon, J. A. Bhatti, and T. E. Humphreys, "Know your enemy: Signal characteristics of civil GPS jammers," GPS World, vol. 25, no. 1, pp. 64–71, 2012.

[9] Exelisinc, "The Threat of GPS Jamming", 2015. [Online].Available:http://www.exelisinc.com/solutions/signalsentry/Documents/ThreatOf GPS Jamming_Feb.2014.pdf, [Accessed: 30-Dec-2015].

[10] E. Kaplan and C. Hegarty, Understanding GPS, Norwood, MA, USA: Artech House, 2006.

[11] Nu-Trek Inc., "Anti-Jam RF Front Ends and Anti-Jam Solutions," 2015. [Online]. Available: http://www.nu-trek.com/., [Accessed: 30-Dec-2015].

[12] D. Shepard, J. Bhatti, and T. Humphreys, "Drone hack: Spoofing attackdemonstration on a civilian unmanned aerial vehicle," GPS World, 2012. [Online].Available: http://gpsworld.com/drone-hack/, [Accessed: 02-Jan-2016].

[13] European Space Agency, "Simulation Software to Guard Against Satnav Spoofers," 2016. [Online].Available:http://www.esa.int/Our_Activities/Navigation/Simulation_software_to_ guard _against_satnav_spoofers, [Accessed: 02-Jan-2016].

[14] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," in Proc. 21st Int. Techn. Meeting Satellite Div. Inst. Navig. (ION GNSS 2008), Savannah, GA, USA, Sep. 2008, pp. 2314–2325.

[15] C. Gu¨nther, "A Survey of Spoofing and Counter-Measures," NAVIGATION, J. Inst. Navig., vol. 61, no. 3, pp. 159–177, Fall 2014.

[16] O. Isoz, D. Akos, T. Lindgren, C.-C. Sun, and S.-S. Jan, "Assessment of GPS L1/Galileo E1 Interference Monitoring System for the Airport Environment," in Proc. 24th Int. Techn. Meeting Satellite Div. Inst. Navig. (ION GNSS 2011), Portland, OR, USA, Sep. 2011, pp. 1920–1930.

[17] M. Luo, G. Xie, D. Akos, S. Pullen, and P. Enge, "Radio frequency interference validation testing for LAAS using the Stanford integrity monitor testbed," in Proc. 2003 Nat. Techn. Meeting Inst. Navig., Anaheim, CA, USA, Jan. 2003, pp. 233–242.

[18] P. W. Ward, "Simple techniques for RFI situational awareness and characterization in GNSS receivers," in Proc. 2008 Nat. Techn. Meeting Inst. Navig., San Diego, CA, USA, Jan. 2008, pp. 154–163.

[19] P. W. Ward, "What's going on? RFI situational awareness in GNSS receivers," InsideGNSS, vol. 2, no. 6, pp. 35–42, Sep./Oct. 2007.