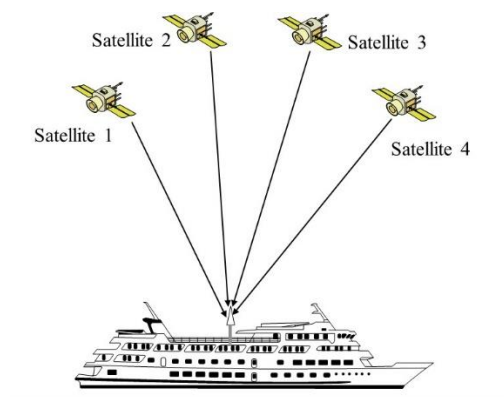


## Satellite navigation systems' vulnerabilities and alternative solutions

Modern IT-Information Technology and OT-Operational Technology systems, including those in the maritime sector, are inherently vulnerable to cyber-attacks. The IT manages administrative operations, while OT includes a wide range of programable controllers, which enable the convergence of the cyber and physical systems. Both IT and OT are critical in the maritime business and industry, therefore the TalTech's Maritime Academy Team of researchers works together with network security, software engineering, forensics, and human factor cyber experts to develop a holistic approach to security, safety, and resilience of maritime infrastructure. To put it simply, the Team is working to develop methods for the early detection and prevention of system failures, whether accidental or intentional. The focus is on systems that are essential for maritime navigation, first and foremost those on board the ship. The Team is also working on back-up solutions, so that in the event of a system failure, an alternative backup solution can automatically take over.



Obtaining ship's 3D position and time in relation to at least four satellites<sup>1</sup>

What would this mean in real scenario? – Let us assume that the GPS receiver on board, for some reason, is not working properly. This can happen for several reasons. For example, the cable between the antenna and the GPS receiver may be damaged or improperly plugged in. However, GPS receivers can be vulnerable to various types of malicious attacks. One example is jamming. Jamming is usually based on a small transmitter that works on almost the same frequency as the satellites. This noise can knock out the GPS receiver in radius of several tens of kilometers. Jamming resistance can be increased with CRPA-Controlled Reception Pattern

---

<sup>1</sup> Adapted from: Kjerstad N., *Electronic and acoustic navigation systems*, NTNU, Ålesund, Norway, 2016.

Antenna, but it is quite expensive and mainly available for military use. Spoofing is another, more sophisticated method of disturbance. Here, an emitter transmits signals, which the GPS receiver will be able to read as a satellite and thereby use as a completely erroneous line of position. Spoofing will be able to cause great errors in all receivers within range of vision. It requires more complicated equipment and more competence in comparison to jamming. Furthermore, it can easily be confused with multipath by the receiver, and therefore difficult to identify as an external source of error. To avoid the negative effects of jamming and spoofing, some alternative solutions can be used like hybrid receivers-GLONASS, BeiDou, Galileo, etc.; augmentation-smart support systems; stable clocks in the receivers; micro electromechanical sensors; inertial navigation; radio navigation, and the like. Some of these solutions are relatively costly, but where satellite systems are used in especially critical operations, they are worth considering. In this context, a modernized hyperbolic Loran system, i.e., e-Loran-Enhanced Loran, based on interoperability with GPS, must be mentioned. Additionally, for military purposes, a highly accurate military positioning, velocity, and timing service broadcasted is available in the form of coded PPS-Precise Positioning Service, with accuracy potential of 15 m (95%), or higher. The PPS includes cryptographic keys which remove the effects of selective availability and anti-spoofing connected to commercial GPS users.



Various types of portable GPS receivers<sup>2</sup>

Let's assume that in a case of attack to the satellite receiver, the ship has a modular navigation system, which can be switched to inertial navigation. The inertial navigation is based on a gyroscope and a tachometer that can be used to integrate the path travelled by the ship over a given period. The engine combustion and propulsion parameters can also be used to

---

<sup>2</sup> Ibid.

implicitly determine the ship's position, in addition to gyroscopes and speedometers. The inertial navigation system is usually combined with a Kalman filter, which compares a mathematical model of the ship's behavior in certain conditions with the data from the sensors and estimates the error, i.e. corrections, which are sent back to the inertial system. However, the inertial navigation system requires the last accurately recorded position of the ship. The TalTech Team is working to develop and improve the mathematical model of an experimental autonomous vessel, including advanced control of autopilot, which operates completely independently of the USA's GPS or any other global navigation satellite positioning system like Russian GLONASS, China's BeiDou, European Galileo, Indian IRNSS, or Japan's QZSS.

Let's not forget that satellite navigation is complemented by terrestrial and astronomical navigation. Referential objects on land and at sea can be useful for position estimation when the vessel is relatively close to the coast or in a sailing zone of high traffic density. If the ship is offshore, at the vast sea, a nautical almanac and (digital) sextant can help determine the ship's position relative to the stars. The alternatives to GPS and other global satellite navigation systems are available, while their improvements and further automation are actively under way.

