Assessing the Security of a Navigation System: A Case Study using Enhanced Loran

Sherman C. Lo, *Stanford University*
Benjamin B. Peterson, *Peterson Integrated Geopositioning*
Per K. Enge, *Stanford University*

BIOGRAPHY

Sherman C. Lo is currently a senior research engineer at the Stanford University Global Positioning System (GPS) Laboratory. He is the Associate Investigator for the Stanford University efforts on the Department of Transportation's technical evaluation of Loran.

Benjamin B. Peterson served as head of the Engineering Department at the U. S. Coast Guard Academy, in New London, CT. After his retirement from the Coast Guard, he founded Peterson Integrated Geopositioning, LLC

Per K. Enge is a professor in the Department of Aeronautics and Astronautics at Stanford University. He is the director of the Stanford GPS Laboratory and the Center for Position, Navigation and Time.

1.0 INTRODUCTION

Global Navigation Satellite Systems (GNSS) has become increasingly interwoven into the fabric of our infrastructure and economic system. However, as GNSS becomes more important for safety of life and economically critical infrastructure, subversive elements will be increasingly tempted to deny or spoof its signals. The fact that GNSS has vulnerabilities is well known and it is becoming recognized that back ups to GNSS are necessary [1]. Indeed, we are hopefully moving to a more comprehensive approach to position, navigation and timing (PNT) architecture. An element that should be central to the consideration is security. This paper examines the security capabilities of Loran as a case study for examining both a secure navigation system and a secure back up to GNSS.

Loran, in particular the next generation Enhanced Loran (*eLoran*), has many properties that make it a good complement to GNSS. It has similar outputs and performance as GNSS. As it is an area navigation (RNAV) system, it can be used to drive the same interfaces as GNSS. *eLoran* is being developed to provide performance levels that can support non precision approach (NPA), harbor entrance approach (HEA), and stratum 1 frequency and precise timing. At the same time, it is an independent system and has failure modes that differ from GNSS. The attractiveness of Loran as part of a full PNT architecture has been recognized by the US Department of Homeland Security (DHS). In 2008, the DHS announced that *eLoran* will be implemented to provide "an independent national positioning, navigation and timing system that complements the Global Positioning System (GPS) in the event of an outage or disruption in service [2]." Europe has also recognized this with the General Lighthouse Authority (GLA) of England, Ireland, and Scotland also promulgating the development of *eLoran* for maritime use [3].

While having a back up implies security through redundancy, the *eLoran* system can provide even stronger security to PNT. Its characteristics make many of the attacks significantly more difficult than in GNSS. Its higher power makes it more robust to on-air attacks. The system can also incorporate signal authentication messages. In addition, its dissimilar characteristics makes attacking Loran technically different from attacking GNSS. *eLoran*, in this context, is extremely attractive as a part of a comprehensive PNT architecture.

This paper examines the capabilities of *eLoran* to enhance navigation security. It begins by addressing the various attacks that can affect navigation systems and features of the Loran system useful to resisting possible attacks. The first analysis

examines the ability of *eLoran* to resist on-air jamming and spoofing. It quantifies *eLoran*'s resistance in terms of attacker requirements. The second analysis examines techniques to increase the robustness of *eLoran* to spoofing. Finally, it examines integrating Loran and GNSS to improve overall navigation security to deliberate tampering. Accordingly, the first two analyses demonstrate the capabilities of *eLoran* in handling different jamming and spoofing attacks. The ability allows a properly designed receiver to provide trustworthy navigation outputs. The final part of the paper discusses how to use a secure output (such as from *eLoran*) with GNSS for authenticated navigation solutions.

2.0 NAVIGATION SECURITY AND LORAN

Navigation security is increasingly important for two reasons. The first is the increased adoption and integration of navigation technologies. Navigation security is needed to ensure that the PNT outputs we rely on are indeed reliable. The second is the global increase of information technology threats. Secure navigation can serve as a building block for protection of information and assets. These two distinct points can be encapsulated as "security for navigation" and "security from navigation", respectively.

This paper focuses primarily on the "security for navigation" as it should be a requirement when getting "security from navigation." To understand navigation security, it is important to under the threats and attacks that may be inflicted upon it.

This section discusses attacks and Loran characteristics that may be useful for security. It categorizes the various possible attacks and introduces common defenses. It focuses on specific Loran features and how they apply to security against attacks. More background on navigation security measures and Loran are available in literature [4][5][6].

2.1 Attack Models and Common Defenses

Attack models are useful for the assessment of system robustness and are a standard tool used by the security community. In assessing the security of a navigation system, we divide the attacks into two major categories – on-air (or over-the-air) and off-air attacks. On-air attacks are ones where the adversary attempts to compete with or overwhelm the broadcast signal. Off-air or direct injection attacks are ones where the adversary, who may be a complicit user, directly inputs into the receiver.

