Submitted version of: J. Rossouw van der Merwe, Xabier Zubizarreta, Ivana Lukčin, Alexander Rügamer and Wolfgang Felber, "Classification of Spoofing Attack Types," European Navigation Conference (ENC) 2018, submitted on October 2017. accepted on May 2018.

Classification of Spoofing Attack Types

J. Rossouw van der Merwe, Xabier Zubizarreta, Ivana Lukčin, Alexander Rügamer and Wolfgang Felber
Fraunhofer IIS
Nuremberg, Germany
johannes.roussouw.vandermerwe@iis.fraunhofer.de

***Abstract*— All spoofer attacks have different requirements, impacts, success rates and objectives; therefore, to assess the threat and to develop appropriate counter measures, a clear classification is needed. Being aware of the different existing types of threats, allows an improved design of preventative measures to counter these attacks. This paper classifies spoofer attacks with a layered model. This allows assessing the risks and strategies of operational spoofers with the goal of prevention. The layered model consists of the deployment architectures, the take-over strategy, the control strategy and the application. The paper expands the strategies to manipulate a position of receiver, highlights operational difficulties and suitable counter measures. This emphasises that even if a signal is successfully spoofed, controlling a target receiver is not trivial. Additionally, the most probable spoofing attacks are presented and the applicable anti-spoofing methods are outlined.**

***Index Terms*—Spoofing, global navigation satellite system (GNSS), receiver design, receiver hardening, preventative engineering.**

I. Introduction

A spoofer falsifies global navigation satellite system (GNSS) signals to attack a receiver, thereby altering the receiver position, velocity, and time (PVT) solution [1], [2]. Spoofing is illegal, as it interferes with the primary user of the spectrum, hence an attack is associated with criminal or military activity. The spoofer transmits in the electromagnetic spectrum (EMS); therefore, it is an electronic warfare (EW) attack on the receiver [3]. Further, if the spoofer influences the receiver's PVT, then it is also an information warfare (IW) attack: as unauthorised access on the receiver hardware is achieved.

The spoofing goal may be to remove the navigation reliability in a restricted area (denial of service), or to manipulate the perceived location of the receiver (decoy). In both cases, the receiver developer would like to detect the spoofing attack, and (if it is possible) counter the attack to maintain navigation capability and integrity. The literature focuses on these anti-spoofing methods [2], [4]–[6]. However, there are limited publications on the spoofing attack types. In order to develop directed and applicable anti-spoofing methods, the spoofing threat and capabilities should first be understood. This follows the principle of adaptive engineering [7]: it is a professional obligation to pro-actively assess, reflect upon and address a larger problem for the welfare of society. The two key stages of this approach are to asses and reflect upon the challenges, before a directed and effective solutions can be obtained.

This paper places the spoofing threat into context, such that directed anti-spoofing methods can be selected via Pareto analysis in receiver design [8]. Pareto analysis focuses on the most significant issues first, to eliminate the majority of problems efficiently. The more the threat is understood, the better applicable preventative methods can be developed, according to the principles of adaptive engineering. To empower that, spoofing from an attack point of view is discussed. From this perspective, it enables understanding what the natural limits are and highlights which counter methods are required. Spoofing attack types, methods and strategies have different performances, requirements, countering potentials and success rates. However, all these attacks are often grouped together when discussed — resulting in confusion when addressing the topic of spoofing. This is most evident in the media exaggeration that a vehicle can be completely controlled [9], [10].

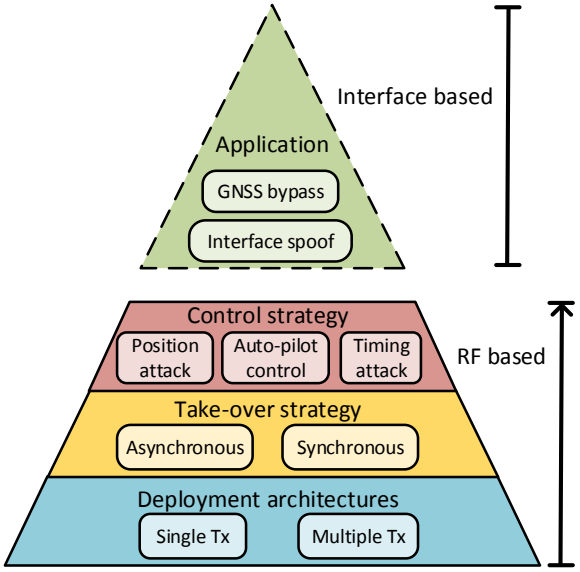


Fig. 1. Spoofing classification layers

An holistic approach is taken, from the equipment selection all the way through to the strategic advantages of a falsified PVT solution. The spoofing attacks are classified into four layers (similar to the open systems interconnection (OSI) model), as illustrated in Fig. 1.

At the base, the deployment of the transmitters for the spoofing attack is considered. This includes how many transmitters are used and where they are spatially deployed. The second level is the take-over strategy, i.e. how the spoofer

can force a receiver to lock onto the fake signal. This is also called the take-over. Once a receiver is captured (level three), the strategic goal of the spoofer determines how the PVT solution will be manipulated, i.e. the control strategy. These three layers are connected as they form part of the design for a radio frequency (RF) based attack. To simplify the interaction between these three levels, the following three questions are raised: "*Where does the attacker install the antennas?*", "*How does the attacker intent to capture the receiver?*", and "*What does the attacker intent to do if successful?*". If the final system can be spoofed without transmitting a signal (i.e. the GNSS module is bypassed or falsified), an application level spoofer is used (level four).

The contribution of this paper is twofold. First, classification of spoofer attacks through a layered model (as presented by Fig. 1), is used to place current spoofing attack types, within the literature, into context. Second, the theory behind the control strategies is expanded, including the differences between position attacks and attacks which aim to control an autonomous system.

Different single- and multi-transmitter deployment strategies are discussed in Section II. The signal generation required for takeover and control of a spoofer is examined in Section III. Assuming a successful take-over of a receiver, the manipulation of the position and auto-pilot based attacks are assessed in Section IV. Attacks based on timing are discussed in Section V. Network and application level attacks are assessed in Section VI.