Today, there is also a risk of intentionally disabling AIS-Automatic Identification System devices or hacking AIS targets. The AIS is used to identify and locate ships, as well as for communication and sharing routes. Virtual AIS is used as an add to navigation to check whether the system works as intended or not. In the event that this system does not work properly, the radar and advanced camera systems combined with radar can come to the rescue.

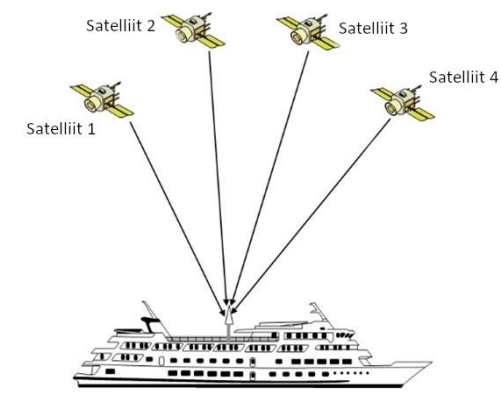
Instead of making a conclusion, allow us to make a small digression. The old sailors used to say: A sailor needs sea, boat, and sky to sail. Let's remind ourselves that Columbus sailed to America, da Gama reached India, while Magellan circumnavigated the globe using only magnetic compass ('south pointing fish') and astrolab. The mechanical chronometer was discovered much later.

Last but not least, the crisis that we are going through at the moment can be an opportunity for huge developments in the maritime sector and in general!

Sanja Bauk, Dan Heering, Yiğit Gülmez.

## Satelliitnavigatsioonisüsteemide haavatavused ja alternatiivsed lahendused.

Kaasaegsed info- ja käidutehnoloogia süsteemid, k.a süsteemid, mis on kasutusel merendusesektoris, on loomupäraselt haavatavad küberrünnakute suhtes. Infotehnoloogia (*information technology* - IT) haldab administratiivseid toiminguid, samas kui käidutehnoloogia (*operational technology* - OT) hõlmab mitmesuguseid programmeeritavaid kontrollereid, mis võimaldavad küber- ja füüsiliste süsteemide ühildamist. Nii IT kui ka OT on merendustegevuses kriitilise tähtsusega, mistõttu TalTech Eesti Mereakadeemia teadlaste meeskond töötab koos võrguturbe, tarkvaratehnika, kohtuekspertiisi ja inimfaktori ekspertidega, et arendada välja terviklik lähenemine merenduse infrastruktuuri turvalisusele, ohutusele ja vastupidavusele. Lihtsamalt öeldes töötab meeskond välja meetodeid nii juhuslike kui ka tahtlike süsteemirikete varajaseks avastamiseks ja ennetamiseks. Eelkõige keskendutakse nendele meresõiduks olulistele süsteemidele, mis asuvad laeva pardal. Meeskond töötab ka varulahenduste kallal, et rikke korral saaks alternatiivne lahendus automaatselt süsteemi üle võtta.



Laeva 3D-asukoha ja aja saamine vähemalt nelja satelliidi<sup>1</sup> suhtes.

Mida see tegelikult tähendaks? Oletame, et pardal olev GPS-vastuvõtja ei tööta millegipärast. See võib juhtuda mitmel põhjusel. Näiteks võib antenni ja GPS-vastuvõtja vaheline kaabel olla kahjustatud või valesti ühendatud. Vastuvõtjad võivad olla ka haavatavad mitmesuguste pahatahtlike rünnakute suhtes. Üks näide on GNSS signaali segamine (*jamming*). Segamine põhineb tavaliselt väikesel saatjal, mis töötab peaaegu samal sagedusel kui satelliidid. See võib GPS-vastuvõtja kümnete kilomeetrite raadiuses välja lülitada. Segamiskindlust saab suurendada CRPA-kontrollitud vastuvõtumustriga antenni abil, kuid see on üsna kallid ja

<sup>1</sup> Kohandatud: Kjerstad N., *Electronic and acoustic navigation systems*, NTNU, Ålesund, Norra, 2016.