On-air attacks can come in several forms. One common category of GNSS attack is on-air jamming or interference. Jamming is the broadcast of radio-frequency (RF) power that interferes with a receiver's ability to track the genuine signals resulting in denial of service (DoS). Many incidences of GNSS jamming have been reported. The other category of on-air attack is broadcast spoofing where a competing signal is transmitted so that the user receiver generates an incorrect position. This threat is real and there have been anecdotal accounts of GNSS spoofing as well as an actual spoofer demonstration [7][8]. Different spoofing techniques exist. The transmission of simulated signals is one spoofing method. Spoofing techniques can also utilize the genuine broadcast signal. A simple example is relay spoofing or meaconing where the actual broadcast is received at one location and repeated at another. A more sophisticated version is to variably delay the components (signals from different transmitters) of actual broadcast and rebroadcast the signal to generate false ranges ("delay and relay" or selective delay). Another version is to modify the actual broadcast signal.

Forms of direct injection attacks are similar to those of on-air spoofing attacks. They typically need a complicit or oblivious user as they require direct access to the receiver. Given this, they are simpler to implement than on-air attacks as the spoofed signals do not need to compete with the broadcast signal.

Several defenses against these attacks are possible. A physical defense is one possibility. Strong signal broadcasts represent a physical barrier against on-air attacks as the adversary needs to overcome the power of the genuine signal. This is one advantage of Loran that will be examined in the next section. Another way to increase genuine signal power relative to an adversary is to use directional antennas. The signal power approach is really the only defense against jamming. Another example of a physical barrier is tamper-proofing. This may prevent injection attacks if the antenna and receiver represent one tamper proof unit.

A second type of defense comes from signal design and authentication. On-air spoofing effects may be detectable depending on how the spoofing is conducted. This is especially true on modulated pulses as the spoofer cannot predict the data on the pulse. The on-air attacks section discusses checks of the signal and data for countering such a spoofer. Data and navigation authentication is another area that will be examined in this paper. It basically

means providing information to check that the signal can only be generated by the genuine source. Hidden information is a second method. This is providing information that is hidden in the signal that can only be known to the genuine source. The information is later revealed so verification is possible. A related technique is the use of location dependent marker. A third defense is hidden signal, an example of which is the GPS P(Y) code. If adversaries cannot know the broadcast signal, then they cannot spoof it. Table 1 categorizes these attacks and potential defenses.

Attacks	**Physical Defense**	**Signal-Processing Based Defense**
Jamming (DoS)	Signal Power, Directional Antenna	Increasing receiver sensitivity
On-air Spoofing	Signal Power, Directional Antenna	Signal and data cross checks, Hidden (Location) Markers, Hidden Signals
Direct Inject Spoofing	Tamper Proof	Authentication, Hidden (Location) Markers, Hidden Signals

Table 1. Attack Scenarios and Defense Options

2.2 Loran Features for Security

There are many features of Loran that are useful in providing security to the signal. Foremost is its signal frequency and power. The Loran is a low frequency (LF) transmitted at a power level of 400 kW or more. At 100 kHz, the signal has a wavelength of three kilometers thus requiring a large antenna to transmit efficiently. Even a quarter wavelength antenna is physically difficult to realize. Thus, the most common Loran antenna in service is a 625 foot (190 m) top loaded monopole (TLM). Antennas as tall as 1350 feet (411.48 m) have been used. The high signal power, necessary to overcome atmospheric noise at long ranges, makes the signal more difficult to jam and spoof. For the antenna to be portable and conspicuous cannot be too large. These high power and LF features of Loran make it difficult for adversaries to set up portable, inconspicuous, over-the-air attacks. However, this means that the achievable radiated power will be orders of magnitude less than an actual Loran transmitter. As a rule of thumb, antenna efficiency is proportional to the square of the antenna height. Thus, generating an effective jamming or spoofing broadcast poses a significant challenge for over-the-air attackers. The next section quantifies the challenge.

eLoran incorporates a data channel that utilize pulse position modulation (PPM) to add data to the nominal Loran pulse. The data channel is designed to provide system information and differential Loran corrections. However, it can be used provide authentication information to validate the data and source of the signal. A version of the authentication message system has been tested [9]. In addition, the data modulation itself may be useful in detecting on-air spoofing as well be discussed later.

Another difference between Loran and GNSS is that the former shares its frequency using time division multiple access (TDMA) while the later does it using code division multiple access (CDMA). That Loran is a pulsed broadcast also has security implications. This characteristics makes it more susceptible to "delay and relay" spoofing as signals from different stations are easily separated in time. The TDMA implementation in Loran still has intrasystem interference, known as cross rate interference. This interference is location and time dependent and may be useful for cross checking measurement results.

These features likely present the most significant challenge for over-the-air attackers. This will be discussed greater detail in the next section.

3.0 ON-AIR ATTACKS

The analysis presented in this section quantifies the ability of an on-air adversary to jam or spoof the Loran signal. The section examines reasonable attack requirements and studies the relationship between jamming or spoofing effectiveness and equipment necessary. It analyzes the minimum antenna height needed to generate different levels of attack. Scenarios are presented to better illustrate the results. The last part proposes additional methods of detecting and limiting the effects of on-air spoofing of *eLoran*.