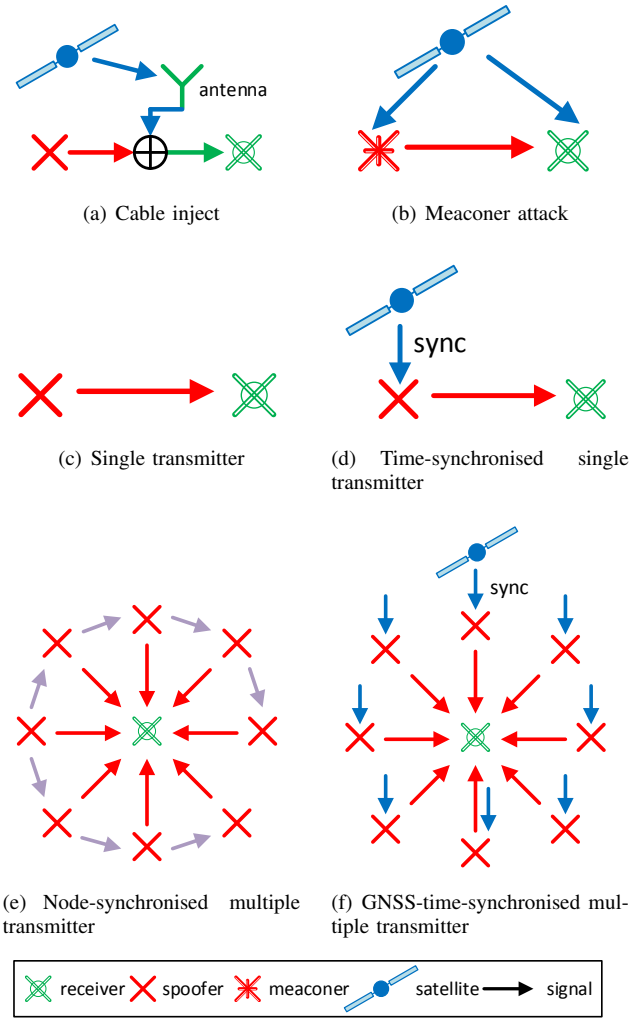
II. Deployment Architectures

The operational deployment of a spoofer in the field determines the spatial performance of the spoofer and the spatial mitigation capability of a receiver. As a spoofer transmits an electromagnetic (EM) signal, all receivers which operate in the spectrum of the same geographical region will be affected[1]. If a single target is required to be spoofed, then highly directional antennas should be used to limit unnecessary spatial interference in other directions. If a larger area around the spoofer should be affected, then omni-directional antennas can be considered. However, it should be kept in mind that a larger area can unnecessarily be affected. The terrain should also be considered when selecting the deployment locations.

GNSS signals have low reception power (approximately -155 dBW) due to the high propagation losses from the satellites to the earth; hence, a spoofer does not require much transmission power. A good strategy is to transmit the minimum necessary power to achieve operational success, as this naturally limits the area of effect (AOE). Through the use of multiple synchronised spoofers, the transmission power can also be reduced, because multiple signals can constructively interfere to create a stronger signal at specific areas.

[1]Transmitting a signal in spectrum which is not allocated to the user is illegal. Before deploying any system, adequate permission from the local governing authority is required. Using a spoofer in the GNSS frequency bands is, unless permission is granted, illegal, and therefore not encouraged by the authors.

The physical deployment strategies of a spoofer system are shown in Fig. 2: red crosses represent locations of spoofers; red arrows are the transmission of the spoofing signals; the location of the target receiver is marked with a green cross; the actual GNSS signals are shown with blue arrows; and links between spoofers are shown with purple ones.



(a) Cable inject (b) Meaconer attack

(c) Single transmitter (d) Time-synchronised single transmitter

(e) Node-synchronised multiple transmitter (f) GNSS-time-synchronised multiple transmitter

Fig. 2. Comparison of physical configuration for spoofing attacks

The method requiring the least hardware is a *cable inject* [5], as shown in Fig. 2(a). In this case, the spoofer does not require a signal to be transmitted, as the signal is combined with the receiver hardware. This is a common occurrence for a cooperative spoofing attack, where the attacker chooses to manipulate his own hardware. Such an attack occurs when a spoofer is indented to misreport or camouflage the location of a vehicle or a vessel.

Conceptually, the simplest spoofing attack is a *meaconer* (Fig. 2(b)). A meaconer simply re-transmits received GNSS signals. Therefore, the receiver PVT will be equal to the transmitter PVT, with an added time delay. Such an attack is simple, cheap and requires only a re-transmission of the

GNSS signals. An inherent property of a meaconer is that even encrypted GNSS signals can be affected, and all receiver effects will be captured in the spoofing signal. The shortcoming is that there is limited manipulation capability of the victim receiver's PVT, since the only manipulation opportunity is to physically move the meaconer to the desired PVT. Further, the time delay can result in a receiver detecting the spoofed signal. This is due to the time divergence from the trusted time, or the fact that there are multipath components before the main peak: the line of sight (LOS) signal is always the first received signal and all multipath signals should come after a time-delay. As a meaconer has to receive and transmit, some coupling and self-interference issues exist, resulting in practical deployment challenges. An advanced meaconer can use an array of antennas, to isolate different satellites spatially, and then replay the signals with different delays. This allows the PVT to be altered and changed — in principle, even for encrypted signals.

A *single transmitter* is the simplest non-repeating spoofer deployment (Fig. 2(c)), as limited hardware and synchronisation is required. The spoofer can do a *time-synchronisation* to the GNSS signal (Fig. 2(d)), to improve certain spoofing attacks, like a synchronous take-over. This will be discussed in more detail in Section III.