saadaval peamiselt sõjaliseks kasutamiseks. GNSS signaali võltsimine (spoofing) on teine, keerukam häirimismeetod. Sellisel juhul edastab saatja signaale, mida GPS-vastuvõtja suudab lugeda satelliidina ning sellega tekitada ka olukorra, kus meeskond võib laeva asukohta valesti määrata. Selline rünnak suudab põhjustada suuri vigu kõigis vaateväljas olevates vastuvõtjates. Võrreldes segamisega nõuab see keerulisemaid seadmeid ja suuremat pädevust. Peale selle võib vastuvõtja seda kergesti segi ajada mitmerajalise signaaliga (multipath) ja seetõttu on seda raske tuvastada kui välist veallikat. Signaalide segamise ja võltsimise negatiivsete mõjude vältimiseks võib kasutada mõningaid alternatiivseid lahendusi nagu hübriidvastuvõtjaid (GLONASS, BeiDou, Galileo jne), täiendavaid nutikaid tugisüsteeme, stabiilseid kellasid vastuvõtjates, elektromehaanilisi mikroandureid, inertsiaalset navigatsiooni, raadionavigatsiooni jms. Mõned nendest lahendustest on suhteliselt kulukad, kuid kui satelliitsüsteeme kasutatakse eriti kriitilistes operatsioonides, tasub neid kaaluda. Selles kontekstis tuleb mainida kaasajastatud hüperboolset Loran-süsteemi, st e-Loran (Enhanced Loran), mis põhineb koostalitlusvõimel GPS'iga. Lisaks on sõjalistel eesmärkidel saadaval väga täpne sõjaline positsioneerimise, kiiruse ja aja määramise teenus, mida edastatakse kodeeritud kujul (Precise Positioning Service – PPS), mille täpsuse potentsiaal on 15 m (95%) või suurem. PPS sisaldab krüptograafilisi võtmeid, mis kõrvaldavad valikulise kättesaadavuse ja võltsimisvastase võitluse mõju, mis on seotud kommertslike GPS-kasutajatega.



Erinevat tüüpi kaasaskantavad GPS-vastuvõtjad

Oletame, et satelliitvastuvõtja ründamise korral on laeval modulaarne navigatsioonisüsteem, mida saab lülitada inertsnavigatsioonile. Inertsnavigatsiooni aluseks on güroskoop ja tahhomeeter, mida saab kasutada laeva läbitud teekonna integreerimiseks teatud aja jooksul. Lisaks güroskoobile ja logile saab laeva asukoha kaudseks määramiseks kasutada ka laeva peamasina põlemis- ja käitamisparameetreid. Inertsnavigatsioonisüsteemi kombineeritakse tavaliselt Kalmani filtriga, mis võrdleb laeva käitumise matemaatilist mudelit teatavates

tingimustes andurite andmetega ja hindab viga, st korrektsioone, mis saadetakse tagasi inertsiaalsesse süsteemi. Inertsnavigatsioonisüsteem vajab aga laeva viimast täpselt registreeritud asukohta. TalTechi meeskond töötab välja ja täiustab eksperimentaalse autonoomse laeva matemaatilist mudelit, sealhulgas autopiloodi täiustatud juhtimist, mis töötab täiesti sõltumatult USA GPS'ist või mõnest muust globaalsest satelliitnavigatsioonisüsteemist, nagu Venemaa GLONASS, Hiina BeiDou, Euroopa Galileo, India IRNSS või Jaapani QZSS.

Ärgem unustagem, et satelliitnavigatsiooni täiendab maapealne ja astronoomiline navigatsioon. Referentsobjektid maal ja merel võivad olla kasulikud asukoha hindamiseks, kui laev on suhteliselt lähedal rannikule või suure liiklustihedusega tsoonis. Kui laev on avamerel, siis aitavad laeva asukoha määramisel tähtede suhtes abiks olla merenduslik almanahh ja (digitaalne) sekstant. Alternatiivid GPS'ile ja muudele globaalsetele satelliitnavigatsioonisüsteemidele on olemas, samas kui nende täiustamine ja edasine automatiseerimine on aktiivselt käimas.

Tänapäeval on olemas ka oht, et laevade Automaatse Identifitseerimise Süsteemi (Automatic Identification System – AIS) seadmeid võidakse tahtlikult välja lülitada või AIS'i sihtmärke häkkida. AIS'i kasutatakse laevade identifitseerimiseks ja asukoha määramiseks, samuti sidepidamiseks ja marsruutide jagamiseks. Virtuaalset AIS'i kasutatakse navigatsiooni lisana, et kontrollida, kas süsteem töötab ettenähtud viisil või mitte. Juhul, kui see süsteem ei tööta korralikult, võivad appi tulla radar ja täiustatud kaamerasüsteemid koos radariga.

Kokkuvõtte tegemise asemel lubage meil teha väike kõrvalepõige. Vanad meremehed tavatsesid öelda: „Meremees vajab purjetamiseks merd, paati ja taevast“. Tuletagem meelde, et Kolumbus purjetas Ameerikasse, da Gama jõudis Indiasse, Magellan kasutas aga ümbermaailmareisil ainult magnetkompassi ("Iõunapoole suunatud kala") ja astrolaabi. Mehhaaniline kronomeeter avastati palju hiljem.

Lõpetuseks: kriis, milles me praegu elame, pakub võimalusi suurteks arenguteks nii merendussektoris kui ka üldiselt!

Sanja Bauk, Dan Heering, Yiğit Gülmez.