3.1 Jamming and Spoofing

Jamming a signal involves overcoming the broadcast power of the signal. A straight forward jamming broadcast is a transmission at the carrier wave frequency with roughly equal received power. Due to distance, the received Loran power is significantly less than 400 kW radiated by the transmitter. The power falls off at greater than the nominal square of the distance due to attenuation for propagation along the ground [10]. This can be seen in Figure 1 which uses the nominal groundwave model from [11]. A 400 kW (radiated power)

transmitter 300 kilometers away (which is equivalent in signal strength to the same transmitter at 500 km subject to square distance loss) is roughly equivalent to a 40 W (radiated power) transmitter 5 km away. It is also equivalent to a transmitter radiating 4 kW to a user 0.5 km away. The 300 km distance serves as a reasonable value for distance between a user and a close transmitter.

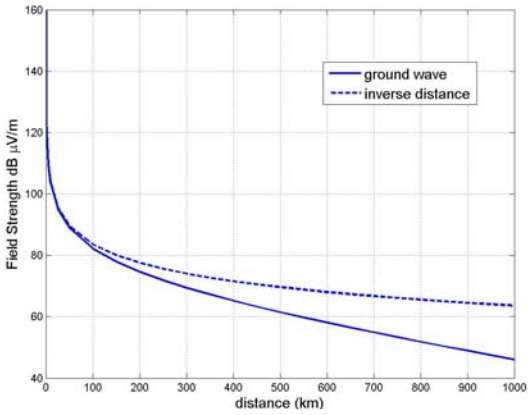

Figure 1. Loran Field Strength as a function of distance from transmitter

Spoofing a Loran signal by overcoming the transmitted signal is even more challenging than jamming. Part of the difficulty lies transmitting a Loran signal from a short, high Q, antenna. Short, high Q antennas have bandwidths that are much narrower than the signal bandwidth. Thus broadcasting a Loran signal from such antennas results in even more inefficiency than transmitting a pure tone (as may be used by jamming) [12]. As a result, these antennas are more likely to spoof by broadcasting a tonal or near tone signals. It is possible to spoof Loran with such a signal if properly designed. Additionally, the spoofing can be achieved with less power than jamming on both Loran and GNSS. Since less power is used, this form of spoofing has limits in positions spoofable. For example, assume a spoofer wants to create an error of 30 m with an antenna 5 km away from the user receiver. If the user is receiving a signal from a 400 kW transmitter that 300 km, the transmitted spoof power needed is 160 mW. To induce a larger error of 150 m from that distance, 4 W would be required. Table 2 presents these reference jamming and spoofing scenarios.

Scenario	5 km	0.5 km
Jamming	40 W	0.4 W
Spoof 30 m error	160 mW	1.6 mW
Spoof 150 m error	4 W	40 mW

Table 2. Spoofing Scenarios and Required Power

In these scenarios, no assumptions are made about the antenna available to the attacker. In the subsequent analysis, it is assumed that the antenna is a simple monopole that is reasonably short, perhaps 30 m or less. This seems like a reasonable assumption as an attacker, in order to be discrete, would either have to quickly set up an antenna or set up structure inconspicuously. This implies that the structure can not be too large or have too many elements (guy wires, etc.) to avoid detection. More likely, reasonable attacks are limited to antenna heights of 30 meters or less due to likely difficulties in covertly installing, accessing or operating larger structures.

3.2 Antenna Model

Understanding the potential of an attacker requires determining the ability to radiate power from a very short antenna. A very short antenna is one whose height is much less than the transmitted wavelength. As the Loran wavelength is 3 km, even a 100 m antenna may be considered very short! Assuming a short monopole antenna on a perfect ground plane is used, the standard radiative resistance is given by Equation 1 [13]. If radiative resistance is a governing factor alone, then radiating the power levels in the previous section would only require currents on the order of amperes or at most tens of amperes. However, the full impedance, and hence reactance, must also be considered.

$$R_r = 40\pi^2 \left(\tfrac{\mathrm{h}}{\lambda}\right)^2 \Omega \qquad (1)$$

For a very short antenna, the reactance of the antenna is mostly capacitative. Equation 2 gives the reactance of a short monopole antenna where Δz is twice the antenna height (h) and a is the wire radius [13]. A similar result can be gained from empirical derivations. Equation 3 is the capacitance from a vertical wire of length h and diameter d with k being an empirical factor related the height above ground of the low point of the wire [14]. The reactance derived from Equation 3 is seen in Equation 4 and is essentially the same as Equation 2 for wires close to the ground ($k \sim .44$).

$$X_{\mathrm{A}} = \tfrac{1}{2}\left\{\frac{-120\lambda}{\pi\Delta \mathrm{z}}\left[\ln\left(\tfrac{\Delta \mathrm{z}}{2a}\right) - 1\right]\right\}\Omega \qquad (2)$$

$$C = \frac{24.16h}{\log\left(\frac{2\mathrm{h}}{d}\right) - k} 10^{-12} F \qquad (3)$$

$$X_{\mathrm{A}} = \frac{-30\lambda}{\pi h}\left[\ln\left(\tfrac{2\mathrm{h}}{2a}\right) - \ln(10)\bullet k\right]\Omega = \frac{-1}{\omega C} \qquad (4)$$

The current flow is simply the voltage difference divided by the magnitude of the impedance. This is given in Equation 5 where R_{ohmic} (given in Equation 6) is the ohmic resistance (losses) in the antenna. For simplicity and conservativeness, the ohmic term is ignored. These equations show that voltage difference in a short antenna is effectively governed by the reactance.