A limiting factor of a single spoofer is that all signals have the same angle of arrival (AOA). Therefore, the receiver can use spatial filtering, like null-steering, to remove the spoofed signals. This spoofing can also be detected by monitoring the carrier-phase in a moving receiver, as all signals will behave in the same manner [11]. The receiver can also detect a spoofer, by estimating the AOAs through direction finding (DF) techniques. The GNSS satellites tend to be scattered, and will have different AOAs; as opposed to the spoofing signals, where all will have the same AOAs. The drawback for the receiver, is that either a moving antenna, multiple antennas or an integrated navigation system (INS) is required — in all cases the cost and complexity of the receiver increases.

Multiple transmitters potentially alter the AOAs of the spoofed signals (Fig. 2(e) and II). Usually, the more transmitters there are, the more precise the AOAs can be altered. As the GNSS signals originate from any positive elevation angle, a three dimensional (3-D) transmitter deployment scheme would be required to fully deceive a receiver.

The transmitter nodes could be synchronised such that the PVT solution of the receiver can be manipulated. The simplest method to achieve this, would be to have one *master node* (transmitter) that time-synchronises the other (slave) nodes (Fig. 2(e)). This is often impractical as the transmitters should be connected via some medium, whether it is a cable, radio or optical link. The cost of the infrastructure and calibration is challenging in such systems. An elegant solution would be to use *GNSS timing* to synchronise the nodes (Fig. II); however, some interference is expected as each node requires a transmitter and a receiver.

If the transmitters surround the target, the transmission beams may constructively interfere at a single location, thereby achieving surgical spoofing[2]. As a consequence, lower transmission power is required, therefore, the AOE is reduced. This requires a high level of synchronisation (taking into account the receiver's carrier-phases) and accurate target tracking to function, making it improbable. Given the fact that a receiver may have spatial filtering capabilities, this method is less effective against a high performance receiver.

III. Signal generation

This section discusses the different spoofing attacks from a signal design perspective. To achieve spoofing, a signal which is similar to the expected GNSS signals, would be generated. A GNSS signal has three levels which are vulnerable to spoofing [2]:

1) **Signal processing level**: The specifications related to the signal polarisation, modulation type, carrier frequency, signal bandwidth, pseudo random noise (PRN) sequences, reception power and Doppler frequency-range are published for most GNSS signals. A spoofer has to replicate these specifications in order to capture a receiver.
2) **Data bit level**: The data bits of the navigation message follow a defined frame-structure. This structure is also published for most GNSS signals. The navigation message contains the almanac, satellite ephemeris, telemetry information, time and authentication keys (if any). Authentication methods at this level have been suggested, as means to verify that the received message originates from a licit service provider [12]. The navigation message could be implemented by the spoofer such that the receiver would trust the signal. Further, the navigation message provides the necessary information to compute the PVT solution.
3) **Navigation and position solution level**: The pseudoranges of the associated satellite could be manipulated by altering the time-offsets of a signal. Consequently the PVT of the receiver would also be manipulated. If the resultant PVT is not valid, then the spoofer can be detected. Therefore, a spoofer could adequately alter the pseudoranges for the desired PVT.

The more thorough and realistic the spoofing signal is generated, the higher the likelihood is that the spoofing attack will be successful and that the spoofer will be trusted. Inversely, to detect a spoofer signal, all of these layers should be checked. Here are some examples of what can be checked:

- Are the signals received at an abnormally high power?
- Are different signals from the same system received (e.g. is L1 C/A and L2-C receivable)?
- Is the bandwidth and centre frequencies of the signals as expected?
- Do the signals have similar Doppler and carrier-phase movements?

[2]Surgical spoofing is similar to surgical jamming, where only a limited (small) geographical area within a larger space is affected by the attack. It is based on the interference between signals, but is not easy to achieve in a real-world scenario.

- Is there a sudden jump in the time?
- Are all signals with the correct bandwidths present in the spectrum?
- Are some information of the navigation message missing?
- Are atmospheric effects present between two frequency bands?
- Did the almanac and satellite ephemeris information suddenly change from previously stored values?
- Does the navigation message differ from any assistance data?
- Does the PVT solution suddenly jump or move irrationally?
- If the system uses authentication keys: are they authentic?

If a receiver is capable of using multiple signals or multiple frequency bands, then all of the applicable signals are required to be spoofed to ensure a take-over. If only a subset of the signals are spoofed, then the receiver can receive contrasting pseudoranges which result in an ambiguous PVT solution — in many cases the receiver is unable to generate a PVT.

Signal design is the first line of defence against a spoofer, and is considered a preventative measure. The use of encrypted signals (e.g. GPS M-Code or Galileo public regulated service (PRS)) [13], or signal authentication methods such as navigation message authentication (NMA) [14], are strong ways to validate the received signal. Adding unpredictable features, making the navigation messages non-deterministic, further complicates the spoofer design.

One-way keychain based NMA schemes, such as Time Efficient Stream Loss-tolerant Authentication (TESLA), have the highest acceptance and solve the issue of NMA [15]. With a planned start in 2019, TESLA based Open Service Navigation Message Authentication (OS-NMA) is to be broadcast as a part of the Galileo satellite navigation system's integrity navigation message (INAV). Thereby providing message level authentication to a broad user segment. The implementation of the OS-NMA does not require any hardware modifications as it is purely message-level based protocol. Therefore, it could be implemented in most GNSS receivers with minimal software or firmware updates [16]. NMA is a strong spoofing counter measure and should be considered for receiver design.

A. Asynchronous spoofing attacks

An asynchronous spoofing attack (also known as a power-take-over or hard-take-over) transmits a non-time-synchronised signal. Time-synchronisation would imply that the correlation peak of the spoofed signal is within the tracking window of the receiver. Consequently, an asynchronous attack is often rejected by the tracking channels, as the time and Doppler offsets are likely incorrect. This attack is defined as *spoofing by non-coherent superposition* by Günther [5], and a *GPS signal simulator* attack by Montgomery et al. [17], [2]. To successfully perform such an attack, the spoofing signal would generate a higher power at the receiver than the GNSS signals. This causes the tracking stage of the receiver to fail and the receiver to try to re-acquire the signals. The increment of power makes this attack simple to detect — e.g. by using the automatic gain control (AGC) stage of the receiver.

If a satellite is not yet acquired or if a tracking channel has lost lock and is attempting to re-acquire the signal, then the higher power will most likely cause the acquisition to be on the spoofed correlation peak. If a satellite is already in track, then the tracking channel could get broken. This could either be achieved by transmitting significantly higher power, such that the correlation noise exceeds the correct correlation peak, or by utilising a jammer [18].

An asynchronous attack does not require the target receiver position to be known, and is therefore considered a brute-force attack. In some cases the use of a warm – or hot start for the acquisition may still allow the lock onto the correct GNSS signal. The limitations include the following: the higher power or jamming signal is detectable, a jump in the PVT is observed, it may come to the partial success (i.e. not all satellites are successfully spoofed) that would result in an erroneous PVT. Many of these limits result in simple detection of the spoofing attack.

Meaconing and replay based attacks are considered asynchronous, as an additional time delay between the actual signals and the replayed signals exist. This delay is caused by the processing latency of the replayer, as well as the travel time between the meaconer and the target receiver. Although a meaconing tends to be a simple replay, some more advanced methods exist. If the message symbols are unpredictable, then a security code estimation and replay (SCER) attack could be carried out in estimating them [13]. This requires a replayer to estimate the signal, before alterations to the signal can be made. Isolating signals before adding individual time delays would also have to be achieved. In this case a meaconer can be classified as a synchronous attack.

B. Synchronous spoofing attacks

Synchronous spoofing attacks (also known as a smooth-take-over or a soft-take-over) transmit spoofing signals which have overlapping correlation peaks. To achieve this, the spoofer would have some information about the location of the receiver. Just by time-synchronised transmission at increased power relative to the actual GNSS signals, the receiver would most likely lock onto the spoofer. This could improve the stealthiness of the attack, when the spoofer starts with low power, and then gradually increases it until lock of the receiver is achieved. This change in power could be estimated by the spoofer, or be compared to the received power with a co-operative receiver.

This attack is defined as *spoofing by coherent superposition* by Günther [5]. To achieve synchronisation, the spoofer would most likely require a GNSS receiver as a reference. As such, Humphreys et al. [19], [2] classifies this as a *receiver-based spoofer*. If a multi-antenna configuration is used, this attack is classified as a *sophisticated receiver-based spoofer* by Ledvina et al. [20], [2].

These methods control the take-over and are less likely to be detected by the receiver. No jamming or high power

transmission is required for these methods, hence the impact on other GNSS receivers can be minimised. Each satellite in the constellation, the spoofer location, the position of the target receiver and the positions of all other receivers influence this attack. If the time difference or the Doppler difference between the spoofed signal and a GNSS signal is sufficiently high at a non-target receiver, then the tracking channels will naturally suppress the presence of the spoofing signal.

The impediment is that the position of the receiver and all applicable delays have to be known. As a consequence, the receiver location has to be tracked, using additional sensors like radar, sonar, lidar, optical, etc. or be co-located. This increases the design complexity and cost of the system. The performance of the tracking is an additional source of system degradation.

If the position is not known, the position could be guessed, but this would have a doubtful probability of success [21]. None the less, it could be attempted.

The improved stealthiness and theoretical performance of these spoofing attacks are therefore subject to the complexity associated with them. In many cases, these type of attacks are impractical and difficult to achieve.

A variation of synchronous spoofing attacks is to "null" the GNSS signals. This is done by transmitting a signal which is equal to the GNSS signal, but phase-inverted at the target receiver relative to the GNSS signal. The nulling-signal will destructively interfere (cancel out) the GNSS signal. As the GNSS signal is no longer visible to the target receiver, a spoofing signal can simply and uncontested take-over the receiver.

This attack would require that the nulling-signal is exactly phase inverted and amplitude matched to the correct signal, thereby making this attack even more difficult to achieve than a basic synchronous attack [4]. Experimental results have found that the calibration requirements of this attack are difficult to achieve. Theoretically, this attack should have superior performance to a basic synchronous attack, if it is successful.

IV. Position altering strategies

In this section it is assumed that the spoofing attack is successful. The strategies to manipulate the PVT data of the receiver in different scenarios are theoretically analysed. The high level manipulation of the receiver position is considered.

Once a spoofer has captured the lock of the receiver, it can manipulate the signals such that the receiver has the incorrect time or position. The change in position and time would not be done abruptly, as this would cause the receiver to loose lock or to detect that the signals are false. Therefore, the spoofer signals would change in such a way that the receiver believes that the signal is real. As an example, if the spoofed position moves faster than what is physically possible by a vehicle on which the receiver is mounted, then it is easily detectable. Therefore, in all of the attacks described in this section, the physical limitations of the receiver would be considered.

A. No auto-pilot capability

Diagrams of the position based attacks are shown in Fig. 3. Each diagram has three lines: the blue line is the physical position of the receiver over time; the red line the spoofed position; and the green the perceived position of the spoofer. Note that the green line is drawn at an offset to ease the display of the scenarios. The arrows indicate the movement direction. A dot indicates the starting point (e.g. 3(b)), or a discrete change in direction (e.g. 3(h)). Circles indicate that a position is stationary (e.g. 3(b)), or becomes stationary ((e.g. 3(e)). Lastly, a circle with a dotted line represents a jump in position (e.g. 3(a)).

An asynchronous attack does not know the position of the receiver, hence the spoofer would start at an arbitrary location relative to the receiver's position. If the attack is successful, then the perceived location of the receiver will "jump" to the new location, as shown in Fig. 3(a). This is a common attack and has been demonstrated a number of times [22].

If the receiver is stationary, and a synchronous spoofing take-over moves the perceived location away, then a *static pull-off* is achieved (Fig. 3(b)). In the reversed scenario, the spoofer stays stationary, while the receiver moves away (Fig. 3(c)). This is a *static lock*. These two methods are simple dynamic attacks.