$$I = \frac{V}{|Z|} = \frac{V}{\sqrt{\left(R_r + R_{ohmic}\right)^2 + X_A^{\ 2}}} \qquad (5)$$

$$R_{ohmic} = \frac{2h}{2\pi a}\frac{R_s}{3} \qquad (6)$$

From the result, the radiated power can be calculated given an assumed voltage difference and an antenna radius. It is assumed that the maximum voltage potential is 45 kV which seems like a reasonably conservative. The results for an antenna radius of 5 cm at maximum voltages of 5, 25, and 45 kV are seen in Figure 2. The results have some dependency on antenna radius with the general trend being radiated power increases with antenna diameter. Table 3 shows the antenna height needed to achieve the required radiated powers from the scenarios discussed for three different antenna radii.

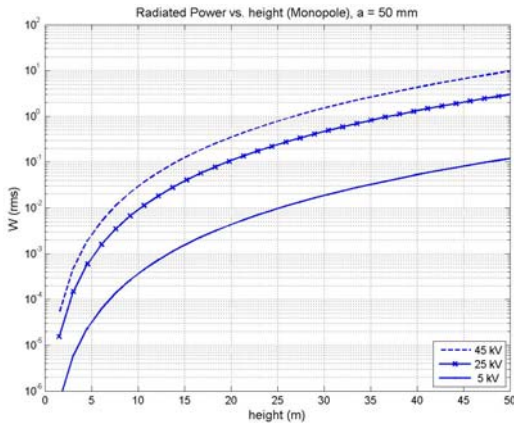

Figure 2. Radiated Power vs Monopole Antenna Height

Scenario (5 & ½ km)	a = 2.3 mm	a = 25.4 mm	a = 50 mm
Jamming (40 W, 0.4 W)	90 m, 27 m	78 m, 22 m	73 m, 21 m
Spoof 30 m error (160 mW, 1.6 mW)	21 m, 6.1 m	17 m, 4.7 m	16 m, 4.2 m
Spoof 150 m error (4 W, 40 mW)	49 m, 14 m	42 m, 12 m	39 m, 11 m

Table 3. Attack Scenarios and Required Monopole Antenna Heights for different radii (a)

The results indicate that, unless an attacker is quite close, an on-air attack would require antenna structures that are quite large - over 15 meters in the most optimistic case at 5 km. At ½ km, the antenna heights are more achievable but they will still likely be noticed if they are at that distance to the user.

Note that extrapolating the analysis out to Loran antenna heights or even mini-tower heights results in radiative power that are over an order of magnitude lower than assumed or measured. There is no discrepancy as the analysis applies specifically to very short antennas and it does not consider other factors such as top loading. As antennas get larger, the reactance is lower than suggested by Equation 2 due to inductance. In fact, measurements of an operating Loran antenna show a reactance of -25 Ω, much less than calculated by the equation [12]. It is well known that proper top loading can also improve performance. Depending on number of guy wires and location of the insulator, output power can improve by significant multiples. For example, for eight equally spaced guy wires, radiated power can be improved by over a factor of eight [15]. However, this increase comes at the expense of significant set up time and costs. This is something that an attacker is not expected to do because of their desire not to be detectable or caught.

In fact, the analysis assumptions represent an optimistic case from the attacker's perspective. It assumes away many losses such as ohmic and matching losses. It assumes no transmitter inefficiencies. It also assumes a perfect ground plane which an attacker is may not be able to approximate due to the amount of preparation needed to set this up.

3.3 Modulated Pulse Cross Check

Spoofing can be detected on modulated Loran pulses especially if its effect is large. Spoofing as described previously, affects the broadcast Loran signal by overlaying that signal. The spoofing is achieved through an overlay to signal with a known time of arrival (TOA). However, the TOA of PPM pulses are not known *a priori*. Hence, the effect of the overlay cannot be predicted. The attacker has two choices. One choice is to not spoof the PPM pulses. However, this causes all the data bits to be shifted by the amount of the spoofing. This shift can be easily detected. So to avoid detection, the attacker's must spoof the modulated signals. Since the PPM time shift is not known *a priori*, the overlay cannot be matched to individual PPM pulses. The most likely scenario is that a spoofer

overlays a tone or near tone that is in phase with the non-modulated pulses. This tone will have different effects on the PPM modulated pulses. Using 9th pulse modulation as an example, the effect of the tone on an unshifted pulse will be different than that on a pulse that is delayed 2.5 μsec. If the spoofing is too great, it will result in certain bits systematically being mistaken for other bits. This systematic error can be checked and hence the spoofer can be detected. Figure 3 shows an example of this where spoofing of 300 meters results in pulses nominally shifted 2.5 and 3.75 μsec being registered as pulses shifted by 3.75 and 5 μsec, respectively when spoofed.

An attacker can try to eliminate the systematic nature of its effect on PPM by randomly changing the synchronization of the tone on the modulated pulse. Technically, this is more difficult to achieve. Regardless of the technical challenge, this will lead to a high symbol error rate. The discrepancy can be checked by the receiver by comparing its actual error rate to expected error rate. Hence, with cross checking of modulated pulses, the maximum range error that can be induced is likely 250 m or less.