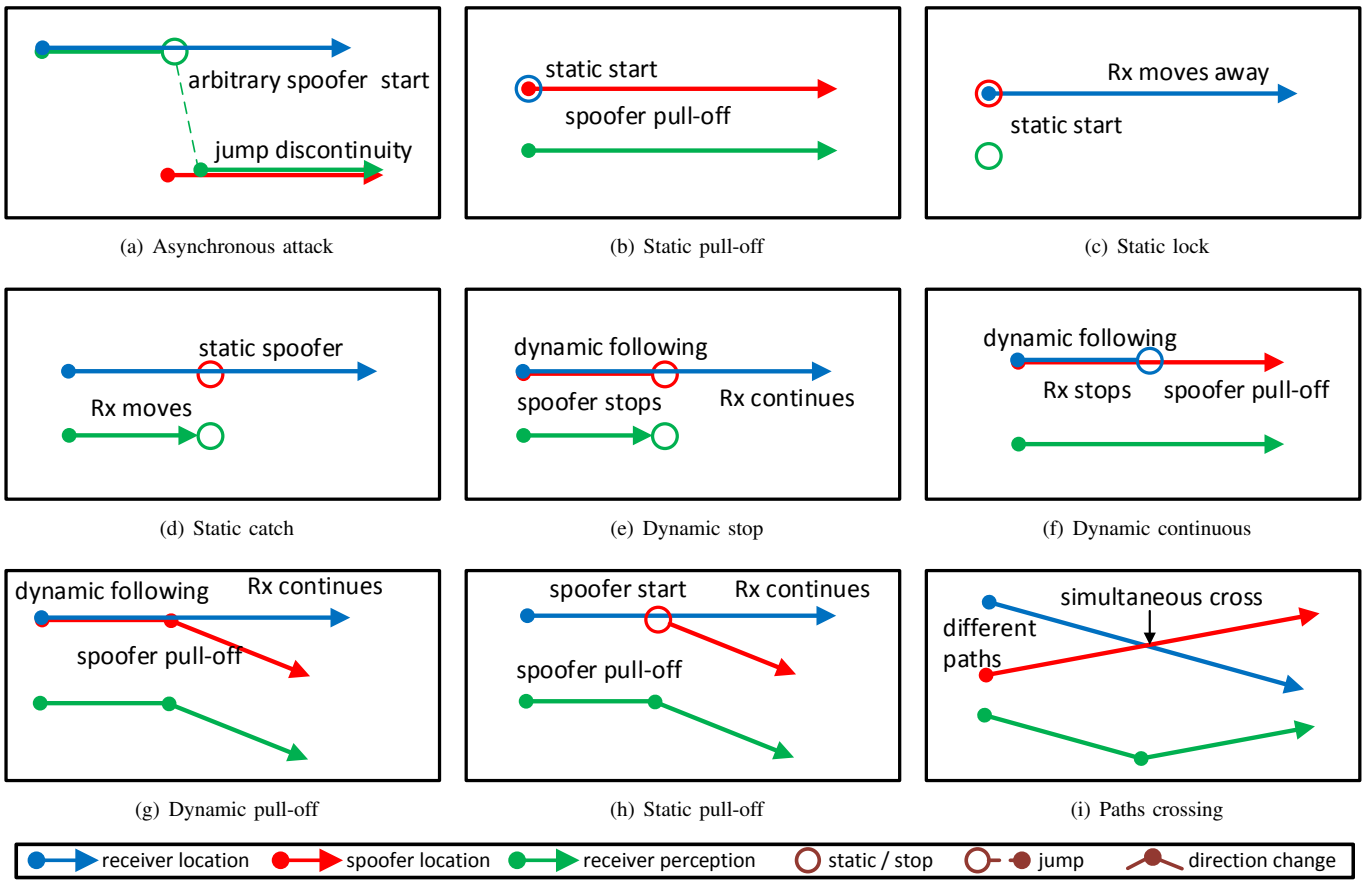
If a spoofer has a static location, and the receiver happens to move over the said location, the perceived receiver location can be halted. Fig. 3(d) shows the *static catch* example. This is unlikely to occur in practical systems. This strategy would be improved if the spoofer initially follows the receiver before halting, and causing a *dynamic stop* (Fig. 3(e)). This method would also allow more time to achieve the take-over. In the opposite scenario, the spoofer stops while the receiver persists in a *dynamic continue* (Fig. 3(f)).

If the spoofer moves initially with the receiver, then at a certain time it pulls away into a different direction, a *dynamic pull-off* is achieved (Fig. 3(g)). This is what is traditionally regarded as a spoofing attack. However, note that the spoofer does not change the physical position of the target receiver, only the perceived location. A more difficult version of this attack is similar to the static-catch, but where the spoofer immediately changes position once the receiver is caught (Fig. 3(h)). With this strategy, the *static pull-off*, is difficult to achieve, as there is little time to do the take-over.

Lastly, if a spoofer and the receiver cross paths at the same time, then it is possible to catch the receiver on the transition stage (Fig. 3(i)). This *paths crossing* scenario is highly unlikely, and, therefore, considered improbable to achieve.

B. Auto-pilot capability

In theory, a spoofed signal can control a vehicle. This is often cited as the worst case scenario for an autonomous vehicle, as it causes control-loss of the vehicle. In practice this is not necessarily the case. Through the use of sensor fusion with other navigational systems (including accelerometers, gyroscopes, inertial measurement unit (IMU), radar, lidar, optical tracking, sonar, altimeters, odometers, optical-navigation,



(a) Asynchronous attack (b) Static pull-off (c) Static lock

(d) Static catch (e) Dynamic stop (f) Dynamic continuous

(g) Dynamic pull-off (h) Static pull-off (i) Paths crossing

Fig. 3. Comparison of position attacks

compass, radio-telemetry, radio-navigation and magnetic navigation), the autonomous vehicle can potentially disregard the spoofed position and continue with valid navigation.