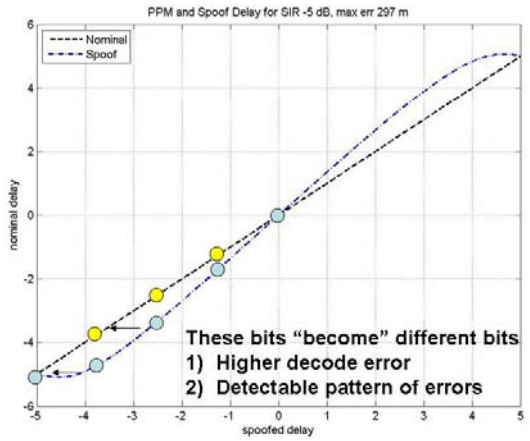

Figure 3. Actual PPM delay vs. delay with spoofing (usec)

3.4 Other Spoofing Checks

Spoofing may also leave other signatures on the signal that can be checked. One detection method is to examine multiple tracking point. A short monopole is narrowband and hence difficult to "instantaneously" turn on and off. As a result, spoofing will likely affect multiple Loran cycles. Even if the relative phase between a likely spoof signal and the Loran signal is maintained, the Loran signal envelope changes resulting in a different spoofed "error" at each tracking point. The deviation can be derived by both analysis and simulation. Figure 4 shows an example from simulation. In the figure, spoofing a 239 m error on the 30 microsec (sixth zero crossing) tracking point results in a 280 m error at the 25 microsec (5th zero crossing) and a 340 m error at the 20 microsec point.

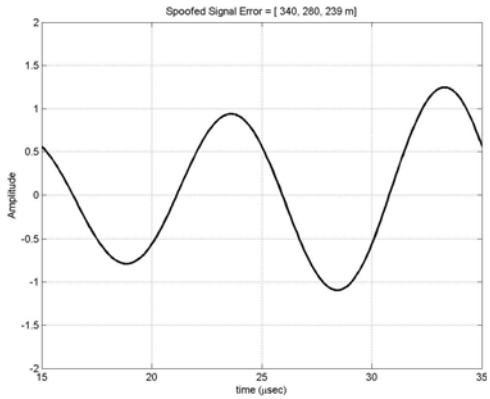

Figure 4. Effect of Spoofing on Zero Crossing Tracking Points

Another means of detecting spoofing is the use of magnetic (H) field antennas. These antennas allow for the determination of received signal direction [16]. A single, over-the-air spoofing antenna can only generate signals from one direction. Hence a receiver designed to use an H field antenna will be able to distinguish the spoofer from the true system which would have signals coming from multiple directions. Furthermore, the receiver can check the consistency of the incoming signal directions with its calculated location.

4.0 DIRECT INJECTION ATTACKS

Resistance to on-air attacks is only one form of robustness. Direct injection attacks such as when the receiver is connected to a spoofing simulator also can pose a navigation security issue. Often times such an attack comes from a complicit user with an incentive to deceive the navigation system. Examples include avoiding restricted zones or road toll charges. Such attacks circumvent the physical difficulties mentioned in the previous section. Other security features are necessary to mitigate such attacks. We are examining and developing two useful techniques for Loran to counter these attacks. These are: 1) authentication and 2) hidden markers.

4.1 Authentication

In the context of navigation, ideal authentication is the verification of both the source of the signal and that it has not been maliciously delayed. While

authentication schemes based on data or source authentication techniques have been suggested, these are designed only to provide the former. Ensuring the second is more difficult with these techniques. Still these techniques are important as they can be used with other techniques such as hidden markers to provide greater to introduced delays.

One data authentication protocol that has been suggested for navigation is Time Efficient Stream Loss-tolerant Authentication (TESLA) [17][18]. TESLA, based on symmetric key cryptography, is discussed in the next segment. TESLA has been test implemented on Loran [9]. As these protocols are made for data communication channel, some effort should be taken to better adapt them for navigation. Data efficiency is a concern as navigation systems have very low bandwidth compare to most data communications. Additionally, message loss also needs to be considered. This paper does preliminary development of modified forms of TESLA to more effectively use the bandwidth and handle loss. Creating more navigation tailored forms of authentication is currently ongoing research at Stanford.

Cryptographic signatures are another category of data authentication techniques that could be used for navigation signal authentication. Cryptographic signatures use a public-private key pair (asymmetric keys). They require distribution of a public key that is confirmed to be from the true system. In addition, these require a mechanism for revoking and redistributing public keys should a private key be compromised. When compared to a system based on symmetric keys, asymmetric systems require much more processing (multiple orders of magnitude) and longer keys. This gap can be narrowed with newer techniques such as those based on elliptic curves [19].