Further, to change the physical position of the receiver, the spoofer should move inversely. For example, if the vehicle should accelerate, then the spoofed position should move slower. The speed control system of the vehicle will then try to keep the required speed and accelerate the vehicle[3]. This means that to successfully control an autonomous vehicle,

1) the position of the target receiver would have to be known,
2) the auto-pilot path would have to be known,
3) any control systems of the target would have to be known and modelled, and
4) the influence of other sensors would have to be limited.

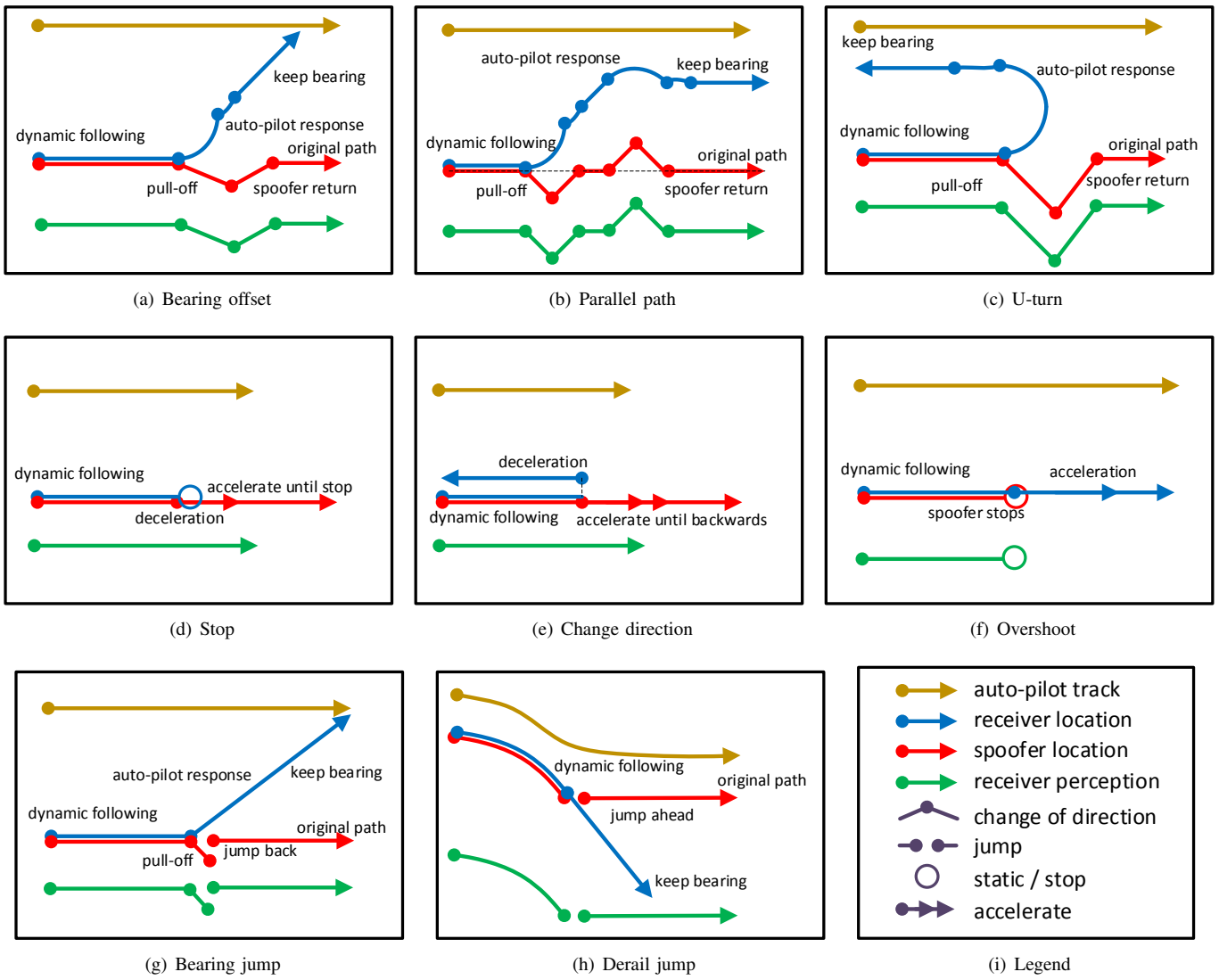
If correct security precautions are implemented (e.g. keeping the control system a black box or not revealing the auto-pilot path), then it is possible to counter this type of attack. This illustrates the difficulty to achieve an autonomous vehicle "high-jack". Despite this difficulty, there are some reports of success in the literature — almost all of them in controlled environments [23], [24].

For the remainder of this section, it is assumed that an auto-pilot based attack is achieved as the receiver completely trusts only the GNSS receiver location. Based on this assumption, the strategies on how to manipulate the PVT are considered and presented in the remainder of this section. Diagrams of auto-pilot based attacks are shown in Fig. 4.

Each diagram has four lines: the blue the physical position of the receiver over time; the red the spoofed position; the green the perceived position of the spoofer; and the yellow the path the auto-pilot is programmed to follow. Note that the yellow (above) and green (below) lines are drawn at an offset to ease the display of the scenarios.

The simplest attack against an auto-pilot would be a *bearing offset* (Fig. 4(a)). This is the attack which is displayed in the famous "high-seas" trials [24]. The spoofer starts synchronised with the receiver position. At a point the spoofer slowly drifts to one direction. The auto-pilot will notice that the vehicle is off-course and will steer in the opposite direction. Note that the longer the spoofer drifts off-course the more aggressive the auto-pilot will respond, as the error according to the auto-pilot is increasing. This results that the receiver path and the spoofer path are not mirrors of each other, and consequently the auto-

[3]In this example an odometer will most likely overwrite the speed control system, rather than the GNSS receiver. Thereby also illustrating the sensor fusion argument.