4.2 Basic TESLA

TESLA is a data authentication technique based on symmetric key protocols. The basic form has been described in [9][17][18] and is overviewed in this section. First, the sender creates a generator key, K_N, which is used to develop a sequence of keys using a one way hash function (H). The basic generation of this sequence is given in Equation 7.

$$K_{n-1} = H\left(K_n\right) \quad (7)$$

The base key (K_0) is the last key generated by hashing and there are a total of N+1 keys ($K_N, \ldots, K_0$). Once the sequence has been generated, the base key can be issued to all users. Security requires that the user can verify that the base key comes from the true source. A secure receiver may be designed to accomplish the verification through the internet or by examining multiple sources. In addition to the key, a verified broadcast schedule for the keys in the sequence is also obtained. As a result of the key generation, the base key can only verify the other keys but cannot generate them. This is a crucial point.

$$MAC_n = MAC\left(\left[M_{n,1},\ldots,M_{n,m}\right], H^1\left(K_n\right)\right)$$

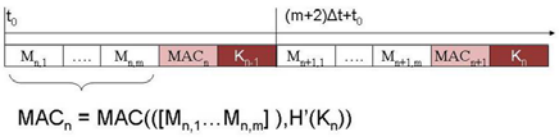

Figure 5. Basic TESLA message sequence for Navigation

The authentication of messages proceeds with the transmitter sending a set of *m* messages where *m* is the roughly number of messages between authentications. Increasing *m* makes the authentication more data efficient at the cost of longer authentication time and increased susceptibility to message loss. The susceptibility to loss is discussed later. Next it sends a message authentication code (MAC). In TESLA, the MAC is generated using a keyed-hash MAC (HMAC) algorithm. The HMAC algorithm uses an input key to create a unique MAC. In TESLA, the HMAC input key is derived from the hash of a key from the generated key sequence. The key sequence key is presumably the next unrevealed key from the sequence. The hash function used to transform that key to the input key is different from the one used to generate the key sequence. If the last authentication used key K_{n-1}, then K_n is used. Since the key K_n has yet be revealed, only the true transmitter can generate the MAC. The transmitter will later transmits K_n within its scheduled time window. Any MAC based on key K_n generated prior to its time window $[t_n, t_{n'}]$ can only have been generated by the authentic sender. Under TESLA, the user receiver must have loose time synchronization to the sender. If the user uncertainty is *dt*, then assurance exists only if the user receives the MAC prior to time t_n-*dt*.

A message design and implementation of TESLA for Loran has been made and demonstrated [9]. The implementation of TESLA on Loran used 8 messages per authentication, requiring significant

portion of the bandwidth. The ratio all messages to authentication messages is 8/(*m*+8). The authentication process could be spread out over time by increasing m, however message loss poses a problem since the loss of any of the *m*+8 message can prevent authentication. The probability of authentication is given by Equation 8 with *s* being the number of messages needed for authentication. While *s*=8 was implemented, this can be lower with the changes discussed next.

$$p_{auth} = \left(1 - p_{loss}\right)^{m+s} \quad (8)$$

4.3 Adapting TESLA for Navigation Channels

Adaptations of TESLA for navigation channels are possible to make it more suitable for Loran. One important issue is data loss. Modifications can be made to be more tolerant of message loss in a data efficient manner. One modification that can achieve this is to use a given key for several MACs. This change is useful especially if the key is longer than the MAC. This can be the case for *eLoran* as proposed MACs are in the neighborhood of 40 bits while keys are likely 120 bits or more. Another method is to authenticate only a random subset of messages. This can be achieved by providing a message mask which indicates the messages used to generate the MAC as seen in Figure 6. Suppose only a fraction (*f*) of the messages, are used, then the probability of authentication is given by Equation 9. A comparison of the performance of this implementation with nominal TESLA in terms of probability of authentication is seen in Figure 7. While an attacker may be able to occasionally pass an invalid message onto the user, the attacker cannot always guess correctly and their subterfuge can thus be detected.

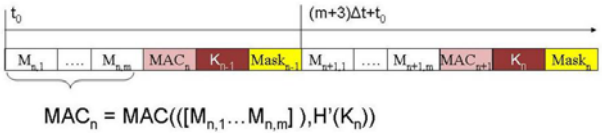

Figure 6. TESLA with Message Mask

$$p_{auth} = \left(1 - p_{loss}\right)^{fm+s+1} \quad (9)$$

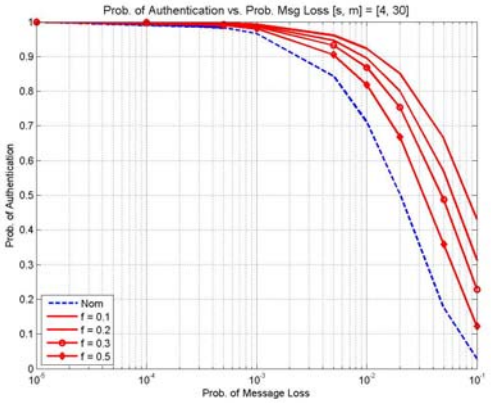

Figure 7. Probability of Authentication for Nominal TESLA and TESLA with Mask

Becker suggests an even more fundamental modification whereby only time is authenticated. In the technique, keys are released at exact times [20]. The receiver then validates the key and time with the stored base key and internal time. Provided that these are consistent, then the receiver is certain that the signal is from the source and is not delayed more than the uncertainty of internal time. The work so far represents initial efforts modifying data authentication to meet the needs and constraints of navigation systems.

One can imagine some feasible selective delay attacks even with TESLA implemented. So authentication protocols alone do not provide complete protection. It does, however, represent a critical piece of the solution. In the following discussion on using hidden and location factors for potential use, the ability to have authenticated data is important to the use of these factors for security.

4.4 Hidden and Location Dependent Markers

Location dependent information provides complimentary verification to data authentication. It can provide confirmation of location while techniques such as TESLA only verify that the data is unchanged. Hence, it overcomes a weakness of adapting data authentication to navigation. To provide the confirmation, trustworthy data is often needed and so data authentication is a critical component. One example of how this can be achieved on Loran is through the examination of cross rate interference (CRI). CRI effects are location dependent and will interfere with different data bits depending on location. So, different bits are "hidden" (i.e. the interference pattern differs) depending on location. With Reed Solomon error correction, these interfered (and not interfered) bits may be identified. Data authentication is needed to

verify that the messages are indeed from the actual transmitters and not spoofed data (since the spoofer would know every bit of that data). If these checks are implemented on the receiver, a direct injection spoofer must be able to replicate the lost and available bits at that location. If the spoofer is not at the spoofed location, this is more difficult. The unfortunate issue is that the resolution of this check is not likely not good, perhaps several kilometers. It is possible to augment the Loran broadcast specifically to improve the performance of the concept. We are currently investigating potential ideas in this area.

Hidden markers and code can be thought of as being a form of location dependent information as the user's location makes the information is difficult to observe. Other forms of hidden markers to aid authentication within the navigation signal have been suggested in the past. Scott suggested using hidden code within the GPS signal which can be decorrelated later using authenticated data. For Loran, Scott suggested using very small, nearly undetectable modulation using PPM to place hidden markers that can be detected later. These are really location dependent markers as they are only hidden because the receiver is at some distance from the transmitter.

5.0 A MULTISYSTEM APPROACH

Prior sections quantify and qualify the robustness of *eLoran* to potential attacks on radionavigation. This section examines how to use the resulting trusted signal or system as the cornerstone to trustworthy navigation. Specifically, having a trustworthy system such as *eLoran* can be leveraged to increase security within an integrated system. We examine basic ways of using a trusted signal to help determine the trustworthiness of other signals or systems. Hopefully, more detailed work will be presented in later papers.

One trusted signal is can be used to help validate a position solution. A straight forward use based on techniques used by receiver autonomous integrity monitoring (RAIM) algorithms. A trusted signal is an outlier for a spoofed position so RAIM can be used test if whether the trusted measurement is consistent with the other measurements. In fact, it is easier than traditional RAIM as the "outlier" is already isolated. So one way is to calculate a solution based on all non trusted measurements and examine the residuals of the trusted measurements (after eliminating common clock error). An example will be used to illustrate.

In this example, there is one trusted Loran signal and multiple (N) unverified GNSS signals. The Loran signal has a maximum bias b and error with variance σ_l^2 while the N GNSS signals are assumed to have variance σ_g^2 and are uncorrelated. If unspoofed, the GNSS signals have nominal biases that are negligible. We want to determine if the GNSS derived position has been spoofed. With one trusted signal, only deviations in one direction, that of the signal, are detectable. Assume that the maximum acceptable deviation is B. Using traditional weighted sum squared error RAIM, we can develop bounding distribution for a no fault (no spoofing or spoofing < B) and a faulted case (spoofing > B). We can use the technique discussed in [21] to overbound. Without going into the details of the derivation from [21], the bounding distributions for the two cases are given by Equations 11 and 12 provided the weighting matrix, W, is given by Equation 10. The first and second terms of the χ^2 distribution are the degree of freedom (for a 2-D and time solution) and the non centrality parameter, respectively. The degree of freedom equals the number of independent signals minus the number of dimensions to be solved (3 or 4). With this traditional hypothesis testing and thresholds for fault detection can be used.

$$W = \begin{bmatrix} \sigma_l^2 & 0 & \cdots & 0 \\ 0 & \sigma_g^2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_g^2 \end{bmatrix}^{-1} \quad (10)$$

$$H_0 \sim \chi^2\left(N-3, \left(\frac{b^2}{\sigma_l^2}\right)\right)$$

$$H_1 \sim \chi^2\left(N-3, \left(\frac{(B-b)^2}{\sigma_l^2}\right)\right) \quad (11, 12)$$

This RAIM approach is not necessarily the most efficient means of detecting spoofing. In fact, it does not directly utilize the fact that the authenticated "outlier" is known. Another means is to compare the range from the authenticated Loran using the position solution of the GNSS satellites with the measured Loran range. If that value is above some threshold, then spoofing or errors may exist.

6.0 CONCLUSIONS

The paper examines navigation security by presenting a case study of the security capability of *eLoran*. The first part of the paper discusses the possible attacks that could affect the signal and user. The attacks are divided into two categories: on-air and direct injection.

In analyzing on-air attacks, the paper quantifies the amount of power needed to jam or spoof Loran signals and determines the feasibility of an attacker to achieve these levels. While the required power is several orders of magnitude larger than that need to jam GNSS, it is still not very large. The difficulty in attacking Loran lies in generating the required radiated power from a short antenna. The analysis shows that generating a few milliwatts of output at low frequency on a small antenna requires significant input voltage. Hence, on-air jamming and spoofing is tremendously challenging and requires significant infrastructure to achieve. While certain forms of spoofing are easier, they still represent a significant challenge to an attacker. Even if the equipment issues can be overcome, spoofing effectiveness is limited in terms of the error inducible and detectability.