(a) Bearing offset (b) Parallel path (c) U-turn

(d) Stop (e) Change direction (f) Overshoot

(g) Bearing jump (h) Derail jump (i) Legend

Fig. 4. Comparison of auto-pilot based attacks

pilot with the dynamics of the vehicle under attack needs to be accounted for and modelled in advance in a specific attack. After some time, the spoofer would return to the path of the auto-pilot, the auto-pilot would respond by staying on the course it is currently on. As a result the vehicle would move with a bearing offset (different direction).

If two successive bearing offsets are carried out, equal in size but in opposite directions, then a *parallel path* could be created (Fig. 4(b)). Hence the vehicle would move in the same direction, but with an offset of the track. The time between the two manoeuvres, would determine how large the offset will be.

Alternatively, if the bearing offset is timed correctly, it would be possible to reverse the direction of the vehicle in a *U-turn* (Fig. 4(c)). It should be noted that the vehicle would move back on an offset.

The speed of the vehicle could also be altered. If the spoofer and the receiver are moving together, and the spoofer starts to accelerate, then the auto-pilot would start to decrease the speed until the vehicle *stops* completely (Fig. 4(d)). At this point the spoofer would proceed to move on the correct path. If the vehicle is capable of dual-direction moving, then the same principle could be applied to force the vehicle to *change direction* (Fig. 4(e)). The opposite method would be to decelerate or stop the spoofer, hence the speed-control system would start to accelerate and *overshoot* its target location (Fig. 4(f)).

If the spoofer moves with the receiver and then drifts away (similar to the bearing offset), but then "jumps" back to the correct location, then a smoother bearing offset could be achieved (Fig. 4(g)). This *bearing jump* is simpler to predict the final bearing, but risks loosing lock of the receiver or to be detected. Similarly, if the auto-pilot follows a complex path, it is possible to just skip ahead during a manoeuvre of the auto-pilot, thereby fooling location of the auto-pilot on the pre-determined path (Fig. 4(h)). This would cause a natural

change of bearing, and is called a *derail jump*.

As seen from the different strategies, it is evident that even if the spoofing take-over was successful, and if no other navigational aids were used by the auto-pilot, it would still be a difficult and tedious task to try to control the auto-pilot. Knowledge of the vehicle, control systems used and the auto-pilot path would be required, and complex manoeuvres with many limitations would have to be made to enable position manipulation. This shows that full vehicular manipulation is highly improbable. Further, if the correct precautions are taken, then the control of a vehicle can be denied to a spoofer control. Considering all these effects, only an unprotected or co-operative vehicle will be susceptible to a spoofer control attack.

V. Timing and information altering attacks

This section evaluates how the timing and symbol decoding of a receiver could be manipulated using a spoofer. Many systems rely on GNSS timing for operation [25]. If a spoofer attacks a stationary target — like a measurement station — there is little to be gained by spoofing the position. One option would be to have the correct position for the spoofing signals, and add the same *pseudorange ramp* to each signals. As a result the position would remain constant, but the time changes. This would cause timing instabilities in the system. Alternatively, a *pseudorange jitter* could be applied for small-scale timing instabilities. A side effect is that the positioning precision would be reduced. A controlled version of this attack is to create a *position jitter*, where the jitter of the pseudoranges is an inter-dependant process. Lastly, the pseudoranges could also be made unstable and jitter through the addition of a *jammer*; however, this would be a relatively small jitter error and will be easy to detect. Strictly per the definition, this method should not be considered as a spoofer attack, even though the intent is to alter the timing of the receiver.

The spoofer could also transmit a signal which has the same properties as the actual GNSS signal, with the only difference being that the information encoded onto the signal is altered. This could be done to create fake navigation messages of the satellites, which are interpreted by the receiver. Falsifying the ephemeris data to cause poor PVT solutions or to alter the position is possible, but it is not simple to achieve. Altering the time or other data in the messages could also influence the receiver. Such an attack is considered an information based attack, as the information of the GNSS signals is altered. As such, this type of attack is more associated with IW. NMA could provide an effective way to avoid such type of attacks.

The attacks discussed in this section are rarely reported, but they can have the impact on a receiver. The strategic gain of these attacks is low, especially considering the effort needed to achieve the attack. It can therefore be concluded that timing based attacks are currently considered as a low priority to develop anti-spoofing methods for, and jeopardize the correct operation of the system minimally.

VI. Application and network level attacks

In many cases, the PVT of a receiver can be altered after the PVT has been calculated. It can be performed to overwrite the GNSS interface of an integrated system with the desired data. Such an attack has the property of only affecting the targeted system, and does not require spoofing EM signals to be transmitted. Therefore, only a single targeted device could be attacked. In many cases the user aims to spoof his own device.

To achieve this, the communication between the GNSS localisation module and the application requiring a location could be intercepted, falsified and attacked. This could be carried out on hardware level [26] where a GNSS module is bypassed and replaced with a GNSS module emulator; or on software level where the data-interface is hacked [27]. The restriction of this method is that it is a network or application level based attack, hence, an understanding of the target device's interfaces is required.

As an example, the location of a smart-phone could be hacked such that targeted application has a false position. This has been used to cheat on location based games such as *Pokemon-GO!*.

It could also be possible to spoof correction data, like the real time correction message (RTCM) or ionospheric correction data. This would be a correction-based spoofing attack and is aimed to reduce the PVT accuracy.

VII. Conclusion

This paper presents a layered classification of spoofing attacks, to broaden the understanding on the types of attacks that are possible and evaluate the spoofer probability. The classifications include the deployment architectures (physical locations), signal generation, position altering strategies, timing and information altering strategies and application and network level attacks.

Viewing the attack from a spoofer's point of view, the strategic value of the attacks are exposed. This allows the identification and targeted design of preventative measures to counter spoofing. This follows the principle of adaptive engineering — as reflecting upon the spoofer-attack allows countering solutions to become evident. The low strategic value of some attacks (e.g. pseudorange jitter), can thereby be disregarded as a threat and consequently be ignored in receiver hardening design. On the contrary, attacks with high strategic value should be addressed with high priority.

It is found that many of the spoofing types are difficult, impractical and too complex to achieve, or only achievable in specific circumstances (e.g. auto-pilot based attack). Therefore, it can be concluded that these types of attacks are currently not a viable threat. In such cases, the development of anti-spoofing methods are not as crucial; however, it is possible that with the advancement of technology the *status quo* will change. If this is the case, preventative development for future threats is needed.

Some attacks present a clear threat and need to be addressed and considered in receiver design, for example an

asynchronous attack. The recent development of NMA algorithms allows the authentication of signals, and is therefore an effective system feature to counter spoofing attacks. A multi-system, multi-signal approach provides a good counter measure to spoofing, as it is unlikely that all signals are spoofed simultaneously (this forces the spoofer to be more complex). As it is costly to have a multi-transmitter spoofer, it is advised to use a multi-antenna receiver with AOA verification and with spatial filtering, Lastly, integrating different sensors (e.g. IMUs, proximity detectors, radar, cellular-positioning, active transponders, etc.) will also reduce the impact of a spoofing attack.

Understanding the spoofers goals and strategies allows the spoofer threat to be exposed. Therefore, the directed and efficient counter measures can be developed for the greater well-being of society. Spoofing threats should not be underestimated and the already available anti-spoofing methods, should be implemented on a broader scale.

REFERENCES

[1] John A. Volpe National Transportation Systems, "Vulnerability assessment of the transport infrastructure relying on the global positioning system," *U.S. DoT*, 2001.

[2] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, vol. 2012, pp. 1–16, 2012.

[3] C. M. Pereira, J. Rastegar, C. E. McLain, T. Alanson, C. McMullan, and H. L. Nguyen, "Countering gps jamming and ew threat," 2007.

[4] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, June 2016.

[5] C. Günther, "A Survey of Spoofing and Counter-Measures," *Navigation*, vol. 61, no. 3, pp. 159–177, 2014.

[6] A. Rügamer and D. Kowalewski, "Jamming and Spoofing of GNSS Signals ? An Underestimated Risk?!" in *Proceddings, FIG Working Week 2015, May 17 - 21, 2015, Sofia, Bulgaria*, 2015.

[7] J. VanderSteen, "Adaptive engineering," *Bulletin of Science, Technology & Society*, vol. 31, no. 2, pp. 134–143, 2011.

[8] P. Ngatchou, A. Zarei, and A. El-Sharkawi, "Pareto multi objective optimization," in *Proceedings of the 13th International Conference on, Intelligent Systems Application to Power Systems*, Nov 2005, pp. 84–91.

[9] M. Darwish. (2017) Did Russia make this ship disappear? [Online]. Available: http://money.cnn.com/2017/11/03/technology/gps-spoofing-russia/index.html

[10] D. Goward. (2017) GPS spoofing incident points to fragility of navigation satellites. [Online]. Available: http://www.nationaldefensemagazine.org/articles/2017/8/22/viewpoint-gps-spoofing-incident-points-to-fragility-of-navigation-satellites

[11] M. Psiaki, S. Powell, and B. O'Hanlon, "Gnss spoofing detection using high-frequency antenna motion and carrier-phase data," in *Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013)*, 2013.

[12] G. Caparra, "Navigation message authentication schemes," *InsideGNSS*, October 2016.

[13] T. E. Humphreys, "Detection Strategy for Cryptographic GNSS Anti-Spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073–1090, APRIL 2013.

[14] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, "A blueprint for civil GPS navigation message authentication," in *2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*, May 2014, pp. 262–269.

[15] G. Caparra, "Evaluating the security of one-way key chains in tesla-based gnss navigation message authentication schemes," *2016 International Conference on Localization and GNSS (ICL-GNSS) in Barcelona*, 2016.

[16] X. Zubizarreta, "Assesment of galileo open service navigation message authentication," Master's thesis, 2017.

[17] P. Y Montgomery, T. E Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil gps spoofer," vol. 1, pp. 124–130, 01 2009.

[18] R. H. Mitch, R. C. Dougherty, M. L. Psiaki, S. P. Powell, B. W. O'Hanlona, J. A. Bhatti, and T. E. Humphreys, "Signal characteristics of civil gps jammers," in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, 2011.

[19] T. E. Humphreys, B. M. Ledvina, M. Psiaki, B. W. O'Hanlon, and J. P. M. Kintner, "Assessing the spoofing threat: Development of a portable gps civilian spoofer," pp. 2314–2325, 01 2008.

[20] B. Ledvina, W. Bencze, B. Galusha, and I. Miller, "An in-line anti-spoofing device for legacy civil gps receivers," pp. 698–712, 01 2010.

[21] N. O. Tippenhauer and C. Popper, "On the requirements for successful gps spoofing attacks," in *CCS '11 Proceedings of the 18th ACM conference on Computer and communications security*. Elsevier, 2000.

[22] W. De Wilde, J. Van Hees, G. Cuypers, J. Dumon, J.-M. Sleewaegen, and B. Bougard, "Spoofing threats: Reality check, impact and cure," in *Proceedings of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017)*, 2017, pp. 1289–1327.

[23] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned Aircraft Capture and Control Via GPS Spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[24] J. Bhatti and T. E. Humphreys, "Hostile control of ships via false gps signals: Demonstration and detection," *Navigation*, vol. 64, no. 1, pp. 51–66, 2017, navi.183.

[25] D. P. Shepard, J. A. Bhatti, T. E. Humphreys, and A. A. Fansler, "Evaluation of smart grid and civilian uav vulnerability to gps spoo?ng attacks," in *In Proceedings of ION GNSS 2012*, 2012, pp. 3591 – 3605.

[26] O. Pozzobon, C. Wullems, and M. Detratti, "Security considerations in the design of tamper resistant gnss receivers," in *2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, Dec 2010, pp. 1–5.

[27] O. Pozzobon, C. Wullems, and K. Kubik, "Requirements for enhancing trust, security and integrity of gnss location services," in *The 60th Annual Meeting of the Institute of Navigation (ION)*. Dayton Marriott Hotel, Dayton, OH: Institute of Navigation, 2004.