For direct injection attacks, the paper examines potential defenses that are or could be incorporated into the system. The paper develops techniques to aid the authentication of the Loran signal. While this has benefits against on-air attacks, it represents a major defense against direct injection attacks. This paper shows some ways of adapting techniques such as TESLA and location markers that are both feasible and can mitigate direct injection vulnerabilities. The paper also presents the concept of location based markers on Loran and how it could be utilized.

Finally, the paper shows that once there is a trusted navigation signal, traditional techniques can be applied to leverage that trust help secure unverified measurements.

7.0 DISCLAIMER

The views expressed herein are those of the authors and are not to be construed as official or reflecting the views of the U.S. Coast Guard, Federal Aviation Administration, Department of Transportation or Department of Homeland Security or any other person or organization.

8.0 ACKNOWLEDGEMENTS

The authors gratefully acknowledge the support of the Federal Aviation Administration and Mitchell Narins under Cooperative Agreement 2000-G-028. They are grateful for the support their support of Loran and the activities of the LORIPP. The authors would also like to acknowledge Tim Hardy and John Pinks at Nautel.

9.0 REFERENCES

[1] "Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System," John A. Volpe National Transportation System Center, August 20, 2001.

[2] Press Office, U.S. Department of Homeland Security, "Statement from DHS Press Secretary Laura Keehner on the Adoption of National Backup System to GPS," February 7, 2008

[3] General Lighthouse Authorities of the United Kingdom and Ireland, Research and Radionavigation, "The Case for *eLoran*," Version 1.0, May 2006

[4] Scott, L., "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems", Proceedings of the Institute of Navigation GPS Conference, Portland OR, Sept 2003

[5] Kuhn, Markus G., "An Asymmetric Security Mechanism for Navigation Signals", 6th Information Hiding Workshop, 23-25 May 2004, Toronto, Canada, Proceedings, LNCS 3200, pp. 239–252, Springer-Verlag.

[6] Bowditch, Nathaniel, "Chapter 12: Loran", *The American Practical Navigator*, Paradise Cay Publications, 2004

[7] Forssell, Borje, "The Dangers of GPS/GNSS", Coordinates, February 2009

[8] Humphrey, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., and Kintner, Jr., P. M., "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," Proceedings of the Institute of Navigation GNSS Conference, Savannah, GA, Sept 2008

[9] Qiu, Di, Lo, Sherman, Peterson, Benjamin, and Enge, Per, "Geoencryption Using Loran," Proceedings of the Institute of Navigation National Technical Meeting, San Diego, CA, January 2007

[10] International Radio Consultative Committee, "Ground-Wave Propagation Curves for Frequencies Between 10 kHz and 30 MHz", CCIR Recommendation 368-7, Geneva last updated 1992.

[11] Lo, Sherman and Enge, Per, "Analysis of the Enhanced LORAN Data Channel", Proceedings of the 2nd International Symposium on Integration of LORAN-C/Eurofix and EGNOS/Galileo, Bonn, Germany, February 2001, pp. 159-168

[12] Hardy, T., "The Next Generation LF Transmitter Technology for (e)LORAN," Proceedings of the Royal Institute of Navigation NAV08/International Loran Association 37th Annual Meeting, London, UK, October 2008

[13] Stutzman, Warren L., Thiele, Gary A., *Antenna Theory and Design*, Second Edition, John Wiley & Sons, Inc, New York, 1998

[14] Jordan, Edward C., *Electronmagnetic Waves and Radiating Systems*, Second Edition, Prentice-Hall, Englewood Cliffs, NJ, 1968

[15] Watt, Arthur D., *VLF Radio Engineering*, Pergamon Press, Oxford, 1967

[16] Johannessen, Erik, "Loran's Role in Future PAT," Proceedings of the 35th Annual Convention and Technical Symposium, Groton, CT, October 2006 (Presentation only)

[17] Wullems, C., Pozzobon, O., Kubik, K., "Signal Authentication and Integrity Schemes for Next Generation Global Navigation Satellite Systems," Proceedings of the European Navigation Conference GNSS, Munich, July 2005

[18] Perrig, A. Canetti, R., Tygar, J.D., and Song, D., "The TESLA Broadcast Authentication Protocol," CryptoBytes, 5:2, Summer/Fall 2002, pp. 2-13

[19] National Security Agency (NSA), The Case for Elliptic Curve Cryptography, 2009, http://www.nsa.gov/business/programs/elliptic_curve.shtml

[20] Becker, Georg, et. al., "Efficient authentication mechanisms: A Radio-navigation case study," Proceedings of the Institute of Navigation GNSS Conference, Savannah, GA, September 2009

[21] Lo, S., Peterson, B., and Enge, P., "Proving the Integrity of the Weighted Sum Squared Error (WSSE) Loran Cycle Confidence Algorithm" Navigation: The Journal of the Institute of Navigation, Vol. 54 No. 4, 2007